Trans Atlantic Consumer Dialogue

DOC NO: INFOSOC 46-11 DATE ISSUED: JUNE 2011

Resolution on Consumer Protection in Cloud Computing

Consumers, businesses and governments are increasingly using cloud computing services to store and share data. These services can offer users many benefits such as a large storage capacity, convenient access from any computer, and a high level of security. Use of cloud computing services by governments and businesses can reduce their expenditures for hardware and software, and the resulting savings may be passed along to taxpayers and consumers. However, the use of cloud computing services for data pertaining to consumers also raises many concerns. These concerns center mainly on control of the data: Who has access to it? How can it be used? How easy is it to move one's data from one cloud service to another? How secure is the data? Who is responsible if the data is lost or abused? Unresolved, these concerns are likely to prevent the widespread adoption of these valuable and efficient services. Therefore, governments and businesses must adopt policies that protect consumers with regard to law enforcement access to their data in the cloud, secondary uses of their data, portability and interoperability, data security, data deletion, transparency, and terms of use.

Recommendations

The Trans Atlantic Consumer Dialogue resolves that the governments in the United States and Europe should require these protections for business-to-consumer cloud computing services:

1. Data that consumers store in the clouds should have the same legal protections with regard to access by governments and others as it would if it was stored on their own computers. To the extent appropriate, consumers should receive notice of criminal and civil requests for data that is stored with cloud computing services before such requests are fulfilled.
2. Cloud computing services should not use or allow others to use consumers' data for secondary purposes without first clearly explaining to consumers how it will be used and by whom and obtaining their express affirmative consent. Secondary use should be limited to those purposes for which consumers have provided such consent.
3. Cloud computing services should not be allowed to exploit the physical locations of their servers in order to limit consumers' rights concerning the privacy and security of their data.
4. Cloud computing services should not interfere with consumers' ability to move their data to another service or to use their data in an interoperable manner with other services.

5. Cloud computing services should be required to meet and demonstrate that they maintain adequate security standards to protect consumers' data. Compliance with security measures should be monitored through independent auditing. Consumers should be provided with information about the security of their data and given the means to safeguard their data through tools such as encryption for which only the consumers themselves have the keys.
6. Consumers should have the right to delete the data that they had provided to cloud computing services for storage.
7. Cloud computing services should be required to be transparent about how they operate, what legal protections apply to consumers' data, and whom to contact to ask questions or make complaints.
8. Cloud computing services should be prohibited from using unfair contract terms such as requiring consumers who use free services to agree to a lower level of protection than those who pay or requiring that consumers give up the right to take legal action to resolve disputes.
9. Cloud computing services should be required to provide consumers with clear information on redress and compensation in the event that their data is lost, shared or stolen and with easy- to- use methods for making such claims.

The Trans Atlantic Consumer Dialogue also urges businesses and governments that outsource individuals' data to the cloud to consider these issues and ensure that their contracts for cloud computing services provide for adequate protection. In these instances, businesses and governments should be fully accountable to those individuals for the privacy and security of their data.

Background

Cloud computing has been defined as "the sharing and storage by users of their own information on remote servers owned and operated by others and accessed through the Internet or other connections."[1] There are many popular cloud-based consumer services available in the U.S. and the EU, including webmail (such as Gmail and Hotmail), photo sharing websites (such as Flickr), and social networking sites (such as Facebook, MySpace and Badoo). Convenience is a major reason why consumers use cloud computing; it enables them to access their data from any computer and share it with others easily.[2] Cloud computing services can also protect consumers from loss of data if their computers fail and may offer better data security than they have on their own computers.

While the use of cloud computing services can benefit consumers, it also raises many concerns. These concerns focus mainly on control of the data. Once consumers' data is entrusted to a cloud computing service, it may be accessed and used by the cloud service provider or third parties for a variety of purposes unrelated to fulfilling the services that the consumers have requested. Consumers may have no idea, however, that their data may be accessible to parties

[1] See World Privacy Forum, *Cloud Computing and Privacy*, www.worldprivacyforum.org/cloudprivacy.html.
[2] John Horrigan, *Use of Cloud Computing Applications and Services*, Pew Research Center's Internet & American Life Project, www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx.

to whom they have not specifically provided it, for uses beyond the purposes for which it was originally given. For instance, the data may be sought by the government or others for criminal or civil litigation, or cloud service providers may want to access consumers' data for their own commercial use or to sell it to others.[3]

In the U.S., federal law does not provide adequate protection for the privacy of data in the cloud. While data stored in a consumer's own hard drive is protected from government access by Fourth Amendment rights, requiring a judge's permission in most cases, the same data may lose that protection when transferred to a third party such as a cloud computing service. In a report for the World Privacy Forum, Bob Gellman describes the confusing legal landscape under the Electronic Communications Privacy Act of 1986 as it applies to current Internet activities.[4] He also points out that since the U.S. lacks an overarching legal privacy framework and relies on a narrow sectoral approach, consumers may have no rights concerning the secondary use and sharing of the data that they place in the cloud. While in Europe the EU Data Protection Directive[5] and the Directive on privacy and electronic communications[6] provide a comprehensive privacy framework, the European Network and Information Security Agency (ENISA) recommended in its recent cloud computing risk assessment that European officials should determine how the data protection laws apply to cloud computing services.[7]

Consumers are clearly concerned about the privacy of their data in the cloud. According to one survey,[8] 90 percent of respondents said that they would be very concerned if cloud providers sold their files to others, and 80 percent said they would be very concerned if the service used their photos and other information for marketing. Sixty-eight percent said they would be very concerned if the data was used to tailor advertisements to them.

Data that consumers store in the clouds should have the same legal protections with regard to access by government and others as it would if it was stored on consumers' own computers. To the extent appropriate, consumers should receive notice of criminal and civil requests for data that they have stored with cloud computing services before such requests are fulfilled. Furthermore, consumers' data should not be used by cloud computing services or others for secondary purposes without first explaining those uses and obtaining consumers' express affirmative consent.

Portability is also an important consumer concern. While there may be no contractual barrier to switching from one cloud computing service to another, providers could use proprietary formats or employ technical obstacles to make it difficult to do so. For instance, a consumer might be required to select each file individually to download. For consumers who have spent years uploading data, this could effectively make the service non-portable, locking them in and

---

[3] See Alan Weissberger, *ACLU Northern CA: Cloud Computing – Storm Warnings for Privacy?* Viodi View, http://viodi.com/2009/02/13/aclu-northern-ca-cloud-computing-storm-warning-for-privacy.

[4] Bob Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, 2009, www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF

[7] See www.enisa.europa.eu/act/it/oar/cloud-computing/

[8] See fn 2 supra.

threatening competition. Interoperability is a related issue; unless standardized data formats are used, it might be hard for consumers to use data that they have customized on one service with another service. Cloud computing services should not interfere with consumers' ability to move their data to another service or to use their data in an interoperable manner with other services.

Once consumers entrust their data to the cloud, they must rely on the cloud service provider to keep it secure. One potential benefit to consumers is that the security that the cloud service provider employs may be even stronger than they have on their own computers. Consumers can have no confidence about the security of cloud services, however, unless those services are required to meet adequate security standards and to be independently audited on a regular basis to ensure compliance. Cloud computing services should provide consumers with information about their security. In addition, cloud computing services should provide consumers with the means to safeguard their data through tools such as encryption for which only the consumers themselves have the keys. While the location of the servers that cloud computing services use can actually enhance the protection of consumers' data, cloud computing services should not be allowed to exploit the physical locations of their servers in order to limit consumers' rights concerning the privacy and security of their data.

Consumers should have the right to delete data that they upload to the cloud. To address the fact that sometimes consumers regret deleting data, the Norwegian Consumer Council's best practices standard for cloud storage of photographs may serve as a good model: it recommends that customer files and metadata be quarantined for a period before actually being deleted.[9]

Transparency is a guiding principle for all consumer transactions: consumers cannot make informed choices without understanding exactly what is being offered and on what terms. Many cloud services' terms of service, however, are unclear and missing important information.[10] Information about cloud services' business models is also important; if services are based primarily on monetizing the secondary use of consumers' data that should be made clear. Other key information that should be provided includes what countries' laws apply, who the primary regulatory agencies are, what the termination policy is, and whom to contact if consumers have questions or complaints.[11] This information should be prominently disclosed in clear, easy to understand language.

Another concern is the fairness of terms of service. Many consumer contracts, including those for cloud computing, are one-sided agreements in which the providers disclaim any liability if things go wrong, reserve the right to change terms unilaterally, and require that disputes be resolved through privately-operated arbitration that is binding on consumers.[12] Unfair contract terms for cloud computing services should be prohibited. For instance, cloud service providers

---

[9] See http://forbrukerportalen.no/Articlker/2010/standard_for_secure_online_photo_storage.

[10] Simon Bradshaw, Christopher Millard, and Ian Walden, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, Queen Mary School of Law Studies Research Paper No. 63/2010, http://ssrn.com/abstract=1662374.

[11] See model disclosure form in Appendix B, *Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing*, November 2010, www.consumerfed.org/pdfs/Cloud-report-2010.pdf.

[12] See fn 7 supra.

should not be allowed to disclaim responsibility if they lose consumers' data, or to suddenly terminate services without notice and giving consumers sufficient time to retrieve their data. Furthermore, terms of service should not require consumers who use free services to agree to a lower level of protection than those who pay or require that consumers give up the right to take legal action to resolve disputes. Cloud computing services should provide consumers with clear information on redress and compensation in the event that their data is lost, shared or stolen and with easy- to- use methods for making such claims.