INTERNET POLICY REVIEW
Journal on internet regulation

Volume 2 | Issue 4

# Flawed cloud architectures and the rise of decentral alternatives

**Primavera De Filippi**
*Research and Studies Center of Administrative Science (CERSA/CNRS), Université Paris II (Panthéon-Assas), France*

Published on 01 Nov 2013 | DOI: 10.14763/2013.4.212

**Abstract:** The high degree of centralisation that characterises many cloud-based services raises a series of challenges in terms of (a) security, due to there being only a few points of failure or attack, (b) privacy, due to the users' lack of control over the collection and use of personal data, and (c) user autonomy, given that users increasingly depend on third parties services and infrastructures. After analysing the drawbacks of traditional cloud computing platforms, this article provides an overview of how civil society is progressively challenging the centralised cloud establishment by providing decentralised alternatives to cloud computing which could potentially help overcome these drawbacks.

**Keywords:** Cloud computing, IT system architecture, Informational self-determination, Decentralisation, Infrastructure as a Service (IaaS), Autonomy, Centralisation, Privacy

## Article information

**Received:** 24 Sep 2013 **Reviewed:** 18 Oct 2013 **Published:** 01 Nov 2013

**Competing interests:** The author has declared that no competing interests exist that have influenced the text.

**URL:**
http://policyreview.info/articles/analysis/flawed-cloud-architectures-and-rise-decentral-alternatives

**Citation:** De Filippi, P. (2013). Flawed cloud architectures and the rise of decentral alternatives. *Internet Policy Review*, *2*(4). https://doi.org/10.14763/2013.4.212

Cloud computing has radically modified the way in which users interact with online data. Increasingly, content or information is no longer stored locally into users' devices, but is rather exported into online data-centres, where it can be subsequently retrieved by users, on-demand, regardless of the device they use. This offers a significant number of advantages to end-users, mostly related to elasticity, scalability, and ubiquitous availability of content or data. Indeed, people need no longer invest in their own hardware infrastructure and/or software architecture, since they can now benefit from a dynamic provision of computing resources, which automatically increase or decrease according to actual needs. Besides, given that the data is stored in the cloud – as opposed to locally being stored on users' devices – it becomes readily available and accessible from anywhere and at any time (provided fast internet connection). Files can be temporarily cached and/or simultaneously accessed from multiple devices, without

the need of installing any specific software, and without having to worry about transferring files or syncing them.

Yet, the high degree of centralisation that characterises many cloud-based services raises a series of challenges in terms of (a) security, due to there being only a few points of failure or attack, (b) privacy, due to the users' lack of control over the collection and use of personal data, and (c) user autonomy, given that users increasingly depend on third parties services and infrastructures.

After having analysed the drawbacks of traditional cloud computing platforms, this article will provide an overview of how civil society is progressively challenging the centralised cloud establishment by providing decentralised alternatives to cloud computing which could potentially help overcome these drawbacks.

## DEPENDENCY CONCERNS

While technological advances in information and communication technologies (ICT) are often regarded as an opportunity for social and individual empowerment (Loader & al., 2000; Becker, 2001; Garrett, 2006), there has been – ever since the massive rise in popularity of the personal computer – an inherent tension between the benefits of technology in terms of user's empowerment (Carlson, 2003) on the one hand, and the costs it entails in terms of increased surveillance and control on the other hand (Bloomfield & al., 1992; Boyle, 1997; Barber, 1998).

Most importantly, the shift from local on-premises operated servers to foreign servers aggregating data from many different sources into a few centralised data centres is likely to decrease the autonomy of users who become more and more dependent on the infrastructure provided by the cloud providers. This concern has been strongly voiced by the Free Software Foundation, according to which cloud computing is likely to significantly decrease the autonomy of end-users, to the extent that cloud operators control the infrastructure of communication, the online applications, as well as all the content or data available on the cloud (Wu & al., 2011).

As a result, to the extent that they do not require extensive storage capacity or computing power, nor any particularly low response time or latency[1], many users' devices are devolving from powerful machines capable of running servers or applications on their own to increasingly small and less powerful devices – such as laptops, netbooks, tablets, smartphones, or any other device specifically designed to rely on third party infrastructures, platforms and online services provided by cloud providers (Lametti, 2012; De Filippi, 2013). As clearly illustrated by Jonathan Zittrain, professor of Internet law at Harvard Law School, in his book "The future of the Internet, and how to stop it" (Zittrain, 2008), user's devices are devolving from autonomous systems into "tethered appliances" or "dumb terminals" whose functionalities are entirely dependent on the services proposed by the cloud operators (Zittrain, 2008; p. 41). Even previously decentralised applications based on open and decentralised protocols (such as SMTP for email, or IRC for live communication) are now turning into centralised cloud-based applications (such as Hotmail, Gmail, Gtalk or Facebook for synchronous and asynchronous communications).

Cloud computing raises therefore a series of ethical issues concerning users' autonomy and control (Timmermans & al, 2010). In spite of the decentralised nature of the internet, the advent of cloud computing might, indeed, undermine the autonomy of users (De Filippi, 2013) who

benefit from innovative and personalised online services at the costs of becoming increasingly dependent on them (Haeberlen, 2010). Before the advent of cloud computing, even though hardware manufacturers could, to some extent, regulate users' behaviour by implementing specific features or technical constraints into particular devices, users were (at least theoretically) able to decide by themselves which applications to install and run on their own devices. Today, given that most applications are stored and run directly from the cloud, power is increasingly concentrated in the hands of a few large service providers, which have the ability to determine exactly what can or cannot be done on their platforms. In addition to the obvious concerns that this might entail in terms of data privacy and security (Nelson, 2009), relinquishing control over personal data or information can also undermine users' right to information self-determination (i.e. users' ability to determine, by themselves, how information can and will be used)[2] - a right which Germany has recognised as one of the most important parts of the general right of personality (Allgemeines Persönlichkeitsrecht).

## DECENTRALISED ALTERNATIVES TO CLOUD COMPUTING

Decentralised alternatives to centralised cloud computing platforms could significantly contribute to eliminate – or to the least mitigate – these issues. Indeed, as the advantages of cloud computing have become fairly well acknowledged by the public at large (Miller, 2008), a number of initiatives stemming from civil society have tried to overcome the drawbacks of centralisation with the development of alternative, decentralised applications. While they do not all rely on cloud computing technologies (i.e., virtualisation and distributed computing), most of these applications are presented as an alternative moving away from traditional cloud computing architectures based on centralised data centres and, towards more decentralised architectures based on the deployment peer-to-peer networks running on individual user's devices – the so-called "edge computing" (Wang & al., 2012).

Skype is perhaps one of the first and most popular cloud applications that relies, at least partially[3], on decentralised peer-to-peer architectures to route communications through the network of connected users. Initially developed by the creators of Kazaa, Skype was designed as a decentralised communication system allowing users to make voice-over-IP calls by sharing data between peers. Yet, Skype has been subsequently purchased by a variety of corporations, so that it nowadays combines a decentralised architecture and centralised management, as the whole communication infrastructure is ultimately controlled by Microsoft.

Today, many more cloud applications are being developed in a decentralised manner, so as to benefit from the advantages of cloud computing (as regards ubiquity, elasticity and scalability) without having to bear the costs and consequences of centralisation in terms of resources dependency and control.

Most advanced in this respect is SlapOs, an open source software relying on edge computing technologies for deploying decentralised cloud computing infrastructures. Recently selected to fuel the data centre of the Ivory Coast's Ministry of Interior, it supports various aspects of cloud computing, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Similarly, the Clommunity project provides a series of tools and applications aimed at supporting grassroots communities in bootstrapping, managing and operating community cloud services within the context of community-owned networks (mesh

networks). Other popular alternatives to centralised cloud applications are OwnCloud and CozyCloud, two open source software applications allowing people to run their own private personal server (or "cloud") to aggregate data into a single place to be subsequently reached from anywhere and at any time. As opposed to traditional cloud applications, where all data is controlled by a third party, these applications can be installed on personal servers, allowing for users to maintain ownership and control over their own data. Similarly, Unhosted is a project trying to break the monopoly established by traditional cloud providers over user's data, by separating the software application from the data it processes[4]">http://unhosted.org. Finally, CrossCloud is a project run by Tim-Berners Lee (W3C Director and Professor at MIT) whose goal is to promote interoperability between different cloud services. As such, the service is intended to provide users with the freedom to move data and information among a variety of hardware platforms, software applications, and social networks, while keeping their data and social connections intact.

With regards to more specialised cloud computing platforms, various initiatives have been deployed to counteract the trend towards the growing centralisation of online services. Notable examples of such platforms include Diaspora, a decentralised alternative to Facebook based on a federated network of servers running on users' devices; Kune, a distributed software providing online real-time collaborative software to facilitate the coordination of online communities; and MailPile, an alternative to the most popular web-based emails services, ultimately aimed at helping users take back control over their own e-mails.

In most of these applications, the issue of data sovereignty is key (De Filippi & McCarthy, 2012). Many of these applications have, indeed, been developed to counteract the establishment of walled gardens – closed or proprietary platforms that users generally get trapped into (Lametti, 2012). Yet, even though they could – eventually – provide an attractive alternative to many centralised online services, most of the applications are still under development and thus only benefit from a very limited user-base.

More specialised applications also exist, which are specifically concerned with the issue of data sovereignty and information self-determination. MyProfile is a project which purports to give users back control over the data they produce and share over the internet by means of a centralised and unified user accounts whose data is aggregated into one particular device controlled by the user. SquareTag is another service that helps people manage and keep track of the things they own by endowing them with additional functionalities they would otherwise not have; this is done by creating a personal and individual cloud service for any given object, along with custom applications that enable people to interact with these objects. Finally, Stample is a tool intended to help users build their own knowledge network by harvesting online content and organising into a personal library, rating, highlighting, summarising or annotating content, to eventually share it with selected peers in the network.

## AUTONOMY GAINS

Most of these decentralised cloud applications are also designed to preserve the autonomy and protect the privacy of end-users. Indeed, with the exception of Skype, which, as mentioned above, is ultimately controlled by one single entity, decentralised alternatives to centralised cloud computing platforms are - for the most part - autonomously deployed and independently governed by a particular community of users who both benefit from and contribute to the successful operations of the cloud service (Graham, 2011).

By relying exclusively on the computing resources of individual users' devices, it becomes indeed possible to create powerful and dynamic cloud environments which are not controlled by any third party operator, but only and exclusively by the actual members of the community (Marinos & Briscoe, 2009). Re-claiming ownership over the technical infrastructure of the cloud platform allows users to more easily control the manner in which and the extent to which content or data stored into the cloud will be accessed and subsequently exploited by the community (Wu & al., 2010).

Given the various proven and suspected infringements of privacy and data protection regulations committed by most of the large cloud computing operators (such as Google, Facebook, Apple, etc), users' rights to privacy and information self-determination are likely to be better respected (and protected) in decentralised cloud computing architectures. It has, however, to be noted that decentralised cloud computing applications might entail higher management costs and greater security risks than their centralised counterparts, mainly due to the need for coordinating a large number of untrusted and potentially malicious devices (Camp, 2003).

# POLICY IMPLICATIONS

The emergence of decentralised cloud applications has the potential of providing the same benefits of more traditional cloud applications, without the drawbacks that usually come along centralisation. This is not to say, however, that decentralised cloud applications are not devoid of any problems. While they resolve some of the privacy and security challenges posed by centralised online platforms (Mondal & Kitsuregawa, 2006; Tabaki & al., 2010), decentralised architectures introduce a whole new series of concerns, mostly related to the difficulty to uphold and enforce the law (Hughes & al., 2006). As such, decentralised cloud services can be regarded as having two distinct – and to large extent divergent – effects, which significantly differ as regards their policy implications:

On the one hand, decentralised alternatives to cloud computing constitute an attempt at resolving some of the issues that have not yet been properly addressed by the law. These issues include security, privacy and autonomy concerns affecting internet users who interact on a daily basis with centralised cloud computing platforms and applications. Given the regulatory gap that characterises the cloud computing industry[5] and the lack of political interest in filling this gap – especially in view of the pressure exerted by US government institutions such as the National Security Agency (NSA), which actually expect online service providers to collect and reveal data from their user-base – lobbying and advocacy from civil society is unlikely to result in any practical outcome before a long period of time. As opposed to political action, the implementation of decentralised cloud platforms can, therefore, essentially be regarded as an attempt by civil society to complement and, in certain cases, to supplement the law, by relying on a combination of technological means and distributed governance models.

On the other hand, however, decentralised cloud applications could jeopardize the regulatory framework established so far to enforce national laws into the cyberspace. Indeed, in order to regulate the activities of individual internet users, it is generally much easier for the state to rely on large online intermediaries, such as cloud operators, and delegate to them the responsibility to enforce legal norms onto their users (Bartling & Fischbacher, 2012). The regime of intermediaries liability limitations established in several countries across the world[6] is an example of the growing tendency to rely on private enforcement mechanisms as a means to

ensure proper application of the law in the digital world (Frydman & Rorive, 2002; Swartout, 2011). Yet, moving into the realm of decentralised architectures, it becomes more and more difficult to establish the entity that could be regarded as an actual "intermediary." Given that there is no central data centre nor entity regulating the operations of a distributed cloud application, no specific entity can be held liable for the traffic passing through the cloud's peer-to-peer network. In this regards, the question arises as to the extent in which the operators of decentralized cloud services will be subject to the upcoming EU regulation[7] on data protection to the extent that they may or may not qualify for the so called household exemption. This provision already exists under the Data Protection Directive of 1995. It excludes "natural person[s] in the course of a purely personal or household activity" from being treated as processors of data in the sense of the Directive.

Seen in this light, decentralised alternatives to cloud computing might no longer be regarded as a complement to the law, but rather as a means to escape from traditional law enforcement practices. Indeed, if one agrees that there subsists an inherent trade-off between decentralisation and control (Buchegger & Datta, 2009; Datta & al., 2010), it follows that the greater the degree of decentralisation of any given online platform, the harder it will be for anyone to exert any type of control over that platform. It is, in fact, very hard for the state to regulate the activities of a large number of peers, whose identities are often unclear and whose operations are much more difficult to monitor or control (David, 2010). Hence, while most of the centralised cloud computing platforms can be easily regulated and controlled, cloud applications based on decentralised peer-to-peer networks could potentially be used to ignore, or even bypass the law.

**FOOTNOTES**

1. In the realm of what some call the "tactile" internet - where there is a need for applications to have an extremely low response time - processing power is moved towards the end-users and storage is pushed back into users devices or decentralised servers in order to reduce latency to the minimum.

2. Information self-determination has been defined by Cavoukian (2008) as the ability for users to exercise personal control over the collection, use and disclosure of personal information by third parties.

3. Skype is a hybrid peer-to-peer and client–server system, which relies on a central server of communication, but also benefits from the bandwidth and background processing of computers running the Skype software.

4. Unhosted implements a model whereby only the source code of an application is stored on the web server, so that the application must first be downloaded onto the user's device before it can be executed. The advantage of this model is that users' data could theoretically be hosted anywhere, and – since it never goes through the web server – it cannot be illegitimately exploited by a third party. More information on Unhosted cloud computing services is available at 5. There is, to date, no comprehensive regulatory framework for cloud computing, the industry is ultimately regulated by a large number of independent sectoral laws. In Europe, for instance, despite the European Cloud Computing Strategy whose goal is to establish common standards and best practices in the European cloud computing industry, there is still the need for a coherent and harmonised pan-European regulatory framework for cloud computing, in order to avoid legal uncertainty deriving from different (and sometimes inconsistent) policies and laws in different countries. Similarly, in the US, the cloud computing industry is not

regulated as such, it is indirectly regulated by a variety of national and statutory Acts related to specific bodies of law, such as telecommunications, e-commerce, antitrust, and privacy. The result is - again - a substantial degree of legal uncertainty: given the transnational scope of many cloud services, it is often difficult to assess, precisely, the laws which cloud operator should be subject to. For more details on this issue, see e.g. Kshetri (2012); Sluijs & al. (2011); Wood & Anderson (2011).

6. Intermediary liability limitations regime considerably vary in their scope from one country to another. Most rely, however, on the ability of intermediaries of policing the Internet on the behalf of the State. See e.g. provisions of the European e-Commerce Directive (2000/31/EC) and the European Directive on the enforcement of intellectual property rights (2004/48/EC) for Europe; the Digital Millenium Copyright Act of 1998 and the provisions of the Anti-Counterfeiting Trade Agreement (ACTA) for the US; the Australian Commonwealth Copyright Act, the Broadcasting Services Act and the Racial Discrimination Act of 1975 for Australia; the Canada's Copyright Act of 1921, as amended by bills C-60, C-61, C-32 and C-11, etc.

7. To the extent that the current EU Data Protection Directive 95/46/EC does not properly take into account recent technological developments such as cloud computing, the European Commission has submitted a proposal to update and unify data protection regulations within the European Union through a single General Data Protection Regulation (GDPR), that should be adopted in 2014.

**REFERENCES**

Baliga, J., Ayre, R. W., Hinton, K., & Tucker, R. S. (2011). Green cloud computing: Balancing energy in processing, storage, and transport. *Proceedings of the IEEE*, 99(1), 149-167.

Barber, B. R. Three scenarios for the future of technology and strong democracy. *Political Science Quarterly*, 1998, vol. 113, no 4, p. 573-589.

Bartling, B., & Fischbacher, U. (2012). Shifting the blame: On delegation and responsibility. *The Review of Economic Studies,* 79(1), 67-87.

Becker, T. (2001). Rating the impact of new technologies on democracy. *Communications of the ACM*, 44(1), 39-43.

Berl, A., Gelenbe, E., Di Girolamo, M., Giuliani, G., De Meer, H., Dang, M. Q., & Pentikousis, K. (2010). Energy-efficient cloud computing. *The Computer Journal*, 53(7), 1045-1051.

Bloomfield, B. P., & Coombs, R. (1992). INFORMATION TECHNOLOGY, CONTROL AND POWER: THE CENTRALIZATION AND DECENTRALIZATION DEBATE REVISITED*. *Journal of Management Studies*, 29(4), 459-459.

Boyle, J. Foucault in cyberspace: Surveillance, sovereignty, and hardwired censors. *U. Cin. L. Rev.*, 1997, vol. 66, p. 177.

Buchegger, S., & Datta, A. (2009, February). A case for P2P infrastructure for social networks-opportunities & challenges. In *WONS 2009 : Sixth International Conference on Wireless On-demand Network Systems and Services* (pp. 161-168). IEEE.

Camp, L. J. (2003). Designing for trust. In *Trust, Reputation, and Security: Theories and Practice* (pp. 15-29). Springer Berlin Heidelberg.

Carlson, C. N. (2003). Information overload, retrieval strategies and Internet user empowerment.

Cavoukian, A. (2008). Privacy and Digital Identity: Implications For The Internet. In P*roceedings from Identity in the Information Society Workshop, Lake Maggiore, Italy*.

Datta, A., Buchegger, S., Vu, L. H., Strufe, T., & Rzadca, K. (2010). Decentralized online social networks. In *Handbook of Social Network Technologies and Applications* (pp. 349-378). Springer US.

David, M. (2010). *Peer to peer and the music industry: The criminalization of sharing*. Sage Publications.

De Filippi, P. (2013). Ubiquitous Computing in the Cloud : User Empowerment –vs- User Obsequity, in Jean-Eric Pelet, Panagiota Papadopoulou (eds.) *User Behavior in Ubiquitous Online Environments*, IGI Global.

De Filippi, P., & McCarthy, S. (2012). Cloud Computing: Centralization and Data Sovereignty. *European Journal of Law and Technology*, 3(2).

Frydman, B., & Rorive, I. (2002). Regulating Internet content through intermediaries in Europe and the USA. *Zeitschrift für Rechtssoziologie*, 23(1), 41-59.

Garrett, R. K. (2006). Protest in an information society: A review of literature on social movements and new ICTs. *Information Communication and Society*,9(2), 202.

Graham, M. (2011). Cloud Collaboration: Peer-Production and the Engineering of the internet. In *Engineering earth* (pp. 67-83). Springer Netherlands

Grothoff, D. M. C. (2003). Resource allocation in peer-to-peer networks. *Wirtschaftsinformatik*, 45(3), 285-292.

Haeberlen, A. (2010). A case for the accountable cloud. *ACM SIGOPS Operating Systems Review*, 44(2), 52-57.

Hughes, D., Walkerdine, J., Coulson, G., & Gibson, S. (2006). Peer-to-peer: Is deviant behavior the norm on p2p file-sharing networks?. *Distributed Systems Online, IEEE,* 7(2).

Kshetri, N. (2012). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*.

Lametti, D. (2012). The Cloud: Boundless Digital Potential or Enclosure 3.0?. in Virginia Journal of Law & Technology, 2012

Loader, B., Hague, B., & Eagle, D. (2000). Embedding the net: Community empowerment in the age of information. *Community informatics: Enabling communities with information and communications technologies*, 81-102.

Marinos, A., & Briscoe, G. (2009). Community cloud computing. In *Cloud Computing* (pp. 472-484). Springer Berlin Heidelberg

Mondal, A., & Kitsuregawa, M. (2006, September). Privacy, security and trust in p2p environments: A perspective. In *Database and Expert Systems Applications, 2006*. DEXA'06. 17th International Workshop on (pp. 682-686). IEEE.

Miller, M. (2008). *Cloud computing: Web-based applications that change the way you work and collaborate online*. Que publishing.

Nelson, M. R. (2009). The cloud, the crowd, and public policy. *Issues in Science and Technology*, 25(4), 71-76.

Oram, A. (Ed.). (2001). *Peer-to-peer: Harnessing the Benefits of a Disruptive Technologies*. O'Reilly Media, Inc.

Sluijs, J., Larouche, P., & Sauter, W. (2011). Cloud Computing in the EU Policy Sphere.

Swartout, C. M. (2011). Toward a Regulatory Model of Internet Intermediary Liability: File-Sharing and Copyright Enforcement. *Nw. J. Int'l L. & Bus.*, 31, 499.

Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *Security & Privacy, IEEE*, 8(6), 24-31.

Timmermans, J., Ikonen, V., Stahl, B. C., & Bozdag, E. (2010, November). The ethics of cloud computing: a conceptual review. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on* (pp. 614-620). IEEE.

Wang, L., Ranjan, R., Chen, J., & Benatallah, B. (Eds.). (2012). *Cloud computing: methodology, systems, and applications*. CRC Press.

Wood, K., & Anderson, M. (2011, October). Understanding the complexity surrounding multitenancy in cloud computing. In *e-Business Engineering (ICEBE), 2011 IEEE 8th International Conference on* (pp. 119-124). IEEE.

Wu, R., Ahn, G. J., Hu, H., & Singhal, M. (2010, October). Information flow control in cloud computing. In *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on* (pp. 1-7). IEEE.

Wu, G., Talwar, S., Johnsson, K., Himayat, N., & Johnson, K. D. (2011). M2M: From mobile to embedded internet. *Communications Magazine*, IEEE, 49(4), 36-43.

Younge, A. J., Von Laszewski, G., Wang, L., Lopez-Alarcon, S., & Carithers, W. (2010, August). Efficient resource management for cloud computing environments. In *Green Computing Conference, 2010 International* (pp. 357-364). IEEE.

Zittrain, J. (2008), 'Tethered Appliances, Software as Service, and Perfect Enforcement', In *The Future of the Internet and How to Stop it*, Yale University Press, New Haven, pp. 101-126.