INTERNET POLICY REVIEW
Journal on internet regulation

Volume 2 | Issue 4

Network architecture as internet governance

Francesca Musiani
MINES ParisTech, France, francesca.musiani@mines-paristech.fr

Published on 24 Oct 2013 | DOI: 10.14763/2013.4.208

Abstract: The architecture of a networked system is its underlying technical and logical structure, including transmission equipment, communication protocols, infrastructure, and connectivity between its components or nodes. This article introduces the idea of network architecture as internet governance, and more specifically, it outlines the dialectic between centralised and distributed architectures, institutions and practices, and how they mutually affect each other. The article argues that network architecture is internet governance in the sense that, by changing the design of the networks subtending internet-based services and the global internet itself, its politics are affected – 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 of the internet market.

Keywords: Internet architecture, Internet governance, Decentralisation

Article information

Received: 07 Aug 2013 **Reviewed:** 26 Sep 2013 **Published:** 24 Oct 2013

Funding: This work is supported by the ANR project ADAM - Architectures distribuées et applications multimédia and by the FP7 STREP project P2Pvalue - Techno-social platform for sustainable models and value generation in commons-based peer production in the Future Internet
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/network-architecture-internet-governance

Citation: Musiani, F. (2013). Network architecture as internet governance. *Internet Policy Review*, *2*(4). DOI: 10.14763/2013.4.208

The architecture of a networked system is its underlying technical structure, designed according to a "matrix of concepts" (Agre, 2003). It constitutes the logical and structural layout of a system, including transmission equipment, communication protocols, infrastructure, and connectivity between its components or nodes. This article introduces the idea of network architecture as internet governance[1], and more specifically, it outlines the dialectic between centralised and distributed architectures, institutions and practices, and how they mutually affect each other.

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. 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: by changing the design of the networks subtending internet-based services, and the global internet itself, the politics of the *network of networks* are affected – 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 of the internet market.

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 science and technology studies (STS) scholar Susan Leigh Star (Star, 1999, p. 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, p. 229). The ways in which architecture is politics, protocols are law, code shapes rights (e.g., Lessig, 1999; DeNardis, 2009), are explored today by a number of different authors in relation to networked and online media; 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 key approaches to the question.

Interested in the relationship between architectures and the organisation of society, Terje Rasmussen (2003) has argued that there is a structural match between the development of the technical model of the internet (such as packet switching and distributed routing) and the transformation of the societies in which it operates. In this account, the technical infrastructure of the Internet suggests that ours is a distributed society, based on the ability to handle risk, rather than on central control. On the other hand, information studies scholar and internet pioneer Philip Agre suggests that "Decentralized institutions do not imply decentralized architectures, or vice versa. [...] Architectures and institutions inevitably coevolve, and to the extent they can be designed, they should be designed together" (Agre, 2003, p. 42), but they are not "naturally" related.

IT law scholar Barbara van Schewick 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, p. 2). According to her, this is a first step towards filling a gap in how scholarship understands innovators' decisions 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.*, p. 2-3). Traditionally, she concludes, policy makers 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.*, p. 389).

The relationship between architecture and law-making for networked media has been an increasingly central interdisciplinary preoccupation since the late 1990s/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 programmes led to what remains, perhaps, the most striking 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 relevant. 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).

The work of Tim Wu adds layers to the conceptualisation 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 minimise the costs of law – the possibility of "using code design as an alternative mechanism of interest group behavior" (Wu, 2003).

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 over 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 has contributed to its widespread success, as best illustrated by social media (Schafer, Le Crosnier & Musiani, 2011). Examples of incidents caused by "excessive concentration" are, for example, the global consequences of the Pakistani YouTube re-routing in 2008 or the repeated failures of Twitter infrastructure (e.g., in 2012). These incidents have put into the spotlight some of the possible limits of the concentration model: excessive control, technical and/or legal, by a single commercial entity; the opaqueness

of the modalities of this control vis-à-vis the users; the vulnerability to single-point failures of centralised architectures.

While internet users have become, at least potentially, not only 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 large data centers and server farms. At the same time, such data is most suited to a rapid re-diffusion and re-sharing in multiple locations of a network that has now reached an unprecedented level of globalisation. The current organisation of internet-based services and the structure of the network that enables their delivery – 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 close future. Resorting to decentralised architectures and distributed organisational forms, constitutes a different way to address some issues of management of the network, in a perspective of effectiveness, answer to vulnerabilities, digital "sustainable development" (better resource management), and of maximisation of the Internet's value for society.

ARCHITECTURES SHAPING USER RIGHTS: DECENTRALISATION AND *PRIVACY BY DESIGN*

Systems based on distributed, decentralised, peer-to-peer (P2P) architectures seek their place today in an IT landscape that is mostly one of concentration and removal from users' machines. From the viewpoint of informational data, personal data and exchanged content, this implies that sharing, regrouping and stocking those data in the most popular, and widespread internet services of today means promoting a model in which traffic is re-directed 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 external machines the permission to index this information. The ways in which data circulates, is stored and written in these machines is often uncertain; moreover, the rights that the service provider acquires on such data are often excessive with respect to those maintained by the end user – in such a way that is often opaque for users themselves[2].

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 building specific definitions of privacy protection. It modifies the ways in which the control on informational data, and the responsibility of their protection, are spread out to the users, the service providers and the developers who have created the service.

Three cases of internet services based on a decentralised 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).

Faroo, a P2P search engine developed first in Germany, then in the United Kingdom, displays a "six-levels" distribution model that must prevent the traceability of queries by a central entity; this model is supposed to preserve personal data within the user's own terminal and the P2P client installed on it – unless they are encrypted on that very terminal before leaving 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 personalisation 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 Tribler, a P2P video streaming tool first developed at the Technical University of Delft (The Netherlands), is 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 decentralised 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, Wuala[3], a (formerly) distributed storage platform developed in Switzerland, displayed similar attempts to protect user privacy via 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 could take place. These two operations, conducted before any other (e.g., sharing, downloading or circulating data in the network), were meant, in the vision of Wuala'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.

While developers, across all three case studies, consider that a more articulate protection of privacy is one of the core comparative advantages of their systems (and they "sell" it as such), users wonder, in turn, about the implications of a decentralised architecture for the protection of their data. What does the fact of making available to the whole P2P network a part of one's own computing resources imply, for the "invisible" data collected there? In the cases of Faroo and Wuala – where the P2P model merges, in a peculiar way, with a proprietary software logic, this question is the occasion to make explicit the difficult articulation between the decentralising philosophy subtending the systems, and a closed source code. Pioneer users – for the most part, users-innovators or users-developers themselves – see the closed code as a lack of transparency, even a lack of respect, that prevents them from delving into this aspect with the tools they have available. It is good to have privacy by architecture, these users point out, but we need to have a direct knowledge of this technique on a case-by-case basis, to, eventually, allow for direct modifications of the architecture.

Decentralised 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. With a trade-off: on the one hand, the user sees her privacy reinforced by the possibility of an augmented control on her data, and its handling 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 proportionately, as the provider surrenders voluntarily some of his control over the data and content present on the service. The collective dimension of this responsibility is also emphasised, inasmuch as the infraction to the collective behaviour has not only individual but collective consequences- be it 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.

CONCLUSIONS: HOW ARCHITECTURE MATTERS

"Arrangements of technical architecture have always inherently been arrangements of power," writes STS scholar Laura DeNardis (2012): 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 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 operation of internet services. They shape the sustainability of the underlying economic models and the technical and legal approaches to 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," it is important to achieve reliable forms of regulation – technical, political, or both – without impeding present and future innovation.

Changes in architecture 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[4]. In this sense, future evolutions of internet governance as a field would do well to take into account Michel van Eeten and Milton Mueller's suggestion to expand and include innovative areas such as the economics of cybercrime and cyber security, network neutrality, content filtering and regulation, copyright enforcement, and interconnection arrangements among ISPs (van Eeten & Mueller, 2013).

In the digital world, it is possible to design in detail the architecture of the world users interact with – and as a consequence, it is possible to design the architecture of our global communication infrastructure in order to promote specific types of 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.

FOOTNOTES

1. Internet governance (IG) 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).

2. See this discussion of the terms of use of several social sites, among which Facebook and Instagram: http://www.nyccounsel.com/business-blogs-websites/who-owns-photos-and-videos-posted-on-facebook-or-twitter/

3. The decentralised mechanism subtending the Wuala 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. An example is the Domain Name System and its co-optations. See (DeNardis, 2012) and (Musiani, 2013).

REFERENCES

Agre, P. (2003). Peer-to-Peer and the Promise of Internet Equality. *Communications of the ACM*, 46 (2): 39-42.

Aigrain, P. (2010). Declouding Freedom: Reclaiming Servers, Services and Data. In 2020 FLOSS Roadmap (2010 Version/3rd Edition). Retrieved from https://flossroadmap.co-ment.com/text/NUFVxf6wwK2/view/

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

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.

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

De Filippi, P., M. Dulong de Rosnay & F. Musiani (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.

DeNardis, L. (2013). The Emerging Field of Internet Governance, in W. Dutton (ed.) *Oxford Handbook of Internet Studies*. Oxford: Oxford University Press.

DeNardis, L. (2012). The Turn to Infrastructure for Internet Governance. *Concurring Opinions*. Retrieved 26 Oct 2013, from http://www.concurringopinions.com/archives/2012/04/the-turn-to-infrastructure-for-internet-governance.html

DeNardis, L. (2009). *Protocol politics* (1st ed.). Cambridge, MA: MIT Press.

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 Ordering in Digital Networks. In Brousseau, E., Marzouki, M., Méadel, C. (eds.), *Governance, Regulations and Powers on the Internet*, Cambridge: Cambridge University Press.

Gai, A.-T. (2007). Web 3.0: une autre branche pour l'arbre des possibles. *Le Monde*. Retrieved 26 Oct 2013, from http://pisani.blog.lemonde.fr/2007/02/17/web-30-une-autre-branche-pour-larbre-des-possibles/

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

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*

Technologies, 9-20. Sebastopol, CA: O'Reilly.

Mitchell, W. J. (1996). *City of Bits. Space, Place and the Infobahn*. Cambridge, MA: The MIT Press.

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 8th Media In Transition (MiT8) conference, May 3-5, 2013, Massachusetts Institute of Technology, Cambridge, MA. Available as draft at http://web.mit.edu/comm-forum/mit8/papers/Musiani_DecentralizedDNS_MiT8Paper.pdf

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: The MIT Press.

Reidenberg, J. R. (1998). Lex Informatica: The Formulation of Internet Policy Rules Through Technology. *Texas Law Review*, 76 (3).

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

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

van Eeten, M. & M. Mueller (2009). Where Is the Governance in Internet Governance? *New Media & Society*, 15 (5): 720-736.

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, http://www.wgig.org/docs/WGIGREPORT.pdf

Wu, T. (2003). When Code Isn't Law. Virginia Law Review, 89.