Private Yet Connected? Yes, We can: The Challenge of Decentralized Social Networks

Francesca Musiani

ParisTech REVIEW:

February 4th, 2011

Francesca Musiani
PhD candidate and researcher, Mines ParisTech

Private Yet Connected? Yes, We Can: The Challenge of Decentralized Social Networks

In the age when the massive success of social network sites relies on users' willingness to freely disclose their personal data for profiling purposes, issues of user privacy and personal data protection are under the spotlight. This article addresses current developments in the field of decentralized social networking as a way of countering the trade-off between privacy and connectivity in social network services. We argue that such tools may constitute the first attempt to fully leverage the social opportunity of virtual networking tools.

In the age when the massive success of social network sites relies on users' willingness to freely disclose their personal data for profiling purposes, the project of developing a "privacy-aware, personally controlled, do-it-all, open source social network" may come as a surprise. Widespread public interest in such a project may seem even more surprising.

Yet, this is how the story of Diaspora started. In April 2010, four undergraduates from New York University (NYU) set out to create a decentralized social network. They gave themselves 39 days to raise $10,000, and within 12, they met their target. Dan Grippi, one of the four developers, said in astonishment: "For some strange reason, everyone just agreed with this whole privacy thing".

This strange reason might very well be that, despite all odds, users—at least some of them—do care. While they obviously enjoy, and wish to continue enjoying, the potential of social networking sites for aggregation, communication, exchange, and interaction, users do not see privacy as a right they have to relinquish in exchange for the opportunity to connect. Thus, they might very willingly migrate towards the technology that would allow them to refuse, or at least partially counter, the trade-off between privacy and connectivity. For a start, they are donating their money to individuals who promise to dedicate their time, skills, and resources to develop such technology. These people—like the four young developers of Diaspora, currently the most media-savvy but by no means the only ones—claim that the privacy-connectivity trade-off can indeed be overcome. The solution is called decentralized social networking.

In this article, we address current developments in the field of decentralized social networking. We argue that open-source tools may constitute the first attempt to fully leverage the social opportunity of virtual networking, at a time when issues of user privacy and personal data protection are under the spotlight.

Decentralization, Social Networking, and Privacy of Personal Data

Since the inception of the Internet, the principle of decentralization has governed the circulation of information on the network of networks. However, the introduction of the World Wide Web in 1990 has progressively and widely led to the diffusion of client-server architecture models. The most widespread and diffused Internet-based services (e.g., social networks, instant messaging tools, digital content storage services) are based upon technical and economic models in which end users ask for information, data, Web server farms, information storage, and/or network "traffic" management. Thus, even if traffic on the Internet functions on the generalized distribution principle, it has now taken the form of concentration around servers delivering access to content. It is believed that this trend may expand even further due to the diffusion in the software- and platform-as-a-service (SaaS/PaaS) markets of the so-called "cloud computing" model. In this model, the

12 rue d'Athènes 75009 Paris, France - Email : contact@paristechreview.com / Landline : +33 1 79 85 81 19

Private Yet Connected? Yes, We Can: The Challenge of Decentralized Social Networks

vendor/service provider supplies the hardware infrastructure and the software product, thus hosting both the application and the data in a physical location unknown to the user (the "cloud"); the provider interacts with the user by means of a front-end portal. While cloud computing is the most frequently used network-based approach to organizing structures and services today, it is not the only one and it may not be the most effective. Scholars such as Barbara van Schewick, Eben Moglen, and Niva Elkin Koren have noted that one of the possible, and perhaps most promising, alternatives is decentralization: designing the network in such a way that communication and/or exchanges take place between nodes having the same responsibility within the system. Decentralization thus erases the dichotomy between server (provider of the service) and client(s) (requesters of the service), typical of the client-server model, and replaces it with a situation where every client becomes a server.

The most famous (or infamous, some may say) decentralized computer network models are doubtlessly those that have been used in the last 15 years in peer-to-peer (P2P) file sharing systems. Very frequently framed as a threat to the digital content industry—its most diffused use by the general public being the unauthorized sharing of copyright-protected materials—P2P technology is certainly well-suited to give free, and immediate, access to perfect copies. However, the decentralized, distributed architecture of P2P systems is, at a broader level, suited to promote increased effectiveness, freedom, and stability in online content distribution, enhanced by the direct connections between nodes-users of the system.

Following the widespread adoption of Facebook, and to a lesser extent Twitter, additional social networks have seen massive success in recent years. These networks are Web-based services that allow individuals to build a public or semi-public profile within a system, define a list of other users with whom to interact and establish relationships, and view the list of connections they and their friends make within the system. Among the most controversial aspects of social networks are the uses that managers and administrators make of private information. They often disclose data to third parties and sometimes use them for their own commercial purposes. Relatively few users are actually aware of the possibility of data collection by outside sources with access to company servers—something both legal and technical experts have now qualified as a significant privacy issue.

Towards Decentralized Social Networks

Recently, several research projects and commercial applications have attempted to propose solutions to counter at least some of the limitations of current social networks. Niva Elkin-Koren, dean of the University of Haifa Faculty of Law, has described these initiatives as favoring the "removal of intermediaries" in sharing and networking activities online. They mostly consist of decentralized alternatives to services and instruments that—under the names and centralized architectures of Google, Facebook, and Picasa—constitute today an important part of our everyday lives. Several questions arise: What if decentralized networking was applied to the social network of the future? Are the "first steps" of decentralized social networks the beginning of new implications and possibilities for the safeguard of the right to privacy, while maintaining, and perhaps improving, full connectivity? How are the developers of such tools reshaping the two networking models, so as to mutually reinforce them? We will use a few examples to illustrate what is currently happening in the field, in addition to the highly newsworthy Diaspora case.

The Social Virtual Private Network (VPN) Project, in development at the University of Florida, aims to connect users in a virtual network in which P2P links are automatically created at the application layer (the layer of the network that ensures effective communication between applications) based on links made at the layer of the social networking infrastructure. In short, social links determine network links. In this system, users act as the certification authority for their personal layer; they are given a certificate or key, which they distribute to their friends.

12 rue d'Athènes 75009 Paris, France - Email : contact@paristechreview.com / Landline : +33 1 79 85 81 19

Private Yet Connected? Yes, We Can: The Challenge of Decentralized Social Networks

NoseRub, a protocol for decentralized social networking, allows applications to store information about profile data for each contact. This means that users are able to keep their profile information on their own server and servers interact and synchronize automatically.

The Appleseed Project aims to create an open source, fully distributed, and decentralized social networking software. According to the founders, it is based upon the will to consider the user as "a citizen of the Net, rather than a consumer to target." "[S]pecial attention [is] paid to privacy and security," seen as constantly trampled on by publicity, product placement, and data management, widely present in "classic" social networks. After a period of financial trouble, the project is back in development. When it's done, users will be able to create a profile on an Appleseed compatible website and connect with users on another Appleseed website.

Most recently, as mentioned above, there's been the distributed social networking project Diaspora. After its initial fundraising success, it once again surpassed expectations in the summer of 2010 by raising $100,000. The way in which Diaspora aims at securing the privacy of its users is by making them the hosts of the node that contains their personal information. As Eben Moglen, the project's mentor (and more recently informal advisor) has pointed out, this constitutes "the second-generation social network architecture that offers sharing to everyone, without putting anybody in the middle, holding all the data for everybody else". Its underlying principle, like that of its "older" counterparts, is that the company partially or totally relinquishes its access to users' personal data as a privacy safeguard. This not only increases users' control, but also their responsibility, in terms of personal information. Separate computers, which Diaspora's developers call "seeds," are meant to connect to each other directly. An online technology blogger has described the seed as "an aggregator that will gather your content from around the Internet into a central location, your server. Link your seed to my seed and we can share and converse ... In short, you host your own profile that is a[n] amalgamation of your life online, and share with a select group of people".

The main challenge for these decentralized social networking projects is persuading users to switch to another service, especially one that may be less easy to use and technically developed in the short term. Given that the added value of these initiatives is the possibility for users to set up their own small servers to host their profiles, it's believed that decentralized products will ultimately fail to gain a wide enough following among users accustomed to a less complicated, more easily accessible interface. At the same time, recent public support for open source solutions tells another story. An online commentator says: "Perhaps the most damning critique of Facebook's recent controversial moves has been that a group of programmers have been raising money to create an alternative—and people are donating". If what it takes is awareness and support, this might just be the moment to dare and speed things up.

A Social Opportunity

The different projects and applications that are working towards possible hybrids between decentralization and social networks are perhaps the first attempt to fully leverage the social opportunity of networking tools. As University of Florida researchers Renato J. Figueiredo, P. Oscar Boykin, Pierre St. Juste, and David Wolinskypoint out, an important number of Internet users worldwide interact systematically with social networking websites. Yet, social networking infrastructures, skewed towards finding and establishing *social* links, are scarcely adapted to allowing connections between a user and his or her peers by means of *network* links. Thus, the challenge, and the key to more robust and safe social networks, is envisaging innovative architecture capable of integrating networking at both the interface and application levels, thus improving both connectivity and privacy.

The protection of private data on social networks appears to be bound to improve in two directions. On the one hand, the use of a decentralized, distributed

12 rue d'Athènes 75009 Paris, France - Email : contact@paristechreview.com / Landline : +33 1 79 85 81 19

Private Yet Connected? Yes, We Can: The Challenge of Decentralized Social Networks

or P2P architecture calls for a reconfiguration of data management practices with respect to the most widely used social networks today. This reconfiguration implies potentially far-reaching changes in the service provider's status, in what information it has access to, and in the material locations in which user-created content is stored and shared. On the other hand, these applications are also moving towards possible solutions to address some of the disadvantages of classic P2P networks. They are doing so by strengthening the personal character of requests and authorizations linked to the creation of network friendships, such as the "Add Friends" feature and the attribution of different degrees of trust according to different contacts within the network.

In his 2010 talk at NYU, indicated by the Diaspora team as their main source of inspiration, law professor Eben Moglen argued that what is currently labeled as the "cloud computing" shift only means, in a landscape of Internet-based services where the client-server paradigm is dominant, that "servers have gained [more] freedom. Freedom to move. Freedom to dance; to combine and to separate, re-aggregate, and do all sorts of tricks. Servers have gained freedom. Clients have gained nothing". However, a gain for clients should not necessarily mean the death of the cloud, or vice-versa. In a distributed network, where the boundaries between the client and the server get blurred or erased altogether, the freedom would be distributed as well, and so would the cloud. Indeed, the decentralized cloud may be just around the corner, and some companies have already taken on the challenge. One example is the French-based PaaS TioLive and its hosting and content management service TioLive Grid, which can be used to share the cloud's computing power and resources among the terminals of every contributing user. The idea behind TioLive Grid, says Jacques Honoré, community manager of TioLive, is "total freedom of users on the cloud and the possibility for them to control entirely, and by themselves, their personal data". Once again, we see that total user freedom and privacy are not incompatible goals.

User-hosted personal profiles, less intermediaries, clouds made of users, and so on. A lot can be done to balance the equation, and an increasing awareness of this—not only by a few developers, but by large groups of users as well—is most likely the "strange" reason why, as the astonished Dan Grippi remarked a few months ago, "everyone just agreed with this whole privacy thing." It is now up to researchers, companies, and communities of users worldwide, to leverage the social opportunities of decentralization for an increasingly connected world, where—albeit transformed and constantly recomposed—the private sphere may exist and be respected.

Academic

- Biddle, P., P. England, M. Peinado, and B. Willman (2002). "The Darknet and the Future of Content Distribution." ACM Workshop on Digital Rights Management.
- Boyd, D. and N. Ellison (2007). "Social Network Sites: Definition, History, and Scholarship." Journal of Computer-Mediated Communication, 13 (1).
- Diffie, W. and S. Landau (2007). Privacy on the Line: The Politics of Wiretapping and Encryption, Updated and Expanded Edition. Cambridge, MA: The MIT Press.
- Elkin-Koren, N. (2006). "Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic." New York Journal of Legislation and Public Policy, 9.
- Figueiredo, R. J., P. O. Boykin, P. St. Juste, and D. Wolinsky (2008). "Social VPNs: Integrating Overlay and Social Networks for Seamless P2P Networking." Proceedings of the 2008 IEEE 17th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. Washington, DC: IEEE Computer Society.
- Gross, R. and A. Acquisti (2005). Information Revelation and Privacy in Online Social Networks. Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society,

12 rue d'Athènes 75009 Paris, France - Email : contact@paristechreview.com / Landline : +33 1 79 85 81 19

Private Yet Connected? Yes, We Can: The Challenge of Decentralized Social Networks

Alexandria, VA, USA. New York, NY: ACM.

- Le Fessant, F. (2009). Les réseaux sociaux au secours des réseaux 'pair-à-pair'. Défense nationale et sécurité collective, 3.
- Moglen, E. (2010). "Freedom In The Cloud : Software Freedom, Privacy and Security for Web 2.0 and Cloud Computing." ISOC Meeting, New York Branch, 5 February 2010.
- Solove, D. (2006). The Digital Person: Technology and Privacy in the Information Age. New York, NY: NYU Press.
- Van Schewick, B. (2010). Internet Architecture and Innovation. Cambridge, MA: The MIT Press.
- Wood, J. A. (2010). "The Darknet: A Digital Copyright Revolution." Richmond Journal of Law & Technology, 16 (14).

12 rue d'Athènes 75009 Paris, France - Email : contact@paristechreview.com / Landline : +33 1 79 85 81 19