Westminster Papers in Communication and Culture

Musiani, F. (2015). *Giants, Dwarfs* and Decentralized Alternatives to Internet-based Services: An Issue of Internet Governance. *Westminster Papers in Culture and Communication,* 10(1), 81–94, DOI: http://dx.doi.org/10.16997/wpcc.214

RESEARCH ARTICLE

Giants, Dwarfs and Decentralized Alternatives to Internet-based Services: An Issue of Internet Governance

Francesca Musiani[1]

[1] Researcher, Institute for Communication Sciences, French National Centre for Scientific Research (ISCC-CNRS), Associate researcher, Centre for the Sociology of Innovation of MINES ParisTech-PSL, France
francesca.musiani@gmail.com

This article discusses some of the results of a five-year-long (and ongoing) investigation of alternative approaches to the design of internet services, based on decentralized network architectures. In particular, the paper focuses on the implications of this research for the study and the practice of internet governance, inasmuch as architectural changes affect the repartition of responsibilities between service providers, content producers, users and network operators; contribute to the shaping of user rights, of the ways to produce and enforce law; reconfigure the boundary between public and private uses of the internet as a global facility. I argue that delving into the tensions between the *dwarfs* and the *giants* of the Net – between different technical and organizational architectures, and their *political* consequences – helps us to disengage from what is often a predominantly institutional view of internet governance, and give due emphasis to its less visible, infrastructure-embedded arrangements, its materiality and its practice.

Keywords: internet governance; decentralization; architecture; peer-to-peer; rights; law

1. Introduction[1]

The principle of decentralization has been one of the cornerstones of the internet's genesis: the primary objective of the 'network of networks' was indeed to enable communication between heterogeneous and remote machines, without mandatory transit points. Today, concentration models dominate, around a handful of macro-actors – *giants* equipped with extensive server farms, managing the most part of internet traffic. However, the original principle has not been entirely abandoned, and in all areas of application, developers explore decentralized alternatives, relying on cooperation between users (and their computers). These *dwarfs* of the network form the basis of search engines, social networks, storage platforms that allocate resources and tasks equally among participants in the network.

In this paper, I discuss some of the results of a five-year-long (and ongoing) investigation of alternative, decentralized and peer-to-peer approaches to internet services, and of the social and organizational forms they propose (Musiani, 2013a). To avoid adopting an excessively broad focus – and the impossible mission of summarizing years of work into a single paper – I will focus here, in particular, on discussing the implications of this research for the study of internet governance.[2] As Geoffrey Bowker points out, 'If the governance of the internet is a key sociotechnical issue of our times, then we need to be able to explore both the choices we have made and the roads not taken. If we are to deal with this fundamental political issue of our time, then we need an integrated understanding of what is at stake socially and how changes can be made technologically' (Bowker, 2013).

1.1. P2P, between widespread infractions and promise of equality

Peer-to-peer (P2P) is a technology that continues to cause both excitement and anxiety, despite its relatively simple technical definition of computer networking model structured in a decentralized manner, so that communications or exchanges take place between nodes entrusted with an equal responsibility in the system (Schollmeier, 2001). For a large number of internet users – since the encounter between P2P and the public, prompted by the file sharing software Napster in 1999 – this technology is a *de facto* synonym for the (illegal) download of cultural content; for others, it represents the ultimate utopia of techno-egalitarianism, or suggests a more sustainable organizational model for the societies of tomorrow. While it certainly does not, and cannot, wish to neglect the powerful agency of these normative views, my research does not seek to be a further contribution to the already well-established debate on copyright, and on the sharing/stealing dialectic to which P2P now seems to be almost 'naturally' associated. I have taken as the starting point of my work the basic feature of P2P as a computer network model: the facilitation of direct exchanges of data between equal nodes – equal in terms of their provision of technical resources to the system as a whole, and of the responsibility assigned to them within its operations.

My work of the past five years has focused on the development and the appropriation of internet-based services the conception of which integrates a specific design choice: the delegation of the responsibility and the control of data management and flows to the margins, or the periphery, of these networking systems. The necessary operations for the proper functioning of these systems, and their ability to correctly provide the services for which they are intended, technically depend on users, the 'dwarfs' of the network: their terminals, their computing resources, mobilized in an aggregate manner in order to serve a common purpose.

Thus, my work is not primarily concerned with the type of service that is most often associated with P2P architecture, file sharing. Rather, it focuses its attention on the 'meeting' between the choice of developing a P2P technical architecture, and applications such as information retrieval, video streaming, file storage. We are very familiar with these online activities in our daily practice as internet users, under the name of Google, YouTube, Dropbox – the 'giants' of information technology, based on a client/server network architecture that sets out a clearly identifiable dichotomy between a server that provides resources, and clients requesting them. My work explores the making of systems that, while serving these same, diverse purposes – search, networking, storage – have in common an original feature of their technical architecture, compared to their famous centralized counterparts: all are based on P2P networking technologies.

1.2. Approach and methodology

This work builds on an approach that blends internet studies with science and technology studies (STS) infrastructure studies – first and foremost – with a particular attention to methods that Star (1999) has described as 'ethnography of infrastructure'. This blend of qualitative methods has proven fruitful and has been formulated in order to shed light on the '*ballet* between programmers, software and users' (Abbate, 2012) that builds decentralization into internet-based services, and also to further explore the socio-political implications of this distributed and decentralized approach to the technical architecture of internet services. The underlying hypothesis for this method is that the 'lower layers' of a networked system have, or may have, consequences on the purpose that the system serves, the dynamics that are enacted within it, the techno-legal procedures it entails. Thus, it contributes to shape the present and future of internet governance, enacted not only via institutions but via the sinews of power embedded in the architectures and infrastructures of the internet (DeNardis, 2014). In the case of the present article, space constraints do not allow to present more than a very limited part of the ethnographic work which spans three chapters in (Musiani, 2013b); section 3, 3.1 in particular, will give a 'flavour' of this ethnography. This ensemble of methods, unpacking the discrete, oft-invisible operations and devices that subtend internet-based services, contributes to the disengagement from two equally 'reductionist' conceptions of the internet: either a *de facto* stranger to the institutional forces of the off-line 'reality', or a system that can be entirely assimilated to the codified spaces of traditional politics (Cheniti, 2009). Moving away from this dichotomy allows to give emphasis, in the study of internet governance, to its materiality and *practice*: the set of mechanisms that lead the different actors in the technical, political and economic management of the 'network of networks' to build common knowledge, legitimize some of it as stabilized *facts* of the internet, and shape boundaries able to reconcile the concerns of both experts and users.

Indeed, when it comes to the design and implementation choices subtending technical architectures, issues of materiality take central stage, intertwined with issues of 'code' (i.e. computers being 'programmed' in a specific way). The choice of decentralization, by developers and users alike, entails a number of very 'material' implications. Firstly, it is about the very *existence* of the system. In decentralized networks, there is no external supporting infrastructure; if domestic computers act as servers, server farms belonging to the 'giants' can be substantially reduced or don't need to exist, potentially, thus organizing the global infrastructure of the internet in a very different manner. Secondly, it has implications for what users' machines are equipped to do or not, the amount of control that users can exert on them, how they are appropriated by users; e.g., if domestic computers have P2P clients installed on them, they make specific uses of hardware such as Central Processing Units (CPUs) and hard disks, that are different in a classical, centralized 'cloud' configuration.

2. Network architecture, 'politics by other means'

'Study an information system and neglect its standards, wires, and settings, and you miss equally essential aspects of aesthetics, justice, and change,' once wrote STS scholar Susan Leigh Star (Star, 1999, 339). Indeed, the history of internet innovation suggests that the shaping of technical architectures populating the network of networks is, in the words of philosopher Bruno Latour, 'politics by other means' (Latour, 1988, 229). The ways in which architecture is politics, protocols are law, code shapes rights, are explored today by a number of different authors in relation to networked media (e.g. Lessig, 1999; DeNardis, 2009); in particular, internet-related research has contributed to foster the debate on the intersection and overlap of governance by architecture with other forms of governance. This section, while not pretending to be exhaustive, discusses some of the most interesting approaches to the question.

Information studies scholar and internet pioneer Philip Agre has addressed the relationship between technical architecture and institutions, notably the difference between 'architecture as politics' and 'architecture as a substitute for politics' (Agre, 2003). Defining architectures as the matrixes of concepts (e.g. the distinction between clients and servers) designed into technology, and institutions as the matrixes of concepts that organise language, rules, job titles, and other social categories in particular societal sectors, Agre suggests that the engineering story of rationally distributed computation and the political story of institutional change through decentralised architecture are not naturally related. They reconfigure and evolve constantly, and for these reconfigurations and evolutions to share a common direction, they need work: 'Decentralized institutions do not imply decentralized architectures, or vice versa. The drive toward decentralized architectures need not serve the political purpose of decentralizing society. Architectures and institutions inevitably coevolve, and to the extent they can be designed, they should be designed together.' (Agre, 2003, 42). Also interested in the relationship between architectures and the organization of society, Terje Rasmussen (2003) has argued that the technical model of the internet, and of the systems populating it, point towards central characteristics of modern societies. Thus, there is a structural match between the development of the internet and the transformation of the societies in which it operates. In this account, the technical infrastructure suggests a distributed society based on an ability to handle risk rather than central control.

Working at the crossroads of informatics, economics and law, Barbara van Schewick explores the relationship between the architecture of the internet (and its applications), with economics and competition structures. Her work seeks to examine how changes, notably design choices, in internet architecture affect the economic environment for innovation, and evaluates the impact of these changes from the perspective of public policy (2010, 2). According to van Schewick, this is a first step towards filling a gap in how scholarship understands innovators' decisions to innovate and the economic environment for innovation. After many years of research on innovation processes, we understand how these are affected by changes in laws, norms, and prices; yet, we lack a similar understanding of how architecture and innovation impact each other, perhaps for the intrinsic appeal of architectures as purely technical systems (Ibid, 2–3). Traditionally, she concludes, policymakers have used the law to bring about desired economic effects. Architecture *de facto* constitutes an alternative way of influencing economic systems, and as such, it is becoming another tool that actors can use to further their interests (Ibid, 389).

The relationship between the design of technical architecture for networked media and the making of law has been an increasingly central interdisciplinary preoccupation since the late 90s/early 2000s. Early uses of the metaphor 'code is law' can be found in William Mitchell's *City of Bits* (1995) and in Joel Reidenberg's article on *lex informatica*, the formation of information policy rules through technology (1998). However, legal scholars Yochai Benkler and Lawrence Lessig have arguably been the 'scene-setters' in this field, with their work on sharing as a paradigm of economic production in its own right (2004) and technical architecture as politics (1999), respectively. While the former argued for the rise of a 'networked information economy' as a system of 'production, distribution, and consumption of information goods characterized by decentralized individual action carried out through widely distributed, nonmarket means' (Benkler, 2006), the latter introduced technical architecture as one out of the four main (and interconnected) society regulators, the other three being law, market and norms. The application of this principle to the text of computer programs led to what remains, perhaps, the most famous incarnation of the famous 'code is law' label (Lessig, 1999).

Among the scholars that have since been inspired by this line of inquiry, Niva Elkin-Koren is especially interesting. In her work (e.g. 2006, 2012), architecture is understood as a dynamic parameter in the reciprocal influences of law and technology design, in the field of information and communication systems. The interrelationship between law and technology often focuses on one single aspect, the challenges that emerging technologies pose to the existing legal regime, thereby creating a need for further legal reform; however, the author argues, juridical measures involving technology both as a target of regulation and as a means of enforcement should take into account that the law does not merely respond to new technologies, but also shapes them and may affect their design (Elkin-Koren, 2006). Interestingly, the work of Tim Wu adds layers to the conceptualization of code's relationship with law, moving from Lessig's concept that computer code can substitute for law or other forms of regulation, to code as an anti-regulatory mechanism tool that certain groups will use to their advantage to minimize the costs of law – the possibility of 'using code design as an alternative mechanism of interest group behavior' (Wu, 2003).

2.1. Architecture and the future(s) of the internet

The current trajectories of innovation for the internet are making it increasingly evident by the day: the evolutions (and *in*-volutions) of the network of networks are likely to depend in the medium-to-long term on the topology and the organisational/technical model of internet-based applications, as well as on the infrastructure underlying them (Aigrain, 2011). This is illustrated by what has been this author's main research focus of the past few years: the development of internet-based services – search engines, storage platforms, video streaming applications – based on decentralised network architectures (Musiani, 2013b).

The concept of decentralisation is somehow shaped and inscribed into the very beginnings of the internet – notably in the organisation and circulation of data packets – but its current topology integrates this structuring principle only in very limited ways (Minar & Hedlund, 2001). The limits of the concentrated and centralised urbanism of the internet, which has been predominant since the beginning of its commercial era and its appropriation by the masses, are sometimes highlighted by the same phenomena that have contributed to its widespread success, such as social media (Schafer, Le Crosnier & Musiani, 2011). While internet users have become, at least potentially, not just consumers but also distributors, sharers and producers of digital content, the network of networks is structured in such a way that large quantities of data are centralised and compressed within specific regions of the internet. At the same time, such data are most suited to a rapid re-diffusion and re-sharing in multiple locations of a network that has now reached an unprecedented level of globalization. The current organisation of internet-based services and the structure of the network that enables their functioning – with its mandatory passage points, places of storage and trade, required intersections – raises many questions, in terms of the optimised utilisation of resources, the fluidity, rapidity and effectiveness of electronic exchanges, the security of exchanges, the stability of the network.

Beyond technology, these questions are deeply social and political, and affect the 'ramifications of possibles' (Gai, 2007) the internet is currently facing for its near-term future. They affect the balance of powers between users and service providers, and impact net neutrality. To what extent can network providers interfere with specific uses? Can the network be optimised for specific uses? By enabling individuals, communities and companies to use the internet in the way that creates the most value for them, changes in architecture are likely to increase or diminish the internet's overall value to society. Goals such as user choice, non-discrimination, non-optimisation, may be achieved in a variety of ways according to different designs of network architecture (van Schewick, 2010, 387). Resorting to decentralised architectures and distributed organisational forms, then, constitutes a different way to address some issues of management of the network, in a perspective of effectiveness, security and digital 'sustainable development' (better resource management), and of maximisation of its value to society.

Since the heyday of Napster, which marked the beginning of P2P's 'public' history, decentralized networks have mostly been considered, from a political and legal viewpoint, as a threat for the digital content industry. The most widespread use of such networks being the unauthorized sharing of music or video files, the problem of intellectual property rights has imposed itself as the predominant political and media framing of P2P networks and their uses. However, an equally relevant research question to ask is whether the diversity of P2P appropriations gives way to the construction of a social, political and economic *opportunity* for internet-based services, as well as an *alternative* to the predominant server-based concentration models.

Thus, the 'stories of P2P' that my recent research has been concerned with are representatives of a particular category of decentralized systems. Sladder is a British start-up offering a search engine decentralized at multiple levels of its technical architecture, aiming at making affinities and preferences of users a crucial component of query results. Drizzle is a Swiss start-up that once proposed a distributed file storage system, which also includes social networking features.[3] Delenk, a BitTorrent-based decentralized video streaming system funded by the European Union, is an occasion to observe the political and technical mobilization of P2P as an alternative model for audio-visual services via the internet.[4] All three projects wish to propose alternatives, based on decentralized or P2P architectures, to online services occupying an important place in the daily lives of internet users. The purposes of these systems are applications such as search, storage, streaming, the same that are provided by the 'big players' of the internet, such as Google, Dropbox, YouTube. They are designed to meet the same requirements as these services, from the perspective of the end user (who will continue to search for words, store photos, or watch a video), but are built on a different technical platform that leverages the potential of P2P and decentralization.

3. Architectures shaping user rights: a flavour of ethnography

Systems based on distributed, decentralized, P2P architectures seek their place today in an IT landscape that is mostly one of concentration and removal from users' machines. Sharing, regrouping and stocking information and data in the most popular, and widespread, internet services of today means promoting a model in which traffic is redirected towards an ensemble of machines, placed under the exclusive and direct control of the service provider. Thus, exchanges between users are made by 'copying' data that one wishes to share on one or more external terminals, or by giving these machines the permission to index this information. The ways in which data circulate, are stored and are written in these machines are, most of the times, opaque; moreover, the rights that the service provider acquires on such data are often excessive with respect to those maintained by the end user – in oft-unclear ways for users themselves.

When the operations of data treatment and handling are conducted, partially or totally, on users' terminals directly linked together, this choice of network architecture contributes to build specific definitions and implementations of privacy protection. It modifies the ways in which the control on informational data and the responsibility for their protection are spread out to the users, the service providers, the developers who have created the service. Distributed networking models challenge 'by architecture' the extent, the balance and the very definition of the rights obtained by service providers on users' personal data, vis-à-vis the rights that users maintain on such data. This often comes with a trade-off: on one hand, the user sees her privacy reinforced by the possibility of an augmented control on her data, and on the ways in which they are treated by the P2P client. However, simultaneously and for the same reasons, her responsibility for the actions she undertakes within and by means of the application is increased as well, while the provider surrenders voluntarily some of its control on the data and content present on the service. The collective dimension of this responsibility is also emphasized, and the collective consequences of individual infractions highlighted – regardless of whether the infraction is the storage of inappropriate content, the introduction of unreliable information or spam in a distributed search index, or a 'selfish' management of the bandwidth shared by a P2P streaming system.

Three cases of internet services based on a decentralized network architecture – a search engine, a storage platform and a video streaming software, studied between 2009 and 2011 – have shown how a definition of privacy 'by design', more specifically by architectural design, takes shape in internet services (Musiani, 2013b). With this alternative, 'techno-legal' way of defining privacy, a central role is attributed to the constraints and the opportunities of privacy protection that are inscribed into the technical model chosen by developers (Schaar, 2010).

Sladder, a P2P search engine developed first in Germany, then in the United Kingdom, displays a 'six-levels' distribution model, which must prevent the traceability of queries by a central entity. This model is intended to preserve personal data within the user's own terminal and the P2P client installed on it – unless they are encrypted beforehand, on that very terminal, before they leave it. This feature also allows the developers to work towards reducing the tension – which is a priori very difficult to eliminate – between the confidentiality of personal information and the personalization of search queries, the latter being the 'added value' that social dynamics add to the search engine, and which is based on the very collection of this personal information.

The case of Delenk, a P2P video streaming tool first developed at a Dutch technical university, offers another occasion to follow this tension, as the logic underlying the system is that the history of downloads made by a user are shared by default with other users so as to nourish the software's 'recommendation' algorithm. The solution envisaged by the developers has, once again, to do with an idea of 'privacy by architectural design', as it builds on the decentralized and distributed model to mitigate, in the eyes of users, the impression of exposure and revelation of themselves that the system's social features may provoke: not only can the feature be disabled, but it only sends the download history to other users – it doesn't keep the information on any server controlled by the service.

Finally, Drizzle, a (formerly) distributed storage platform developed in Switzerland, displayed similar attempts to protect user privacy by architecture. The heart of this service was the user's terminal, where, thanks to a dedicated P2P client, the operations of encryption and fragmentation of stored data took place. These two operations – conducted before any other operation leading to share, download or circulate data in the network – were meant, in the vision of Drizzle's developers, as evidence given to the users that the service provider, regardless of its intentions, did not even possess the technical means to break user trust in the system. The following section delves into this case study in some more detail.

3.1. Achieving privacy by design in decentralized storage

In early 2007, when Drizzle first sees the light, the industry of online data storage – a service allowing users to store, save and share data on one or several terminals connected to the internet – is in full development. Google, Amazon, Microsoft and Oracle, to name but a few, propose their storage platforms, each with its specificities and one common denominator: the 'cloud'. According to this model, the service provider is in charge of both the physical infrastructure and the software. Thus, the service provider hosts applications and data at once – in a location, and according to modalities, unknown to or at best ambiguous for the user (Mowbray, 2009). The so-called 'server farms' proliferate, to support and manage this increasing *remoteness* of data from users and users' terminals.

In this context, Drizzle, a small start-up founded by two developers and computer programmers who we will call Dietrich and Kurt, makes an unusual foundational decision: its cloud storage platform will mainly be composed – alongside more 'classical' data centres – of portions of the users' hard disks, directly linked in a peer-to-peer, decentralised network architecture (Schollmeier, 2001; Taylor & Harrison, 2009). This choice entails a number of peculiar features. On the one hand, the implementation of a technical process defined as 'encrypted fragmentation', which consists in encrypting locally – on the user's computer, and by means of a previously installed Drizzle P2P client – the content that will be stored. The content is then divided into fragments, duplicated to ensure redundancy, and spread out to the network. In return, users need to accept to 'pool' – put at the disposal of other users and their computers – the computational and material resources necessary for the operations related to the storage of content. As the service's terms of use point out: 'The user acknowledges that Drizzle may use processor, bandwidth and hard disk (or other storage media) of his computer for the purpose of storing, encrypting, caching and serving data that has been stored in Drizzle by the user or any other users. The user can specify the extent to which local resources are used in the settings of the Drizzle client software. The amount of resources the user is allowed to use in Drizzle depends on the amount of local resources the user is contributing to Drizzle.' The interdependent and egalitarian model subtending the platform will allow its users to barter their local disk space with an equivalent space in the decentralised cloud, thereby improving the quality of this storage space, which will become permanently available and accessible.

By shaping their decentralised storage service, the developers of Drizzle carry on a double experimentation: with the frontier between centralisation and decentralisation, and with sharing modalities that blend peer-to-peer, social networking and the cloud. Drizzle's first steps are taken in a community of research and development that tries to counter the social media 'explosion' by developing P2P systems as an alternative to a variety of internet-based services, including social networks, structured in a centralised manner (Le Fessant, 2009). In a context of user exposure on social networking sites and cloud-based services, and the increasingly widespread storage of applications and data in locations and ways unknown or at best ambiguous, several developers – including Drizzle's – identify in a peer-to-peer type of network architecture a possible way of approaching the protection of personal data privacy with a different angle: through the relocation and 're-appropriation' of data within the terminals of users, who would be able to host their own profiles and the information they contain (see also Moglen, 2010; Aigrain, 2010, 2011).

As in the development of Drizzle, a conception of privacy and confidentiality of personal data, which is conceived of and enforced via technical means – called *privacy by design* (Cavoukian, 2010; Schaar, 2010), is at work. This conceptualisation of privacy is defined by means of the constraints and the opportunities linked to the treatment and the location of data, according to the different moments and the variety of operations taking place within the system. In particular, the confidentiality of data (personal data as well as the content stored in the P2P cloud) is defined by the peculiar role and enhanced features attributed to the password that identifies the user *vis-à-vis* the network.

In Dietrich's intentions, the role of the user-selected and user–generated password for the Drizzle system should have 'stri[cken] the user as soon as he had access to the system for the very first time.' Indeed, the virtual form that is served to users upon subscription may come as a surprise: it informs that 'We do not know your password as it never leaves your computer. Please, do not forget your password and use, if needed, your password hint.' The status of the password is thus negotiated, beyond its usual meaning of unique identifier *vis-à-vis* the system, to define, detail and legitimise the process of local encryption and decryption of data within the Drizzle system. This feature comes to symbolise the specificity of Drizzle's promise of security and privacy as well as users' trust, as it becomes the symbol and the graphical representation of the 'local' dimension of the encryption process – as it never leaves the computer of the user who created it. The operations, for the most part automatically managed, that are linked to the protection of personal data are thus hosted on the terminals of users. Indeed, this entails a modification of the user's role within the service's architecture: node among equal nodes, it becomes a server itself, instead of a starting point and a final point for operations that are otherwise conducted on another machine or group of machines.

Through the attribution of this status to the password, the developers of Drizzle are also proposing an alternative to the balance between the rights exerted by users on their own data and the rights acquired by the service provider on these same data – a balance that is usually heavily bent on the provider's side. However, this reconfiguration in the balance of rights comes with a trade-off. As the password stays with the user and is not sent to the servers controlled by the firm, the latter cannot retrieve the password if needed. Thus, users do not only see their privacy reinforced, but at the same time and for the same reasons, the responsibility for their actions is augmented – while the service provider renounces some of its control over the content that circulates thanks to the service it manages. The meaning of this 'renunciation', Dietrich explains, is double: on the one hand, the Drizzle team wishes to make it evident, almost *translate* into a specific object the user can easily relate to, the 'obscure' and unfamiliar process of client-side encryption, which is an ongoing source of controversies and perplexities. On the other hand, it is also a matter of Drizzle's business model: the more the firm knows about its users, the more it is mandatory for it to submit the users to regular surveillance and control – and this requires an investment of material resources and time that, in its first phases of existence, the firm does not have: 'If we can know what is in your account, starting with your password, we have heightened obligations to police the content and to make sure nobody can eavesdrop on the traffic.'

The development of Drizzle's 'peer-to-peer cloud' allows to observe how changes in the architectural design of networked services affect data circulation, storage and privacy – and in doing so, reconfigure the articulation of the 'locality' and the 'centrality' in the network (Akrich, 1989: 39), suggesting a model of decentralised governance 'by architectural design' for the service. Ultimately, decentralising the cloud leads to a reformulation and 're-balancing' of the relationship between the user and the service provider. The local, client-side encryption of data first, and its fragmentation afterwards – both operations conducted within the P2P client installed by the user, and entirely taking place on his terminal – are proposed by Drizzle as evidence that the firm, in its own words, 'does not even have the technical means' to betray the trust of users. In particular, this conception of *privacy by design* takes shape around the password, which remains locally stored in the user's P2P client and unknown to the service provider. In doing so, it becomes a form of disengagement of the service provider with respect to security issues, its 'auto-release' from responsibility: a detail whose importance may seem small at first, but eventually leads to changes in the forms of technical solidarity (Dodier, 1995) established between users and service provider.

4. How (de-) centralized architectures matter for internet governance

The critiques targeting the interdisciplinary, emerging research field of internet governance – from the difficulty of establishing precise definitions, to the alleged 'unholy marriages' with its subject of study – do not jeopardize the validity and the interest of a field that is not only 'in the making', but interested in an especially dynamic object

(Brousseau & Marzouki, 2012). However, it needs to be acknowledged, as Michel van Eeten and Milton Mueller do, that the literature describing itself as specialized in the internet governance field often tends to focus on a limited number of international institutions and debates about the global politics of the internet. The 'internet governance' qualification does not generally apply to the study of a number of activities and daily practices, on and with the internet, that play a very important role in the shaping and the regulation of the 'network of networks' (van Eeten & Mueller, 2013).

Paying close attention to the tensions between the dwarfs and the giants of the Net – the tensions between technical and organizational models, and their 'political' consequences – can contribute, as Tarek Cheniti has pointed out, to a disengagement from an all-too-frequent dualist conception of the internet as an *a priori* identifiable and rigidly bounded space: either a stranger to the institutional forces of the off-line 'reality', or on the contrary, entirely entrenched behind the codified spaces of traditional politics (Cheniti, 2009). This perspective allows to give emphasis in the analysis to the set of mechanisms that lead different participants in the technical, political and economic management of the 'network of networks' to build common knowledge, legitimize some of it as facts of the internet, and shape limits and boundaries able to reconcile the concerns of both experts and users. It helps identifying and presenting different versions of the worlds in which notions of governance take place, before defining what governance actually is (Ziewitz and Pentzold, 2013).

Arrangements of technical architecture have always inherently been arrangements of power, writes Laura DeNardis (2014): the technical architecture of networked systems does not only affect internet governance, but *is* internet governance. This governance by architecture, or 'governance by design' (De Filippi, Dulong de Rosnay & Musiani, 2013), has important implications at a number of levels, of which the previous section, centred on privacy and the ways in which it can be implemented by architectural design, has given but one example.

Changes in architectural design affect the repartition of competences and responsibilities between service providers, content producers, users and network operators. They affect forms of engagement and *intéressement* (Callon, 2006) in networked systems, of users first and foremost, but also of other actors concerned by the implementation and the operations of internet services. They shape the sustainability of the underlying economic models and the technical and legal approaches to the management of digital content and personal data. They make visible, in various configurations, the forms of interaction between the local and the global, the patterns of articulation between the individual and the collective.

Changes in network architectures contribute to the shaping of user rights, of the ways to produce and enforce law, and are reconfigured in return. A number of legal issues, that go way beyond copyright (despite having often been reduced to this aspect, notably in the case of peer-to-peer systems), are raised by architectural configurations of internet services. To preserve the internet's 'social value' (van Schewick, 2010), it is important to achieve reliable forms of regulation – technical, political, or both – without impeding present and future innovation.

Changes in architectures do, finally, contribute to shift the boundary between public and private uses of the internet as a global facility: they are a crucial factor in defining intellectual property rights, the right to privacy of users/clients, or their rights of access to content. They contribute to define what is a contributor in internet-based services, in terms of computing resources required for operating the system, and of content.

In the end, technical architecture appears as one of the strongest, if not the strongest, structuring element of internet governance: what is shaped into architecture and infrastructure can seldom be undone by institutional negotiation and dialogue alone, and institutions find it increasingly complicated to keep up with 'creative' governance by architecture and by infrastructure (see DeNardis, 2012). In this sense, future evolutions of internet governance as a field would do well to fully take into account Michel van Eeten and Milton Mueller's suggestion to expand to areas such as the economics of cybercrime and cybersecurity, network neutrality, content filtering and regulation, infrastructure-based copyright enforcement, and interconnection arrangements among ISPs (van Eeten & Mueller, 2013).

Information and communication technologies, the internet first and foremost, are increasingly mobilized to serve broader economic, political and military aims, ranging from the theft of strategic data to the hijacking of industrial systems. The rise of techniques, devices and infrastructures destined to facilitate digital espionage, data collection and aggregation, tracking and surveillance is highlighted not only by the recent Snowden revelations, but also by the construction and the organization of a dedicated, increasingly widespread and lucrative market. What lies under the internet governance label is, in fact, an ensemble of fluidly-contoured socio-political and socio-technical controversies, which have in STS-informed approaches to network architecture – its centralization and decentralization – one of the best opportunities to be thoroughly accounted for, richly described and extensively analysed.

5. Conclusions

If it is possible to design in detail the architecture of the world users interact with, it is possible to design the architecture of our global communication infrastructure in order to promote specific types of political, economic and legal interactions over others (De Filippi et al., 2013) with important consequences for the ways in which the future internet will be governed, and for the extent to which its users will be not only customers, but citizens.

Technical architectures, as argued by several authors discussed in this article, may be understood as alternative ways of influencing economic systems, sets of rules, communities of practice – indeed, as the very fabric of user behaviour and interaction. They are very 'material' devices of governance, as well, embedded in the reconfigurations of traffic flows, redistribution of computing power, rearrangements of storage space, downloads of P2P clients, availability and performance of hard disks. The status of every internet user as consumer, sharer, producer and possibly manager of digital content is informed by, and shapes in return, the technical structure and organisation of the services she has access to.

It is in this sense that network architecture is internet governance: changes in the design of the networks subtending internet-based services, and the global internet itself, affect the 'politics by other means' (Latour, 1988: 229) of the *network of networks* – the balance of rights between users and providers, the capacity of online communities to engage in open and direct interaction, the fair competition between actors within the internet market.

Competing Interests

The author declares that they have no competing interests.

Notes

[1] This work is supported by the French National Agency for Research (ANR) within the frame of the programme *ADAM – Architecture distribuée et applications multimédias*. An earlier draft of this paper was presented at the Eighth Symposium of the Global Internet Governance Academic Network (GigaNet) in Bali, Indonesia, October 2013.

[2] Internet governance today is a lively, emerging field, and its definition relentlessly contested by different groups across political and ideological lines. A 'working definition' of IG has been provided in the past, after the United Nations-initiated World Summit on the Information Society (WSIS), by the Working Group on Internet Governance – a definition that has reached wide consensus because of its inclusiveness, but is perhaps too broad to

be useful for drawing more precisely the boundaries of the field (Malcolm, 2008): 'Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the internet' (WGIG, 2005). This broad definition implies the involvement of a plurality of actors, and the possibility for them to deploy a plurality of governance mechanisms. IG has been described as a mix of technical coordination, standards, and policies (e.g. Malcolm, 2008 and Mueller, 2010). See also (DeNardis, 2013) and (Musiani, 2013a).

[3] The decentralized mechanism subtending the Drizzle system, a trade between local storage space and space in a 'P2P storage cloud' spread out to the users, was discontinued in September 2011.

[4] The names used in the case studies are fictitious.

References

Abbate, J. (2012). L'histoire de l'internet au prisme des STS. *Le temps des médias*, *18*: 170–180. DOI: http://dx.doi.org/10.3917/tdm.018.0170

Agre, P. (2003). Peer-to-Peer and the promise of internet equality. *Communications of the ACM*, *46*(2): 39–42. DOI: http://dx.doi.org/10.1145/606272.606298

Aigrain, P. (2010). Declouding freedom: reclaiming servers, services and data. In 2020 FLOSS Roadmap (2010 Version/3rd Edition), available at https://flossroadmap.co-ment.com/text/NUFVxf6wwK2/view/ (accessed 13 June 2014).

Aigrain, P. (2011). *Another Narrative,* Addressing Research Challenges and Other Open Issues session, PARADISO Conference, Brussels, 7–9 Sept. 2011.

Akrich, M. (1989). De la position relative des localités: systèmes électriques et réseaux sociopolitiques. *Cahiers du Centre d'Études pour l'Emploi*, *32*: 117–166.

Benkler, Y. (2004). Sharing nicely: on shareable goods and the emergence of sharing as a modality of economic production. *The Yale Law Journal*, *114*(2), 273–358. DOI: http://dx.doi.org/10.2307/4135731

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom.* New Haven, CT: Yale University Press.

Bowker, G. C. (2013). Preface, in Musiani, F. *Nains sans géants. Architecture décentralisée et services internet*, Paris: Presses des Mines, pp. 7–8.

Brousseau, E., Marzouki, M., & **Méadel, C.** (Eds.), (2012). *Governance, Regulations and Powers on the Internet*, Cambridge: Cambridge University Press.

Callon, M. (2006). Sociologie de l'acteur-réseau. In M. Akrich, M. Callon & B. Latour (Eds.), *Sociologie de la traduction: textes fondateurs.* Paris: Presses des Mines, pp. 267–276.

Cavoukian, A. (Eds.), (2010). Special issue: Privacy by design: The next generation in the evolution of privacy, *Identity in the Information Society*, *3*(2).

Cheniti, T. (2009). *Global Internet Governance in Practice: Mundane Encounters and Multiple Enactments.* Unpublished DPhil Thesis, University of Oxford.

De Filippi, P., Dulong de Rosnay, M., & **Musiani, F.** (2013). *Peer Production Online Communities, Distributed Architectures and Governance by Design.* Communication presented at the Fourth Transforming Audiences Conference, September 3, 2013, University of Westminster, London. PMCid: PMC4089856.

DeNardis, L. (2009). *Protocol Politics: the Globalization of Internet Governance*. Cambridge, MA: the MIT Press. DOI: http://dx.doi.org/10.7551/mitpress/9780262042574.001.0001

DeNardis, L. (2012). The turn to infrastructure for internet governance, *Concurring Opinions*, 2012, available at http://www.concurringopinions.com/archives/2012/04/the-turn-to-infrastructure-for-internet-governance.html (accessed 13 June 2014).

DeNardis, L. (2013). The Emerging Field of Internet Governance. In W. Dutton (Ed.), *Oxford Handbook of Internet Studies*. Oxford: Oxford University Press. DOI: http://dx.doi.org/10.1093/oxfordhb/9780199589074.013.0026

DeNardis, L. (2014). *The Global War for Internet Governance*. New Haven and London: Yale University Press. DOI: http://dx.doi.org/10.12987/yale/9780300181357.001.0001

Dodier, N. (1995). *Les Hommes et les Machines. La conscience collective dans les sociétés technicisées*. Paris: Métailié.

Elkin-Koren, N. (2006). Making technology visible: liability of internet service providers for peer-to-peer traffic. *New York University Journal of Legislation & Public Policy*, *9*(15), 15–76.

Elkin-Koren, N. (2012). Governing access to user-generated content: the changing nature of private odering in digital networks. In E. Brousseau, M. Marzouki & C. Méadel (Eds.), *Governance, Regulations and Powers on the Internet*, Cambridge: Cambridge University Press. DOI: http://dx.doi.org/10.1017/CBO9781139004145.020

Gai, A.-T. (2007). Web 3.0: une autre branche pour l'arbre des possibles. *Transnets*, available at http://pisani.blog.lemonde.fr/2007/02/17/web-30-une-autre-branche-pour-larbre-des-possibles/ (accessed 13 June 2014).

Latour, B. (1988). *The Pasteurization of France*, Cambridge, MA: Harvard University Press. PMCid: PMC338299.

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

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.

Malcolm, J. (2008). *Multi-Stakeholder Governance and the Internet Governance Forum*. Wembley, WA: Terminus Press.

Minar, N. & **Hedlund, M.** (2001). A network of peers – peer-to-peer models through the history of the internet. In A. Oram (Ed.), *Peer-to-peer: Harnessing the Power of Disruptive Technologie*s, 9–20. Sebastopol, CA: O'Reilly.

Mitchell, W. J. (1995). *City of Bits. Space, Place and the Infobahn*, Cambridge, MA: the MIT Press.

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.

Mowbray, M. (2009). The Fog over the Grimpen Mire: Cloud Computing and the Law, *SCRIPTed*, *6*(1): 132–146. DOI: http://dx.doi.org/10.2966/scrip.060109.132

Mueller, M. (2010). *Networks and States: The Global Politics of Internet Governance*, Cambridge, MA: the MIT Press.

Musiani, F. (2013a). *A Decentralized Domain Name System? User-Controlled Infrastructure as Alternative internet Governance*, presented at the Eighth Media In Transition (MiT8) conference, 3–5 May, 2013, Massachusetts Institute of Technology, Cambridge, MA, available as draft at http://web.mit.edu/comm-forum/mit8/papers/Musiani_DecentralizedDNS_MiT8Paper.pdf (accessed 13 June 2014).

Musiani, F. (2013b). *Nains sans géants: architecture décentralisée et services internet*. Paris, Presses des Mines.

Rasmussen, T. (2003). On distributed society: the history of the internet as a guide to a sociological understanding of communication and society. In G. Liestøl, A. Morrison & T. Rasmussen (Ed.), *Digital Media Revisited: Theoretical and Conceptual Innovation in Digital Domains*, Cambridge, MA: MIT Press.

Reidenberg, J. R. (1998). Lex informatica: the formulation of internet policy rules through technology. *Texas Law Review*, *76*(3).

Schaar, P. (2010). Privacy by Design, *Identity in the Information Society*, *3*(2): 267–274. DOI: http://dx.doi.org/10.1007/s12394-010-0055-x

Schafer, V., Le Crosnier, H. & **Musiani, F.** (2011). *La neutralité de l'internet, un enjeu de communication*. Paris: CNRS Editions/Les Essentiels d'Hermès.

Schollmeier, R. (2001). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. *Proceedings of the First International Conference on Peer-to-Peer Computing*, 27–29. DOI: http://dx.doi.org/10.1109/p2p.2001.990434

Star, S. L. (1999). The ethnography of infrastructure. *American Behavioral Scientist*, *43*(3): 377–391. DOI: http://dx.doi.org/10.1177/00027649921955326

Taylor, I. & **Harrison, A.** (2009). *From P2P to Web Services and Grids: Evolving Distributed Communities. Second and Expanded Edition.* London: Springer-Verlag.

van Eeten, M., & **Mueller, M.** (2013). Where is the governance in internet governance? *New Media & Society*, *15*(5): 720–736. DOI: http://dx.doi.org/10.1177/1461444812462850

van Schewick, B. (2010). *Internet Architecture and Innovation*. Cambridge, MA: the MIT Press.

Working Group on Internet Governance. (2005). *Report of the Working Group on internet Governance*, Château de Bossey, June 2005, available at http://www.wgig.org/docs/WGIGREPORT.pdf (accessed 13 June 2014)

Wu, T. (2003). When code isn't law, *Virginia Law Review*: 89. DOI: http://dx.doi.org/10.2307/3202374

Ziewitz, M., & **Pentzold, C.** (2013). In search of internet governance: performing order in digitally networked environments, *New Media & Society*, online pre-publication.

How to cite this article: Musiani, F. (2015). *Giants, Dwarfs* and Decentralized Alternatives to Internet-based Services: An Issue of Internet Governance. *Westminster Papers in Culture and Communication,* 10(1), 81–94, DOI: http://dx.doi.org/10.16997/wpcc.214

Published: 15 September 2015

]u[*Westminster Papers in Culture and Communication* is a peer-reviewed open access journal published by University of Westminster Press

OPEN ACCESS