When social links are network links: The dawn of peer-to-peer social networks and its implications for privacy

Francesca Musiani

When social links are network links: The dawn of peer-to-peer social networks and its implications for privacy

Francesca Musiani*

* Centre de Sociologie de l'Innovation, MINES ParisTech/CNRS, Paris, France

Abstract

Despite the success they enjoy among Internet users today, social networking tools are currently subject to several controversies, notably concerning the uses their administrators make of users' private, personal data. Today, many projects and applications propose decentralised alternatives to such services, among which one of the most promising appears to be the construction of the social network on a peer-to-peer (P2P) architecture. This paper addresses and analyses the "first steps" of applications at the crossroads between social networks and P2P networks. More specifically, it discusses how such applications anticipate modifications in the management of users' right to privacy, by harnessing features such as anonymity and encryption on one hand, and knowledge of identity on the other – aspects generally identified with P2P networks and social networks, respectively – depending on the different functionalities and layers of the application.

Keywords: Peer-to-peer; social network; privacy; architecture; anonymity; identity.

1. Introduction. Connecting social and P2P networks?[1]

Peer-to-peer (often shortened into P2P, abbreviation that will be used in the remainder of this paper) is a computer network model structured in such a way that communications and exchanges happen between nodes having the same responsibility in the system (Schollmeier, 2001). Throughout its relatively brief history, P2P technology has often been treated, in public as well as academic debates, as a threat to the digital content industry – its most diffused use by the public being the unauthorized sharing of materials protected by intellectual property law, more specifically by copyright. It would be difficult to deny that the main strength underlying the worldwide success of P2P-based applications is their permitting free, and immediate, access to perfect copies (Biddle, England, Peinado, & Willman, 2002). Yet, it has recently been argued that the socio-technical significance, and the potential for change, of P2P technology are more likely to be found elsewhere, notably in the capacity of these systems to take advantage of their decentralised,

[1] A French version of this article is published in the journal *Terminal: technologie de l'information, culture et société*, n. 105, within the thematic issue « Technologies (et usages) de l'anonymat à l'heure de l'Internet ». Drafts of this English version were presented at the International Association of Media and Communication Researchers (IAMCR) 2010 Annual Conference, Communication Policy and Technology Section, Braga, Portugal, 18-22 July, 2010, and at the European Association for the Study of Science and Technology (EASST) 2010 Conference, Surveillance and Society Track, Trento, Italy, 2-4 September, 2010. I thank the editors and anonymous reviewers of Terminal, and my audiences of the two conferences, for their helpful questions, comments and suggestions.

distributed architecture so as to promote increased effectiveness, freedom and stability in online content distribution (Elkin-Koren, 2006; Hales, 2006).

The past few years have also witnessed the massive success of social networks – Web-based services allowing 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 see/scroll down the list of connections they, and other users, make within the system (boyd & Ellison, 2007). Among the most controversial aspects of social networks are the uses that their managers and administrators make of users' private, personal data, often by giving external applications the permission to access them, and sometimes according to direct commercial strategies of their own (boyd, 2008). It has been argued, as well, that very few users are actually aware of the fact that by using such applications, they open the door to the access by ill- or non-defined publics to private information stored on the servers of the companies proposing the service – a behaviour that has recently been qualified as "risky" by both legal and technical experts (Acquisti & Gross, 2006; Le Fessant, 2009).

In recent years, several research projects and commercial applications have tried to find their way into this scenario, by proposing solutions able to counter at least some of these limitations; solutions that might favour the "removal of intermediaries" (Elkin-Koren, 2006: 10) in sharing and networking activities online. These propositions mostly consist of decentralised alternatives to services and instruments that constitute today an important part of our everyday lives – under the names and the centralized architecture of Google, Facebook, Picasa, to name just three of the most widespread ones.

My attention will be focused here on one of these tools: the hybrid applications between P2P networks and social networks. More specifically, I analyse the ways in which they anticipate or suggest changes in the management of users' right to privacy, harnessing features such as anonymity and encryption on one hand, and identity knowledge on the other – aspects that are generally identified with P2P networking and social networks, respectively – depending on the different functionalities and layers of the application.

The article is organised as follows. The first section introduces how, in recent times, the concepts of privacy and personal data protection have been defined and operationally treated in the context of the new rights and challenges brought about by networking and sharing activities on the Internet. The second section points out the conceptualisations of such notions in P2P networking and social networking, respectively, and their implications for the subsequent case study analysis. The third section follows and discusses the case study of a distributed and "social" data storage application, treated here as an "experiment at work" of models and tendencies originated from the same concerns, priorities and questions raised in the domain of P2P social networking research, in terms of privacy concerns. Finally, the fourth section opens to the

present and close future of P2P social networking experiments, by discussing, in light of the case study, the opportunities and challenges faced by this innovation – before delving into some concluding remarks.

2. Privacy on the edge? The Where's and How's of personal data management in Web-based services

Since the inception of the Web twenty years ago, a number of voices have raised to define the Internet as the largest public space of today's world, due to the millions of people that every day exchange messages, generate and receive knowledge, strengthen political and social participation, play, buy and sell, through and on the Internet (Di Maggio, Hargittai, Neuman, & Robinson, 2001). Indeed, stressing that the Internet is currently the infrastructure that makes interconnectivity possible at a global level, it has even been argued that the Internet should be treated, from a juridical standpoint, as a common good (Delmas-Marty, 1994; Massit-Folléa, 2008). In addition to these arguments, sometimes blamed for their allegedly excessive technological optimism, the conditions for the preservation of the public space created by the Internet, at a practical level, are also discussed (Rodotà, 2006).

Indeed, the challenges posed by the current management of Internet-based services (challenges we have only begun to hint at in the introduction), and the governance of public space without borders that the Internet helps to create, determine at once new needs and new risks for its users, in their double capacity of consumers and citizens, as well as individuals. For example, the ongoing development of criminal practices online entails new developments in content control and filtering tools, which, in turn, negatively affect the right to privacy and the confidentiality of personal communications (Diffie & Landau, 2007). Is it necessary to actively try and prevent, or control, the Internet's privatization by any particular lobby? Is it desirable to foster among users a bottom-up, self-imposed set of good practices, or is the lack of regulation just a way to leave the Internet in the hands of "the strongest," be they political entities, or the laws of the market? (Musiani, 2009). What, in short, are the conditions for the Internet to elaborate its rules, and how can the "respect of liberties and rights for all its users" (Rodotà, 2006) be achieved, despite the tempting, but rather vague, choice of words?

These questions, entailing at a broader level issues of global Internet governance and management, are especially useful to ask – yet difficult to answer – in the specific context of privacy and personal data protection in sharing and networking activities online. In recent times, the right to privacy has not only entered or updated national constitutions and transnational charts, but with other rights – such as the safeguard of environment, access to information, right to communicate, consumer protection and enlarged/more direct participation in administrative decisions – it is one of the so-called "third generation

rights," the expression of new requirements raised by fast-paced developments in science and technology (Morbidelli, Pegoraro, Reposo, & Volpi, 2004: 44-45). Indeed, the daily life of Internet users is increasingly monitored, in the form of traces whenever they ask for, or provide, goods and services, when they seek information, when they move in real or virtual spaces. Thus, everyone's virtual social representation is gradually delineated with reference to the information left by each interaction and transaction, scattered in a variety of databases, data collections, and – what is most interesting for the purpose of this article – networks: every individual's personal data.

Personal data have been defined in recent European jurisprudence with intentionally broad and comprehensive vocabulary: the European Union Data Protection Directive reads it as

any information relating to an identified or identifiable natural person […, *i.e.*] one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (European Union, 2005).

Thus, in principle, the definition includes any information that relates to an identifiable individual, and considers the possibility that a piece of data may not be sufficiently revealing in itself about the individual it pertains to, but may become such (thus becoming included in sensitive personal data) if associated or aggregated to further information that could likely come into the possession of the data controller. Moreover, the definition acknowledges the different ways in which an individual may become identifiable. While a person's name is an obviously likely identifier, the same person can also be less directly identifiable from other information, including a combination of identification elements such as physical characteristics, pseudonyms or nicknames, occupation, address and family composition. The right of each individual to know what data are stored in which location, and the right to obtain transparency on the gathering and processing of such data by third parties, as is the case with every Web-based service, are very well laid out in the concept of *habeas data*.

As an evolution of the concept of *habeas corpus* – the historical starting point of fundamental personal liberties – the concept of *habeas data* was first introduced in several Latin-American legal systems (Rozo-Acuna, 2002), and more recently "exported" at the international level to highlight the need to safeguard personal data of Internet users, and respond to technological change. As noted by one of the pioneer authors on the subject,

We can say, metaphorically, that today the law of a modern state must provide an instrument that guarantees its citizens their right to use and freely dispose of their personal data, the same way they use and freely dispose of their body. (Frosini, 1988: 47, *my translation*).

The adaptation of the *habeas data* concept to the context of the Internet is not, however, an autonomous process inherent to new technologies, but rather the result of choices made by actors in the market and the

political arena, who may use in different ways the data they "harvest" in the discreet and invisible – yet omnipresent and with strong social implications –infrastructures (Star, 1999: 379), such as computer networks. Thus, the issues concerning the development of the concept of *habeas data* cover both the actions of governments and of businesses. To what extent can governments claim the right to intercept electronic communications daily, for security reasons, or to monitor allegedly criminal activities? Is it possible to have a precise idea of what companies, especially those who are in the position to collect large amounts of personal data such as major search portals, or social networks, do with these data? It has been argued that commercial usage of the Internet may now be taking precedence over other uses, thus exposing the "network society" to the risk of increasingly identifying itself with its market and monetary exchange dimensions, in which only the rights related to transactions in goods and services would be recognized as such (Castells, 2000).

The notions of public and private are interwoven and constantly blurring boundaries, and users of the "network of networks" leave behind them traces of their presence and actions, in their dual capacity as consumers and citizens (Solove, 2006). While the safeguard of data on telephone and email traffic is assured (and, if need be, their disclosure is managed) by law enforcement and juridical entities, private companies proposing Web-based services largely draw, in turn, on their own databases for related commercial purposes, including the definition of targeted marketing strategies (boyd, 2008). While commercial enterprises are generally not allowed to access the databases of Internet service providers (ISPs) in the same way governments are able to do, they can still deduct, or collect, personal information in several ways and by means of several tools – most of them inexpensive – and trace consumer profiles to customize product offerings and find separate market *niches* (Johnson, Crawford, & Palfrey, 2004). The use of *cookies* is, for example, a possible way to record the number of times a person visits a Web page, a feature that does not, in itself, provide enough information about the visitor, but in addition to a number of other pieces of data may, as the EU Directive points out, provide fairly accurate representations of potential consumers. In what David Lyon has defined the "world wide web of surveillance" (Lyon, 1988: 37-47), monitoring of the user/consumer is a growing phenomenon. The increased participation, especially of particular groups of users, to electronic commerce also raises issues of intrusion and surveillance. The ways in which personal data are treated are likely to influence, reinforce or weaken power structures, be they market- or politics-dependent, that rely on the tampering of privacy and related rights in order to thrive and be successful.

3. What privacy? Sharing, networking, and personal data

In both P2P networks and social networks, what has been discussed up to this point in terms of privacy and personal data is relevant in different ways, that entail what types of personal information, data or materials are, or can be, made available in/on the network and how. Privacy issues in social networking services have to do with personal information such as the individual's belonging to certain demographics, and his or her behavioral preferences; those dealing with P2P networks are concerned with how personal digital files are shared, protected and saved within the network. It is worth outlining in some more detail these two conceptualizations of privacy and personal information, so as to better understand how these are re-composed in the application considered as our case study, into possibly innovative conceptions and definitions of privacy.

Social networking services, as noted by boyd & Ellison (2007), may vary substantially in appearance and features, but share an important one: through the Web site constituting the platform of the service, individuals build a profile they deem representative of themselves, for others to be able to get in touch for a variety of reasons, from dating to job recommendation. The profile is built out of information freely disclosed by users of the service, generally concerning demographics, tastes, professional aspirations, political inclinations and behavioral preferences (Dwyer, Hiltz, & Passerini, 2007), and even concerning more directly and personally identifiable information such as addresses, phone numbers, and other contact information. Moreover, while the intended recipient of such information and the "user portraits" it determines are in the first place the authorized contacts of the user within the service, these are not the only entities to whom such information becomes available (Le Fessant, 2009). As pointed out by Gross & Acquisti:

To whom may identifiable information be made available? First of all, of course, the hosting site, that may use and extend the information (both knowingly and unknowingly revealed by the participant) in different ways […] time (that is, data durability) and space (that is, membership extension) may not be fully known or knowable by the participant. Finally, the easiness of joining and extending one's network, and the lack of basic security measures […] make it easy for third parties (from hackers to government agencies) to access participants data without the site's direct collaboration. (Gross & Acquisti, 2006: 74).

In short, privacy implications raised by social networking practices depend on how much of one's identity is, intentionally or unintentionally, disclosed and known to other users; how much the information provided by users is identifiable, how their very identity may come to be (too) openly disclosed – to whom, and for what purposes and uses.

Privacy-related issues concerning P2P networking have to do with a different type of "personal data," the content peers upload and share within the network.

Firstly, a peer's data stream may be compromised by the other peers in the network that are contributing to the very process of data transmission, because these peers have direct access to the data packets. So, users need to have some knowledge about the software they are using, and they need to be aware of what types of materials and information are being shared (or those they do not want to share). As Suvanto points out, it is "quite possible to share the entire hard drive, including sensitive information such as mailbox and private documents. The user has to make sure, that the shared documents do not contain personal information which could be misused." (Suvanto, 2005). Studies have found that users are, for the most part, unaware or only partially aware of the privacy implications of using a P2P application, mostly due to the ease-of-use of many P2P file sharing applications, which may facilitate the task for potential attackers (Li, 2007).

Secondly, another aspect of privacy related to P2P networks concerns the information being sent by the P2P software, that, in order to establish a connection between peers, needs information such as their IP address. In some of the first, most popular P2P file sharing systems, this address has been used openly and directly exposed, thus raising anonymity problems (Suvanto, 2005).

In order to counter such weaknesses, and their exploitation by whatever entity willing to tamper with the stability and integrity of the network, recent P2P developments have been moving in two directions, encryption of contents and improved anonymity. On one hand, by encrypting P2P traffic, not only is the data more safely encrypted, but the P2P connection streams in themselves are less easily detectable, thus making the data traffic more resilient to attacks and blocks. On the other hand, by anonymizing peers, the P2P network can protect the identity of nodes and users on the network, especially in combination with encrypting techniques. As Li points out:

While true anonymity cannot really exist on a network, an anonymous P2P provides enough anonymity such that it is extremely difficult to find the source or destination of a data stream. It does this by making all peers on the network universal senders and universal receivers, thus making it practically impossible to determine if a peer is receiving a chunk of data or simply passing it through. […] using encryption together with anonymous P2P would yield possibly the most secure P2P usage experience available today. (Li, 2007).

Thus, privacy can be defined and conceptualized – as well as assured, or tampered with – by means of different treatments and management of data, and depending on different priorities deriving from external and contextual factors, among which are notably included a variety of rights and prohibitions, and ways to enforce them. Due to its far-reaching implications, that have just been discussed, experts have widely recognized and debated at length the importance of addressing the issue of privacy in applications willing to leverage the potential of social networking sites for aggregation, communication and interaction (Preibusch, Hoser, Guerses, & Berendt, 2007), or the suitability of the distributed networking model to low-

cost distribution of creative content, responsiveness to content demand (Wood, 2010), stability and redundancy in the preservation of data (Hales, 2006), and removal of intermediaries in between-users connections (Elkin-Koren, 2006). A question rises spontaneous out of such concerns: what if the social networking paradigm and the P2P networking system were mixed? Is the dawn of P2P social networks the beginning of new implications and possibilities for privacy? The remainder of this paper attempts an answer to such questions, by means of a case study, and a subsequent discussion of the opportunities and challenges faced by applications – currently moving their "first steps" – at the crossroads between social networks and P2P networks. In doing so, it closely follows how the developers of such applications seek to compose and recompose key features in the creation of the network, such as anonymity, encryption, and identity knowledge – according to different functionalities and layers in the application, and to ultimately reinforce its stability and performance.

4. Experiments at work: the "social storage" example

The interest surrounding hybrids between P2P networks and social networks can currently be retraced in a number of university research projects and start-ups.[2] This interest widens the purely technical debate, and goes as far as to entail the issues discussed above: issues pertaining to economics, history, ethics and law, often strictly linked with better safeguards of the right to privacy (Garnier, 2009). P2P social networking applications are currently in embryonic stages, those of protocols or "visions"; however, some applications at a more advanced development stage are already operational, and can be considered as experiments of models and tendencies originated from the same concerns, priorities and questions raised in the domain of P2P social networking research, especially in terms of privacy and confidentiality.

In order to flesh out these tendencies, I will tell the story of one of these applications, called Wuala,[3] by means of a qualitative analysis of several materials concerning it.[4] A small company based in Switzerland, Wuala proposes a service described by the company itself as « online social storage » (Wuala Features, n.d.) of data (Fig. 1).

[2] As shown e.g. by the seminar *« Le travail coopératif : prochain défi du pair-à-pair ? »,* INRIA Rocquencourt, May 14th, 2009, materials retrieved from http://www-c.inria.fr/Internet/rendez-vous/iliatech/pair-pair.

[3] Originated from the likewise-pronounced French word « voilà », meaning « here are your files » (Wuala Frequently Answered Questions, n.d.).

[4] More precisely, conferences available online, Web site of the company, release notes for the different versions of the application, interventions on the user support forum, interviews of the author with developers.

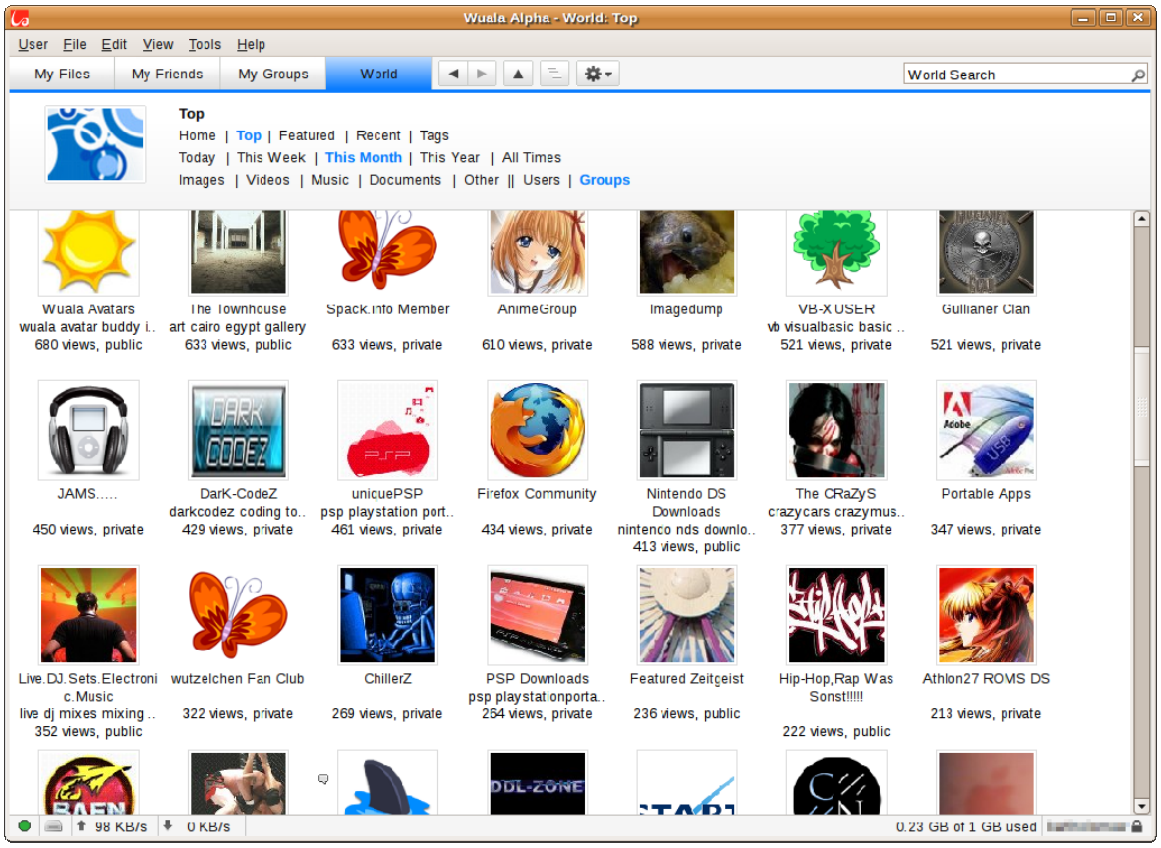

Fig. 1. Screenshot of Wuala interface, 'World' area. Closed Alpha version, running on Ubuntu operating system. Image by Daniel Bartholomew as published on LinuxJournal.com*.*

The creators of Wuala seem to share the concern of many innovators currently tackling the development of « next-generation » P2P applications: i.e., the necessity to conceptualize and manufacture these applications according to a "social-based paradigm" (Pouwelse et al., 2006), the modelization of social phenomena such as friendship links, affinity-based community formation, attribution of trust. This in order to modify the ease of use and the performance of P2P tools – a technology that, while permitting *de facto* the formation of networks, groups and relations, has historically attributed to its nodes-users the role of anonymous, unlinked entities (Pouwelse et al., 2006: 127). As one of Wuala's founders points out:

Wuala is a new way of storing, sharing, and publishing files on the Internet. Unlike traditional online storage systems, Wuala is decentralized and can harness idle resources of participating computers to build a large, secure, and reliable online storage. This enables its users to trade parts of their local storage for online storage and it allows us to provide a better service for free (Stern, 2007).

The *natural* continuity between storage and sharing functions hinted at here, as well as the suitability of P2P technology to the preservation of such continuity, is found in the words of a Wuala team member:

(Y)ou start with one gigabyte of storage, which is provided by us, but if you want more, you can trade local disk space to get additional online storage (Fig. 2). So in a sense, it is an online storage with the power of P2P, which means that you get fast downloads, there is no file size limit, there is no traffic limit and there are a number of other advantages, which really come as a result of the underlying P2P technology (Grolimund, 2007).

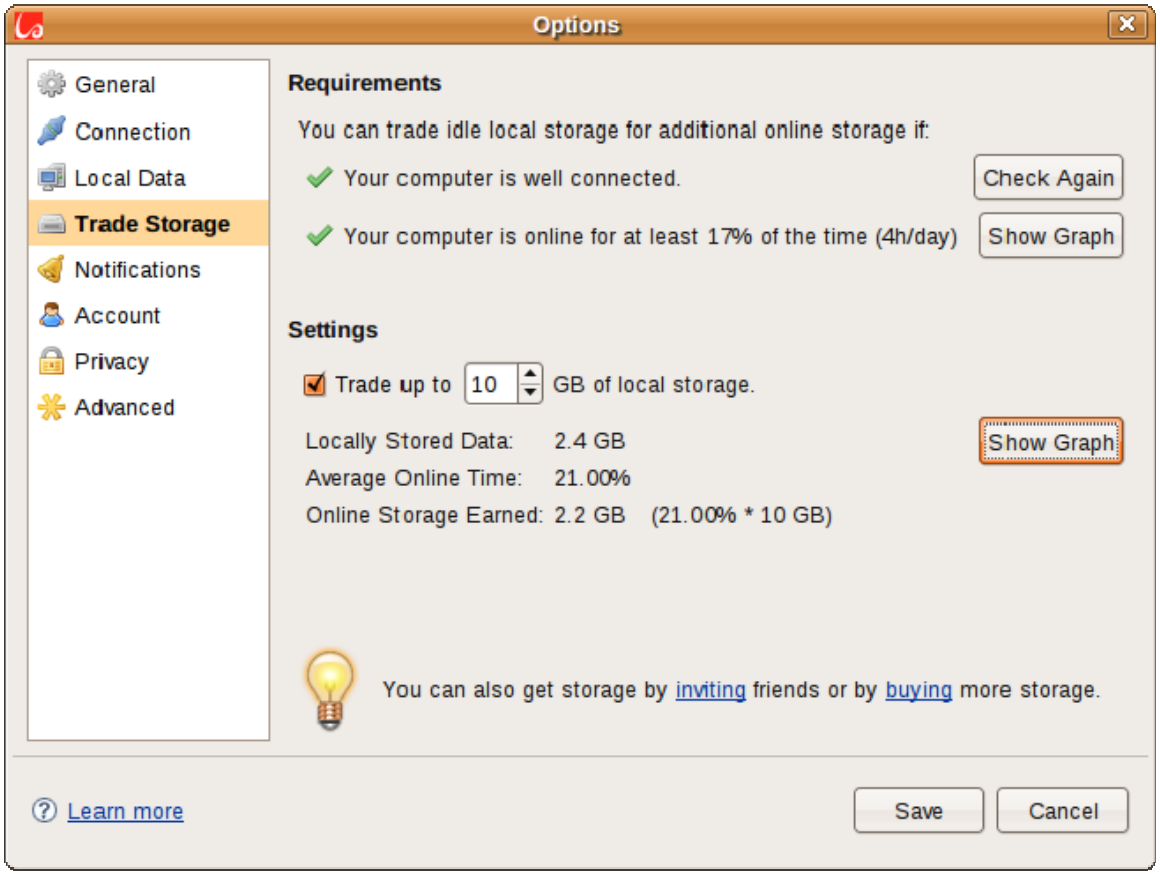

Fig. 2. Screenshot of Wuala's 'Trade Storage' feature, the way it is monitored by the user. Closed Alpha version, running on Ubuntu operating system. Image by Daniel Bartholomew as published on LinuxJournal.com.

Thus, what are these advantages, and why could the Wuala device be an appropriate way to leverage them? As the license to the user, the explanations in the company's website, and the developers

themselves highlight, the advantages have primarily to do with the treatment of aspects linked to the user's privacy. Aspects that are, indeed, more and more explicitly put among the core issues faced by innovators in the domain: a statement emphasized by Wuala's founders, while they underline the specifically European tendency to include such concerns in information technology research:

In Europe, privacy is an important issue and we think that everyone should have a place where he can store files privately. A lot of people are concerned if all their data is stored on servers of big corporations, which is why a lot of users do not use Gmail (and similar services). In our system, everything is encrypted, and it is state-of-the-art encryption (Grolimund, 2007).

4.1. The user's password, the user's computer… the user's responsibility

The first of these aspects – that is indeed striking for users as they first open the application after its download – concerns the password, which is qualified as the unique identifier of the user *vis-à-vis* the application. In particular, what seems unusual is the material location of the password and the treatment it receives. Indeed, the online digital subscription form warns that "your password never leaves your computer, hence, we do not know your password. Please do not forget your password and use, if needed, the password hint you specified when creating your account" (Wuala Frequently Answered Questions, n.d.).

A change of balance begins to appear between the respective weights of the rights that users enjoy on their data, as their creators and first owners, and the rights claimed and acquired by the service provider on the same data, as a condition for the service to be implemented. The trade-off? The service provider cannot retrieve the password if needed: thus, not only do users see their privacy strengthened, but at the same time and for the same reasons, their responsibility of the actions they undertake by means of the application is augmented. While, on their side, service providers relinquish out of their own volition some extent of their control on contents circulating within, and by means of, the service they are managing.

An aspect that has been only hinted at previously, that constitutes a second, important element in the management of the right to privacy, is that the password does not leave the computer of the user who created it. The operations, mostly managed automatically, linked to the protection of personal data are therefore hosted on the very computer of each user; thus, the user's place within the architecture of the application is turned into that of a node among equivalent nodes, rather than that of a starting and arrival point for operations that are otherwise conducted on another computer. The protection of data is also ensured by the fact that « all files are encrypted on your computer, before anything is uploaded. All encryption and decryption is performed locally » (Grolimund, 2007) – thus, once again, at the personal computer level.

4.2. Storing and sharing in a network of peers…

What is the status, at this moment, of the digital material that is stored, or shared, by means of the application? As we recall, Wuala is a decentralised tool, therefore the material location of the contents it manages is the P2P network constituted by the set of computers belonging to the application's users. Thus, the challenge is not only to ensure that the extraction of a complete file is possible at any time, but also – our main concern here – that any user of the system is able to access contents he or she is not the intended recipient of: in short, to reach a balance between the responsiveness of the tool with respect to its intended purpose, and the confidentiality of the data circulating in it. Wuala's developers are addressing this problem by working in three directions: encryption, fragmentation and redundancy – three aspects that are crucial in operations of storage as well as of sharing.

In the first case, when users upload a file in Wuala, this is first of all encrypted on the computer, as we have seen. Then, the encrypted file is split into fragments and these are redundantly encoded, again on the user's computer, before being uploaded in the P2P network of users. For sharing operations, the "friendship key" comes into play, an authorisation of exchange known only to who creates it and who receives it: this is what makes the reconstruction of the file possible. One of Wuala's team members points out:

Now let's say that Alice wants to share the file with Bob. When they first got friends, Alice and Bob have exchanged the friendship key, now Alice encrypts the file key with the friendship key (…) and exchanges it with Bob, who proceeds to download the file. What Bob tries to do is that he wants to find end fragments, a subset of all fragments, from the P2P network. (…) Then the application would decode, decrypt, and open the file. So these are the basic steps when you upload and download a file (Grolimund, 2007).

Every file is therefore stored and introduced in the network under the form of encrypted fragments.[5] Its material location – or rather, its multiple material locations – is therefore the network made of the set of computers; the re-constitution and the extraction of the file are also taking advantage of the P2P network's suitability to safeguard and distribute effectively, and give rapid access to copies, or fragments of copies, directly available on the network of users (Fig. 3).

[5] The scope of the present paper does not allow us to account for the different modifications that have, overtime, concerned the presence and the role of a central server, used both as a security safeguard and as a "main node" so as to ensure redundancy in the bootstrapping phase (i.e., until the number of users adopting the system became sufficient to ensure stability).

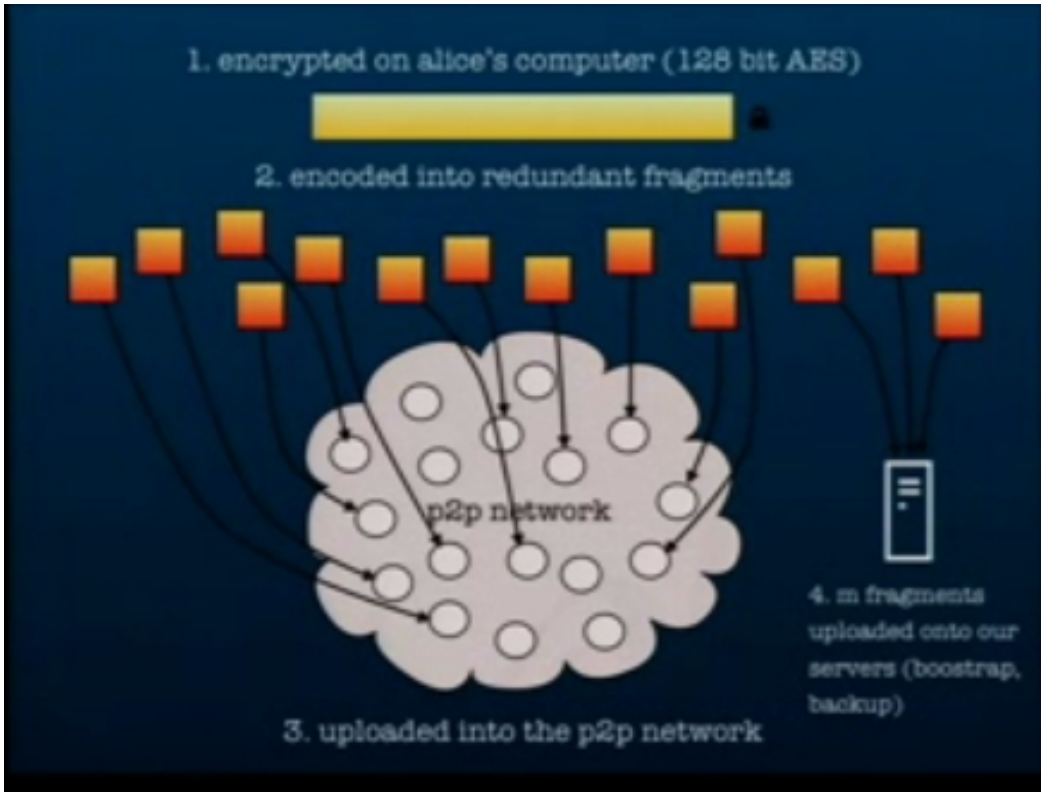

Fig. 3. Screenshot of Dominik Grolimund's Google Tech Talk about Wuala, retrieved from http://www.wuala.com/en/learn/techtalk. Image by Peter Sennhauser as published on Neuerdings.com.

This feature, just as the operations concerning each user's private data taking place on his or her machine, are taking advantage of the capacity of P2P networks to anonymise exchanges with respect to those involving a central authority, internal or external to the tool.

4.3. … creating direct friendship links

The introduction of a mechanism to « add friends », typical of social networks, and the direct relation between the friendship link established and the access to the friend's private data – a relation from which intermediaries are excluded – strengthens the confidentiality dimension in storage and sharing activities in such a way that is, insofar, not allowed by the most popular social networks of today. Le Fessant argues in this respect that "the 'Add Friends' mechanism, based upon the exchange on a private channel of a secret key, valid only once, has two advantages: it authorises the access to some or some other data. Thus, the

user identifies every person connecting to his or her machine; according to the degree of trust attributed, the door is open to some or some other personal data" (Le Fessant, 2009: 34, *my translation*)

When it comes to the reciprocal attribution of trust between users, the rationale behind the tool is no longer anonymity, Wuala's developers say:

(…If you are his friend) you can see that every file has been uploaded by a particular user. You can directly jump to his account and see what other files he shares with you. (…) So our system is really not about anonymising, that was the intention of Freenet, our system is about building a legal platform, an online storage where everyone has his or her space to upload files (Grolimund, 2007).

Moreover, from the user's viewpoint, the "social" functions of the tool are more evident thanks to its interface, built in order to suggest a continuity with today's most popular social networks: vocabulary such as "profile," "share," "friends" and "groups" is reprised, but adapted to the storage mechanism typical of the tool, giving each user the option of attributing different degrees of trust (to friends, or to the network as a whole for public directories), for each of the files stored in Wuala (Fig. 4). As one of the developers points out, "The main window looks very similar to any file system, you have different folders (…) that have different colours. The yellow folders are private, so only you have access to them, the red folders are shared with a definite number of friends, and the blue ones are published, these are the ones everybody can access" (Grolimund, 2007).

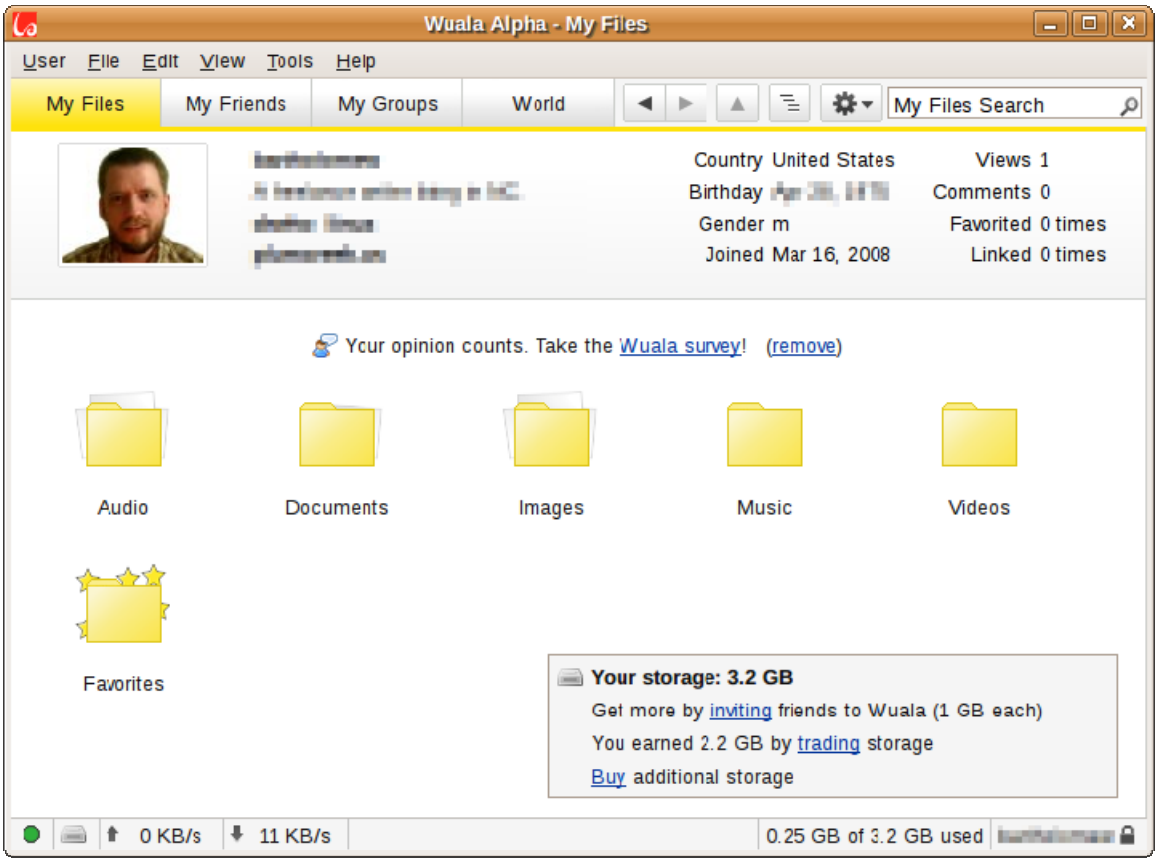

Fig. 4. *Fig. 2. Screenshot of the main Wuala interface. Closed Alpha version, running on Ubuntu operating system. Image by Daniel Bartholomew as published on* LinuxJournal.com.

5. Towards peer-to-peer social networks

Our journey in Wuala's « social storage » allows us to conclude that the main beneficiary of the co-existence of P2P technology at the layer of safeguard and extraction of stored content, and of a social network model at the layer of friendship links and trust attribution, is in the first place the protection of personal data; more broadly, the definition of who or what has access to what data within and by means of the application.[6] Will this tendency find further confirmation, in case peer-to-peer social networks become largely adopted in a close future? And if yes, how?

[6] As the scope of this paper is to use the analysis of Wuala as a case study of possible innovations in terms of privacy in emerging applications of P2P social networking, we do not address here the difficulties and challenges of implementation of a system as Wuala (to name just two, data consistency and the building of a durable reputation system), even if they are very important questions for the functioning and stability of the tool – questions who deserve to be made explicit and delved into in other venues.

The common concern in the different projects and applications that – and increasingly so – are aimed at delving into possible hybrids between P2P and social networks has in fact, I argue, mostly to do with a *social opportunity*: an important number of Internet users worldwide interacts systematically, nowadays, with social networking websites. Yet, social networking infrastructures are very suitable and skewed towards finding and establishing *social* links, but scarcely adapted to allowing connections between a user and his pairs by means of *network* links (Figueiredo, Boykin, St. Juste, & Wolinsky, 2008). Thus, the challenge, and the key to more robust and safe social networks, becomes to envisage innovative architectures able to integrate networking at both the interface and application levels.

The interest of such an approach becomes more evident if we consider it from the perspective of confidentiality and control on personal data, because if it is true that more and more Internet users are also users of social networking services, many of them are also worried by the unclear conditions, or too heavy (in terms of privileges conceded on the data) restrictions, bestowed upon the social networking service provider when they accept to use it (L'Atelier BNP Paribas, 2010).

How to translate these concerns into robust, long-lasting and secure architectures is currently the main preoccupation of interested researchers and developers, while the awareness and the interest of the public at large for privacy-related issues are increasing (Kirkpatrick, 2010).

The Social Virtual Private Networks (VPNs) in development at the University of Florida (Figueiredo et al., 2008) aim at linking users in a virtual network, in which P2P links are created at the application layer, automatically, depending on the links established at the layer of the social networking infrastructure. In this system, every user is the certification authority for its profile layer, giving each member of his layer (thus, his contacts) a certificate or a key he is the creator of (L'Atelier BNP Paribas, 2010), not unlike the friendship key in Wuala.

NoseRub, a protocol for decentralized social networking of which a prototype currently exists, allows applications using the protocol to store information on data composing the profile of each contact. This gives room for users of the network to keep their profile information on their own terminals, and for their terminals to interact and synchronise automatically (NoseRub Quick Facts, n.d.).

Appleseed, a decentralised social network project/vision, is based upon the will to consider the user as "a citizen of the Net, rather than a consumer to target," and on a "special attention paid to privacy and security," seen as constantly trampled on by publicity, product placement, and data management, widely present in "classic" social networks (The Appleseed Project, Docs, n.d.). After a period of financial trouble, the project is in progress again, and aims at building a model of distributed network, in which a profile on an Appleseed website is able to befriend a profile on another Appleseed website, and allows for the two profiles to interact directly.

Most recently, the distributed social networking project Diaspora* has raised nearly ten times more funding than its creators, four New York University (NYU) programming students, initially expected. Has this been achieved by showcasing the project's primary goal as the creation of "the privacy-aware, personally controlled, do-it-all, open source social network" (Diaspora* home page, 2010)? The central role that the privacy-related vocabulary occupies on the project's home page seems an unambiguous indicator of what is important to the developers and what they think is the main specificity and possible stand-out feature of their project – as well as what they believe can matter for their intended pool of users (Fig. 5).

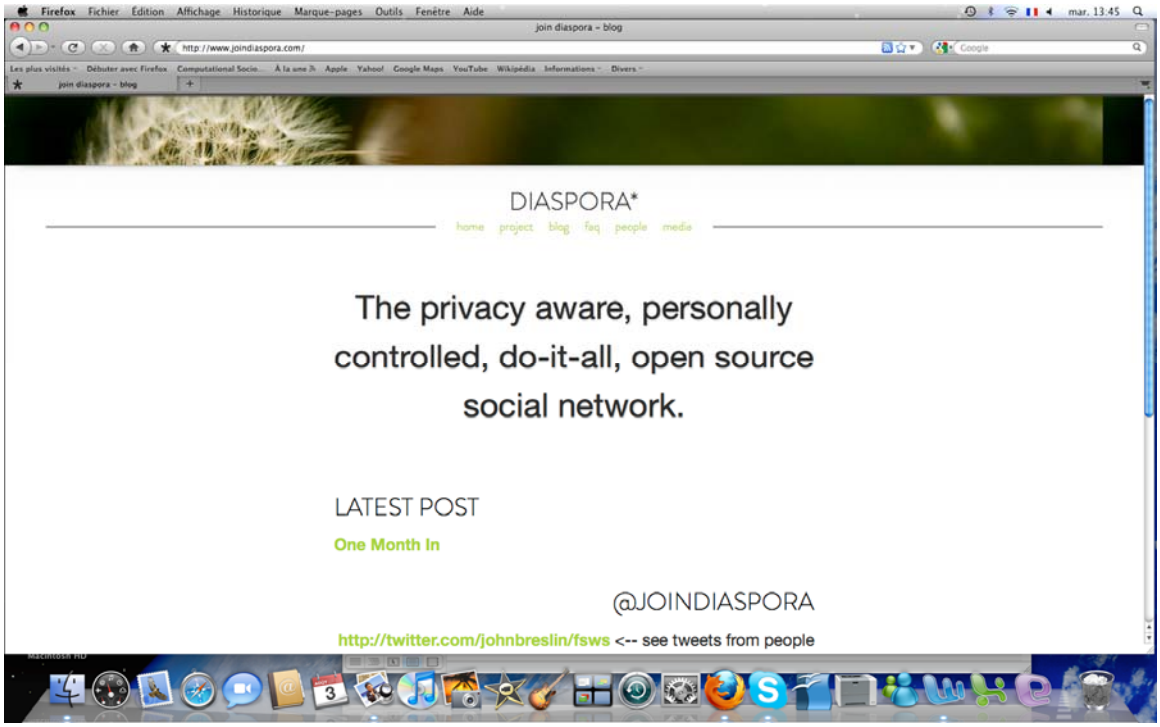

Fig. 5. Screenshot of Diaspora's home page, retrieved from http://www.joindiaspora.com/. Image by Francesca Musiani.*

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 we have seen with Wuala's treatment of passwords, the principle is that the company partially or totally relinquishes its access to users' data, as a guarantee of lack of infringement on their privacy. Totally separate computers, called 'seeds' by the developers, are meant to connect to each other directly. Wilhelm (2010) describes Diaspora*'s seeds as aggregators "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 amalgamation of your life online, and share with a select group of people."

As Diaspora*'s added value proposition is, in short, for users to set up their own seed servers, it is believed that this product may ultimately fail to gain a wide enough following among users accustomed to a less complicated, more easily accessible interface (Wilhelm, 2010; McCarthy, 2010). Yet, as a commentator pointed out, "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." (McCarthy, 2010).

6. Concluding remarks

The analysis of Wuala as a case study – and more broadly, of current projects and main focus of interest in the field of social networking tools in P2P – leads us to observe two directions that may potentially improve the protection of private data of social networks' users, in light of the initial discussion on privacy issues for both P2P and social networking models. On one hand, the use of a P2P architecture calls for a reconfiguration of data management practices, with respect to the most widely used social networks today; this reconfiguration implies potentially long-reaching changes in the service provider's status, in what information it has access to, and in the material locations in which storage and sharing operations of user-created content are conducted. Inversely, these applications are also moving towards possible solutions of some weaknesses of classic P2P networks, that, so as to make filtering, blocks and identifications more difficult for whoever tampers with the network, maintain as much as possible the anonymity of users, even in those cases when the reciprocal knowledge of identity between users as communicating nodes would have contributed to the stability, and robustness, of the network itself. Thus, we observe a tendency to strengthen the *personal* character of requests and authorisations linked to the establishment of friendships on the network, such as the "Add Friends" feature and the attribution of different degrees of trust according to different contacts within the network.

According to Eben Moglen, 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." (Moglen, 2010). Could an increasing awareness of this fact – at least among particular groups of users – be the "strange" reason why, as an astonished Dan Grippi (one of the four Diaspora* developers) remarked a few months ago, "everyone just agreed with this whole privacy thing" (Dwyer, 2010)?

However, the interest in following closely current developments in the emerging field of P2P social networking does not lie on the side of social networks only. As of today, a number of juridical interventions are scheduled or enacted that aim at reducing drastically, or eliminating, a certain type of peer-to-peer traffic – measures that carry within them the risk of losing or minimizing possible benefits that can be drawn from "legitimate/legal" peer-to-peer, increasingly put forward as a valuable alternative for a variety of applications and services.

The newborn hybrids between social and P2P networks are the example of a definition of privacy built upon the dialogue, and not the opposition traditionally observed, of the two aspects of identity knowledge and anonymity. Future research is likely to shed further light on social and juridical implications of this dialectic, as these applications grow in size, scope and reach.

References

Acquisti, A. & R. Gross (2006). *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*. In P. Golle & G. Danezis (eds.), Proceedings of 6th Workshop on Privacy Enhancing Technologies, Cambridge, U.K: Robinson College, 36-58.

Bartholomew, D. (2008). *Online Storage with Wuala*. LinuxJournal.com. Retrieved from http://www.linuxjournal.com/content/online-storage-wuala.

Biddle, P., P. England, M. Peinado, & B. Willman (2002). *The Darknet and the Future of Content Distribution*. ACM Workshop on Digital Rights Management.

boyd, d. (2008). *Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence*. Convergence, 14 (1).

boyd, d. & N. Ellison (2007). *Social Network Sites: Definition, History, and Scholarship*. Journal of Computer-Mediated Communication, 13 (1).

Castells, M. (2000). *Toward a Sociology of the Networked Society*. Contemporary Sociology, 29 (5), 693-699.

Delmas-Marty, M. (1994). *Pour un droit commun*. Paris: Editions du Seuil.

Diaspora* home page (2010). Retrieved from http://www.joindiaspora.com/index.html.

Di Maggio, P., E. Hargittai, W. R. Neuman & J. P. Robinson (2001). *Social Implications of the Internet*. Annual Review of Sociology, 27, 307-336.

Dwyer, J. (2010). *Four Nerds and a Cry to Arms Against Facebook*. The New York Times, May 11, 2010. Retrieved from http://www.nytimes.com/2010/05/12/nyregion/12about.html.

Dwyer, K., S. R. Hiltz, & K. Passerini (2007). *Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace*. Proceedings of the Thirteenth Americas Conference on Information Systems, August 9-12, 2007, Keystone, Colorado.

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: 1-61.

European Union (1995). Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data). Retrieved from http://eurlex.europa.eu/Notice.do?val=307229:cs&lang=en&list=307229:cs,&pos=1&page=1&nbl=1&pgs=10&hwords=95/46/EC~&checktexte=checkbox&visu=#texte.

Figueiredo, R. J., P. O. Boykin, P. St. Juste, & 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, 93-98. Retrieved from http://byron.acis.ufl.edu/papers/cops08.pdf

Frosini, V. (1988). *Informática y Derecho*. Bogotá: Editorial Temis S.A.

Garnier, A. (2009). *Les réseaux sociaux P2P : prospectives et usages*. Communication presented at the seminar « Le travail coopératif : prochain défi du pair-à-pair ? ». INRIA Rocquencourt, 14 mai 2009.

Grolimund, D. (2007). *Google Tech Talk on Wuala*. Retrieved from http://www.wuala.com/en/learn/techtalk. NB: Cited as transcribed by this author.

Gross, R. & A. Acquisti (2005). *Information Revelation and Privacy in Online Social Networks*. Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria, VA, USA. New York, NY: ACM.

L'Atelier BNP Paribas (2010). *Des réseaux sociaux plus confidentiels via une gestion distribuée?* Retrieved from http://www.atelier.fr/reseaux/10/09022010/reseaux-sociaux-gestion-distribuee-peer-to-peer-confidentialite-service-tiers-39347-.html

Hales, D. (2006). *Emergent Group-Level Selection in a Peer-to-Peer Network*. Complexus 2006 (3): 108-118.

Johnson, D. R., S. P. Crawford & J. G. Palfrey, Jr. (2004). *The Accountable Internet: Peer Production of Internet Governance*, Virginia Journal of Law and Technology, 9(9).

Kirkpatrick, M. (2010). *Why Facebook Is Wrong: Privacy Is Still Important*. ReadWriteWeb. Retrieved from http://www.readwriteweb.com/archives/why_facebook_is_wrong_about_privacy.php

Le Fessant, F. (2009). *Les réseaux sociaux au secours des réseaux « pair-à-pair ».* Défense nationale et sécurité collective, 3, 29-35.

Li, J. (last updated 2007). *A Survey of Peer-to-Peer Network Security Issues*. Retrieved from http://www.cse.wustl.edu/~jain/.

Massit-Folléa, F. (2008). *Gouverner l'Internet comme un bien commun mondial?* EuroDIG. Retrieved from http://www.voxinternet.org/spip.php?article251

McCarthy, C. (2010). Diaspora *about to hit $100,000 in donations*. CNET News. Retrieved from http://news.cnet.com/8301-13577_3-20004895-36.html.

Moglen, E. (2010). *Freedom In the Cloud: Software Freedom, Privacy, and Security for Web 2.0 and Cloud Computing*. Speech given at a meeting of the Internet Society (ISOC)'s New York branch, 5 February, 2010. Retrieved from http://www.softwarefreedom.org/events/2010/isoc-ny/FreedomInTheCloud-transcript.html.

Morbidelli, G., L. Pegoraro, A. Reposo & M. Volpi (2004). *Diritto Pubblico Comparato*. Torino: G. Giappichelli Editore.

Musiani, F. (2009). *The Internet Bill of Rights : A Way to Reconcile Natural Freedoms and Regulatory Needs?* SCRIPTed: A Journal of Law, Technology and Society, 6 (2), 504-515.

NoseRub Quick Facts (n.d.). Retrieved from http://noserub.com/quick-facts/

Pouwelse, J. A., P. Garbacki, J. Wang, A. Bakker, J. Yang, A. Iosup, D.H.J. Epema, M. Reinders, M. van Steen, H.J. Sips (2006). *Tribler: a Social-Based Peer-to-Peer System*. Concurrency and Computation: Practice & Experience 20 (2): 127-138.

Preibusch, S., B. Hoser, S. Guerses, & B. Berendt (2007). *Ubiquitous social networks – opportunities and challenges for privacy-aware user modeling*. Proceedings of the Data Mining for User Modelling Workshop, Corfu, June 2007. Retrieved from http://ideas.repec.org/p/diw/diwwpp/dp698.html.

Rodotà, S. (2006). *Una Costituzione per Internet*. La Repubblica. Retrieved from http://www.repubblica.it/2006/06/sezioni/scienza_e_tecnologia/regole-internet/regole-internet/regole-internet.html

Rozo-Acuna, E. (2002). Habeas Data *costituzionale: nuova garanzia giurisdizionale del diritto pubblico latinoamericano*. Diritto pubblico comparato ed europeo, 4, 1829-1872.

Schollmeier, R. (2001). *A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications*. IEEE International Conference on Peer-to-Peer Computing, 101-102.

Solove, D. (2006). *The Digital Person: Technology and Privacy in the Information Age*. New York, NY: NYU Press.

Star, S. L. (1999). *The Ethnography of Infrastructure.* American Behavioral Scientist, 43(3), 377-391.

Stern, A. (2007). *Interview with Wuala CEO/Founder Dominik Grolimund*. CenterNetworks. Retrieved from http://www.centernetworks.com/interview-wuala-founder-ceo-dominik-grolimund.

Suvanto, M. (2005). *Privacy in Peer-to-Peer Networks*. Helsinki University of Technology T-110.551 Seminar on Internetworking. Retrieved from www.tml.tkk.fi/Publications/C/18/suvanto.pdf.

The Appleseed Project, Docs (n.d.). Retrieved from http://appleseed.sourceforge.net/.

Diffie, W., & S. Landau (2007). *Privacy on the Line: The Politics of Wiretapping and Encryption, Updated and Expanded Edition*. Cambridge, MA: The MIT Press.

Wilhelm, A. (2010). *New Social Networking Darling Diaspora* Has An Idea Problem*. The Next Web Social Media. Retrieved from http://thenextweb.com/socialmedia/2010/05/13/diaspora-problems/.

Wood, J. A. (2010). *The Darknet: A Digital Copyright Revolution*. Richmond Journal of Law & Technology, XVI (14). Retrieved from http://jolt.richmond.edu/v16i4/article14.pdf.

Wuala Features (n.d.). Retrieved from http://www.wuala.com/fr/learn/features.

Wuala Frequently Answered Questions (n.d.). Retrieved from http://www.wuala.com/fr/support/faq/c/1#id000100.