INTERNET POLICY REVIEW
Journal on internet regulation

Volume 2 | Issue 2

Cloud computing: analysing the trade-off between user comfort and autonomy

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

Published on 13 Jun 2013 | DOI: 10.14763/2013.2.135

Abstract: This article presents a general analysis of how user autonomy in cloud computing is increasingly put into jeopardy by the growing comfort and efficiency of the user-interface. Although this issue has not been, thus far, explicitly addressed by law, it is a fundamental ethical question that should be carefully assessed to guide the future deployment of cloud services. Different policy decisions might, in fact, significantly affect user's fundamental rights and online freedoms by shifting the balance from one part of the trade-off to the other. This article aims to explore emerging trends in cloud computing technologies and analyse them from an ethical perspective. among other in order to identify the issues they might raise, and the extent to which current laws and regulations take these issues into account.

Keywords: Cloud services, Autonomy, Comfort, Proprietary software, Interoperability, End-to-end, Walled garden, User lock-in, Profiling

Article information

Received: 10 May 2013 **Reviewed:** 11 Jun 2013 **Published:** 13 Jun 2013
Licence: Creative Commons Attribution 3.0 Germany
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/cloud-computing-analysing-trade-between-user-comfort-and-autonomy

Citation: De Filippi, P. (2013). Cloud computing: analysing the trade-off between user comfort and autonomy . *Internet Policy Review*, *2*(2). DOI: 10.14763/2013.2.135

This article presents a general analysis of how user autonomy in the internet cloud is increasingly put into jeopardy by the growing comfort and efficiency of the user-interface. Although this issue has not been, thus far, explicitly addressed by the law, it is a fundamental ethical question that should be carefully assessed to guide the future deployment of cloud computing. Different policy decisions might, in fact, significantly affect users' fundamental rights and online freedoms by shifting the balance from one part or another of the trade-off between user comfort[1].

As mentioned by Eben Moglen (2010) in a talk at the New York branch meeting of the Internet Society (ISOC), the original structure of the internet was "designed as a network of peers without any intrinsic need for hierarchical or structural control"[2] contributing with their own resources to creating the underlying architecture of the network. With the advent of cloud computing, this architecture is being progressively replaced by an increasingly centralised structure, made up of large clusters (or data-centres) aggregating a great number of computing resources into one place (Rimal & al, 2009).

Today, many internet users interact with the cloud in most of their online activities, without always being aware of it. They all cherish the comfort derived from ubiquitous access to a variety of hardware and software resources; they treasure the ability to store their documents online, see their pictures or listen to music at any time and from anywhere - regardless of the device used (Yoo, 2011).

The benefits that users can derive from cloud-based applications are manifold, although they can, for the most part, be associated with the concepts of comfort and ubiquity.

Accessibility is key. Users no longer need to invest into hard-drives, CDs or DVDs in order to store their data, as everything can be stored into the cloud. They no longer have to purchase a significant amount of random-access memory or processing power in order to use sophisticated software, as software can be run directly from a web-browser. Finally, as a result of modern information and communication technologies (ICTs), users no longer need to rely on cables or the like in order to access the internet, as everything can be always and ubiquitously connected by wireless means (Kloch & al, 2011).

Also the size of the device matters. The smaller the device is, the more convenient it is and - to some extent - the more efficient it is, since it suffices to connect it to the cloud to get access to a whole new realm of possibilities, as a humongous amount of data, content, or software applications become instantaneously available, regardless of the processing power or storage capacity of the user's device (Furht, 2010).

Finally, comfort is another key aspect of the cloud. User-friendly interface, attractive look and feel, and a personalised service are the basic ingredients for a successful online application. Oftentimes, the functionality of the services is just as important as the convenience it presents to the users. Integrated services, such as those offered by Google (providing an interconnected suite of web applications, including mailbox, calendars, file storage, photo catalogues, or online documents) and Apple (allowing to link a variety of devices - such as the iPod, the iPhone, the iPad or the iMac - and automatically synchronising them by connecting them to Apple's iCloud) are much more attractive to users than standalone applications, which - despite having more sophisticated features - are ultimately harder to use (Lenk & al, 2009).

The potential of cloud computing and the benefits it offers to many end-users are undoubtedly important. Yet, one should not forget to account for important ethical concerns that must necessarily be considered when assessing the pros and cons of cloud computing. While the large set of privacy concerns resulting from exporting a growing amount of data into the cloud have already been thoroughly analysed by many legal scholars (Pearson, 2009; Robison, 2009; Zhou & al, 2010; Svantesson & Clarke, 2010; Pearson & Benameur, 2010; Jansen, 2011; Gellman, 2012), other dangers have yet to be further explored by internet scholars. Indeed, by relying extensively (or almost exclusively) on cloud-based services, not only are users increasingly losing control or sovereignty over their own content and personal data (De Filippi & McCarthy, 2012), they are, in many ways, also giving up their freedoms and autonomy as individuals (Moglen, 2010; Lametti, 2012).

WHEN COMFORT DICTATES THE ROAD AHEAD

In the context of cloud computing, more comfort often equals less choice. By relinquishing their software applications, processing power and storage capacity, users become increasingly dependent upon the hardware resources and applications provided by online service providers. A shift away from the so called end-to-end principle seems to be taking place. Considered by many as one of the fundamental design principles of the internet network, the end-to-end principle is also an important precondition for user autonomy. Indeed, the principle stipulates that the intelligence of the internet should subsist not in the network itself but rather at its end-points (i.e. at the level of users' devices). This means that the network should remain a mere (and neutral) means of communication, and that end-nodes are powerful enough to be running servers and providing online services for user interaction and online communication. This is in contrast with the trend that emerged with the advent of cloud computing, as more and more cloud-based services are designed to work with centralised clusters or data centres where all computing resources are aggregated and subsequently made available to the public through online applications (Miller, 2008). This encouraged the emergence of "stupid terminals" that merely connect to a series of cloud-based services operated by large online providers on centralised mainframes.

In spite of the apparent advantages for end-users, cloud-based services present a series of drawbacks, for the most part related to the issue of property and control. Indeed, as the possession of user data or content progressively shifts from end-users to online operators, and as an increasing number of software applications becomes accessible only through the user interface specifically provided by the cloud, cloud operators are ever more likely to regulate and control the manner in which and the extent to which these applications can effectively be used (De Filippi & Vieira, 2013).

In terms of comfort and accessibility, the promises of cloud computing might lead consumers to favour small and lightweight devices. These devices are, however, often unable to run independent software on their own. The concept of “software as a service” (SaaS) constitutes as such an important paradigm shift in computing: users devices are no longer self-sufficient, they are tethered to centrally managed cloud applications, whose technical features and characteristics can be unilaterally modified by the service providers, in a way that is often invisible to end-users. While this is similar to standard software with auto-update functionalities, the difference in the context of cloud computing is that users no longer have a choice but to use third-party software provided by online operators. In the words of Jonathan Zittrain - professor of internet law at Harvard Law School - we are moving away from generative technologies (i.e., general purpose devices capable of running any software they encounter, as well as changing them if the need arises) towards increasingly limited and constrained devices that are only capable of carrying out a predetermined amount of tasks and operations (Zittrain, 2006).

WALLED GARDENS AND USER LOCK-IN

The growing dependency that subsists between user devices and cloud providers might lead to a further limitation of choice to the extent that many of these devices - such as Apple's iPod, iPhone and iPad, the Amazon Kindle, the Sony Reader, or the Nook from Barnes & Noble - are based on proprietary software and non-interoperable formats. Although this is a common situation in the software realm (e.g., Microsoft Word and its DOC format), the problem is further exacerbated in the case of tethered devices[3], to the extent that it is no longer possible for users to install alternative software onto their own devices without bypassing or circumventing technological measures of protection. The result is the establishment of “walled gardens”[4] - enclosed systems which users get eventually locked into (Anderson & Rainie, 2010).

More comfort, therefore, also means that it becomes more difficult for users to leave the system they have entered into. Indeed, insofar as user data is stored in foreign data centres controlled by large multinational corporations, it is increasingly difficult for users willing to delete specific data from their accounts to actually determine whether or not such data has been effectively deleted from the system (Viega, 2009). Besides, and perhaps most importantly, while many cloud operators - such as Google, Apple, Facebook, or Twitter - provide a means for users to retrieve their data locally onto their own devices, the lack of a standard, open and interoperable format does not, however, facilitate migration from one platform to another[5]. Users are, therefore, often stuck into a (semi)-proprietary system, incapable of switching back and forth from one service provider to another without losing some (or all) of the data thus far exported into the system (Bozman, 2010).

While this issue has been addressed, to some extent, by the proposed new Data Protection Regulation[6], the right to data portability does not, however, sufficiently enforce interoperability amongst services (De Filippi & Belli, 2012). Cloud computing consequently raises the issue of monopolies and user lock-in, encouraging a series of practices that might eventually harm competition in the market, by reducing the opportunity for users to select between a wide variety of competing services.

PROFILING AND DELEGATED DECISION-MAKING

In addition to data collection, data mining and monitoring techniques can be used for the purposes of profiling and analysis (Gantz & Reinsel, 2011). These practices, which have been unnoticed for a long time, are nowadays massively widespread. Although it is well known that Google constantly and relentlessly processes users’ emails in order to provide targeted advertisements, it is often forgotten that similar data mining and machine learning techniques can be used to profile the user base and allocate each user into specific categories or types[7].

While the implications in terms of privacy and data protection are already well-known (Pearson, 2012), the potential repercussions of these practices on user autonomy are unclear. Although they often consent to the collection and processing of personal data for the purposes of getting a more personalised and customised service, users are, indeed, generally not properly informed of the implications that profiling might have on their individual autonomy.

By aggregating data coming from many different sources, cloud operators can rely on different kinds of data (even anonymised data) to discover the habits and the profile of their user-base (Agrawal & al., 2011). For instance, as Google recently changed its privacy policy to be able to process together data collected from different services, such as Gmail, Google calendar, Google drive, Google+, Youtube or Picasa, it becomes very easy for it to leverage on the data collected from one service in order to customise another.

Finally, one of the most dangerous issues with cloud computing technologies is that they can (and often do) take a series of decisions in lieu of the user - an issue that is most prominently discussed under the label of “filter bubble” (Pariser, 2011). While this might be regarded as an advantage by some users who would rather not deal with everyday issues and concerns (which can most likely be resolved in a faster and most effective way by a computer), automated decision-making could, however, negatively affect the autonomy of these users insofar as they can no longer control the decision they make (Pallett, 2011; Pearson & Benameur, 2010; Chui & al., 2010). This is well illustrated by the recently incorporated feature in Google Search to provide more personalised search results reorganised according to user profiles. These profiles are generated by Google (whether or not the user has opted in to receive personalised results) aggregating information which may be either explicitly provided by users or implicitly inferred by tracking the online habits and navigation behaviours of these users both inside and outside of Google Search[8]. As a result, users benefit from more and more personalised set of results, which are more likely to satisfy the search queries of each individual user. Users are, however, also foregoing the opportunity of exploring a more diverse selection of search results, to subsequently decide - by their own means - which are the most relevant ones.

Thus, the risk is that, without proper checks and balances, delegated decision-making could eventually turn users into passive decision-makers who are no longer aware of the choices that have been unilaterally imposed upon them by the cloud operators.

A GROWING NEED FOR REGULATION

According to Lawrence Lessig - Professor of Law and Leadership at Harvard Law School - "*Cyberspace has an architecture; its code - the software and hardware that defines how cyberspace is - is its architecture. That architecture embeds certain principles; it sets the terms on which one uses the space; it defines what's possible in the space.*” In other words, code - as one of the main driver of regulation for internet infrastructures - *is law* (Lessig, 1999). By analogy, in the context of cloud computing, the user interface - which precisely stipulates what users can or cannot do - *is law* (De Filippi & Vieira, 2013).

Yet, if code indeed regulates the cyberspace, then code must itself be regulated so as to support, or at least comply with the law. Indeed, to the extent that its design or technical features might potentially impinge upon user’s civil liberties and fundamental rights, the user interface must be designed in line with legal principles and provisions. By analogy with the concept of *privacy-by-design* - a concept promoted by Ann Cavoukian (Information & Privacy Commissioner of Ontario, Canada) according to which privacy and data protection principles must be embedded in the design and enforced throughout the entire lifecycle of a technology - the user interface of any cloud-based application should be designed in such a way as to account for its impact on users’ rights and freedoms, from the early design and deployment to the ultimate use and disposal of the service[9].

Indeed, while the collection and processing of personal data are generally agreed upon by end-users - who agree to a series of long and complex contractual agreements that often qualify as contracts of adhesion (Calloway, 2012) - contractual provisions generally only stipulate the terms and conditions for data mining and collection, as well as for the processing thereof. They do not explicitly inform users of what are the actual consequences of these practices in terms of privacy, freedom of expression, interoperability, data sovereignty and control. Users are therefore left with limited autonomy as they lose their ability to make properly informed choices

(Anderson & Rainie, 2010). This raises a series of ethical concerns as regards user freedoms and autonomy, which have - thus far - not been explicitly addressed by the law to the extent that they do not directly impinge upon any of the established users' rights, such as the right to privacy and the freedom of expression.

Thus, while cloud computing is not as such incompatible with user freedoms and autonomy, its downsides have, nonetheless, to be acknowledged so that proper regulation can be enacted to effectively address the risks it might engender.

The problems ultimately relate to the issues of control and responsibility. As a large variety of computing resources (be them either data, software or hardware resources) are exported into the cloud, the question arises as to who actually controls these resources and who is responsible for the usage that is made of them. As more and more tasks and decisions are delegated to a variety of cloud operators, it becomes crucial to determine their corresponding duties and obligations to end-users. Yet, given the large number of actors involved in the provision of cloud-based services (Leimeister & al., 2010), it is often difficult to attribute causal relationships, roles or responsibilities to each actor.

Hence, given the difficulty to address *ex-post* the problems resulting from the loss of user autonomy, it is suggested that the legislator might need to implement a series of “proactive measures” to discourage *ex-ante* the emergence of unfair practices that would excessively limit or constrain users' freedom and autonomy in the cloud.

FOOTNOTES

[1] As opposed to the definition of “autonomy” proposed by Alan Westin in “Privacy and Freedom” (1968), where autonomy is ultimately seen as a function of privacy, we refer here to “autonomy” as the ability of users to decide for themselves on the way they communicate online, i.e. the manner in which and the extent to which they can access, consume or exchange information on the internet.

[2] Except in certain cases, such as the Domain Name System, where a centralized hierarchical structure is needed for the proper functioning of the network.

[3] "Tethered devices" are devices which the user cannot fully control, because the parent companies maintain a certain degree of control over these devices insofar as they can decide on their actual functionalities, the degree of interoperability with other devices, as well as the manner in which and the extent to which they can be used in any given situation. Mobile phones, mp3 players, consoles, tablets are common examples of tethered devices where the seller uses internet connectivity in order to control the use of the devices it sells to end-users.

[4] According to Wikipedia, a walled garden or closed platform is a software system where the carrier or service provider has control over applications, content, and media and restricts convenient access to non-approved applications or content. This is in contrast to an open platform, where consumers have unrestricted access to applications and content.

[5] Although many online services allow users to export their personal information or data, it is often difficult to subsequently import that data into another online platform. Users often have to figure out the process themselves or they must rely on third party services or software applications, which might not always be able to restore all content or preserve all data from the

previous system - such as, for instance, metadata and privacy settings.

[6] Article 18 of the draft Data Protection Regulation of the European Commission introduces a right to data portability (i.e., the right to transfer data from one electronic processing system to another), which includes the right to obtain user data in a "structured and commonly used electronic format".

[7] For an overview of current and prospective applications of data mining and machine learning techniques as employed in the context of several Google services and online applications, see e.g., http://research.google.com/pubs/DataMining.html

[8] For more details on the actual implementation of Google personalized search algorithm, see Google's Patent for Personalization of placed content ordering in search results.

[9] This topic was widely discussed in the 1990s, mostly in the area of Computer-supported cooperative work (CSCW). See e.g. Bellotti & Sellen (1993): Design for Privacy in Ubiquitous Computing Environments.

REFERENCES

Agrawal, D., Das, S., & El Abbadi, A. (2011, March). Big data and cloud computing: current state and future opportunities. In Proceedings of the 14th International Conference on Extending Database Technology (pp. 530-533). ACM.

Anderson, J. Q., & Rainie, H. (2010). The future of cloud computing. Washington, DC: Pew Internet & American Life Project.

Bellotti, V., & Sellen, A. (1993, January). Design for privacy in ubiquitous computing environments. In Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW'93 (pp. 77-92). Springer Netherlands.

Bozman, J. (2010). Cloud Computing: The Need for Portability and Interoperability. IDC Analyze the Future, Sponsored by Red Hat, Inc.

Calloway, T. J. (2012). Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm. Duke L. & Tech. Rev., 163.

Chui, M., Löffler, M., & Roberts, R. (2010). The internet of things. McKinsey Quarterly, 2, 1-9.

De Filippi P., Belli, L. (2012), The Law of the Cloud v the Law of the Land: Challenges and Opportunities for Innovation, European Journal of Law and Technology, 3(2).

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

De Filippi P., Vieira M. S. (2013), The commodification of Information Commons, in International Journal of the Commons, Special Issue : The Knowledge Commons : from historical open science to digitally integrated research networks, 2013 (forthcoming)

Furht, B. (2010). Cloud computing fundamentals. In Handbook of cloud computing (pp. 3-19). Springer US.

Gantz, J., & Reinsel, D. (2011). Extracting value from chaos. IDC iView, 1-12.

Gellman, R. (2012, August). Privacy in the clouds: risks to privacy and confidentiality from cloud computing. In Proceedings of the World privacy forum,.

Jansen, W. A. (2011, January). Cloud hooks: Security and privacy issues in cloud computing. In System Sciences (HICSS), 2011 44th Hawaii International Conference on (pp. 1-10). IEEE.

Kloch, C., Petersen, E. B., & Madsen, O. B. (2011). Cloud based infrastructure, the new business possibilities and barriers. Wireless Personal Communications, 58(1), 17-30.

Lametti, D. (2012). The Cloud: Boundless Digital Potential or Enclosure 3.0?.

Leimeister, S., Böhm, M., Riedl, C., & Krcmar, H. (2010). The business perspective of cloud computing: Actors, roles and value networks.

Lenk, A., Klems, M., Nimis, J., Tai, S., & Sandholm, T. (2009, May). What's inside the Cloud? An architectural map of the Cloud landscape. In Proceedings of the 2009 ICSE Workshop on

Software Engineering Challenges of Cloud Computing (pp. 23-31). IEEE Computer Society.

Lessig, L. (1999). Code: And other laws of cyberspace. Basic Books (AZ).

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

Moglen, E. (2010), Freedom in the Cloud: Software Freedom, Privacy, and Security for Web 2.0 and Cloud Computing.

PALLETT, J. (2011). Automated decision-making. Broadcast Engineering, 53(4), 104-107.

Pariser, E. (2011). The filter bubble: What the Internet is hiding from you. Penguin.

Pearson, S. (2009, May). Taking account of privacy when designing cloud computing services. In Software Engineering Challenges of Cloud Computing, 2009. CLOUD'09. ICSE Workshop on (pp. 44-52). IEEE.

Pearson, S., & Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on (pp. 693-702). IEEE.

Pearson, S. (2012). Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing, Computer Communications and Networks, S. Pearson and G. Yee (eds.), Springer.

Rimal, B. P., Choi, E., & Lumb, I. (2009, August). A taxonomy and survey of cloud computing systems. In INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on (pp. 44-51). Ieee.

Robison, W. J. (2009). Free at What Cost: Cloud Computing Privacy under the Stored Communications Act. Geo. LJ, 98, 1195.

Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. Computer Law & Security Review, 26(4), 391-397.

Viega, J. (2009). Cloud computing and the common man. Computer, 42(8), 106-108.

Westin, A. F. (1968). Privacy and freedom. Washington and Lee Law Review, 25(1), 166.

Yoo, C. S. (2011). Cloud computing: Architectural and policy implications.Review of Industrial Organization, 38(4), 405-421.

Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010, November). Security and privacy in cloud computing: a survey. In Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on (pp. 105-112). IEEE.

Zittrain, J. L. (2006). The generative internet. Harvard Law Review, 1974-2040.