available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Privacy and consumer risks in cloud computing

Dan Svantesson, Roger Clarke

Keywords:
Cloud computing
Consumers
Transborder privacy
Privacy Act 1988 (Cth)
Personal information
Google docs
Privacy policy

ABSTRACT

While vaguely defined, and wide in scope, so-called 'cloud computing' has gained considerable attention in recent times. Put simply, it refers to an arrangement under which a user relies on another party to provide access to remote computers and software, whose whereabouts, including their jurisdictional location, are not known nor controllable by the user. In this article, we examine the privacy and consumer risks that are associated with cloud computing.

1. Introduction

Anyone with an interest in information technology would have found it virtually impossible to avoid coming across the term 'cloud computing' in recent times. While vague and wide in scope, there seems to be a consensus that the term cloud computing typically refers to a technical arrangement under which users store their data on remote servers under the control of other parties, and rely on software applications stored and perhaps executed elsewhere, rather than on their own computers. For this paper, we adopt the definition devised by the second author in an earlier paper:

Cloud computing refers to a service that satisfies all of the following conditions:[1]

- The service is delivered over a telecommunications network;
- Users rely on the service for access to and/or processing of data;
- The data is under the legal control of the user;
- Some of the resources on which the service depends are 'virtualised', which means that the user has no technical need to be aware which server running on which host is delivering the service, nor where the hosting device is located; and
- The service is acquired under a relatively flexible contractual arrangement, at least as regards the quantum used.

While hailed as a new era, cloud computing has gained only a limit amount of attention from a legal regulatory perspective. Yet cloud computing is associated with a range of obvious privacy and consumer risks, such as risks relating to:

- How data provided to a cloud computing operator will be used by that operator;
- How such data will be disclosed by the cloud computing operator, and subsequently used by third parties;
- The security of the data provided;
- The legality (under the consumer's local law) of using cloud computing products;
- Disruptions of the cloud computing service;
- Getting locked into a contractual arrangement that does not cater for the consumer's future needs; and
- Violating privacy laws by the use of cloud computing products.

In this paper, we discuss those, and related, risks.

2. Privacy risks

Cloud computing is associated with a range of severe and complex privacy issues. In this section, we discuss the privacy concerns that are associated with cloud computing and how different cloud computing structures give rise to

[1] Roger Clarke, 'User Requirements for Cloud Computing Architecture', (Forthcoming, Proc. 2nd Int'l Symposium on Cloud Computing, Melbourne, IEEE CS Press, May 2010) <http://www.rogerclarke.com/II/CCSA.html> at 31 January 2010.

0267-3649/$ – see front matter © 2010 Svantesson & Clarke. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2010.05.005

different types of privacy concerns. It extends beyond mere compliance with data protection laws to encompass public expectations and policy issues that are not, or not yet, reflected in the law.

Several early privacy analyses have been published variously by a Privacy Commissioner,[2] an industry association,[3] a news service,[4] an IT provider,[5] and a commercial publisher.[6] At least one privacy advocacy organisation maintains a resource-page,[7] and at least one has issued a policy statement on the matter.[8]

The starting point of any privacy discussion regarding cloud computing must be the realisation that several forms of cloud computing are in their infancy. In other words, in many cases we are dealing with immature technological structures. As a consequence, operators of such cloud computing structures must undertake appropriate Privacy Impact Assessments (PIAs)[9] before launching their product. Further, organisations, businesses and individuals interested in utilising cloud computing products must ensure they are aware of the privacy and security risks associated with using the product and take those risks into account when deciding whether to use it. For anyone intending to use a cloud computing product on a commercial basis, or otherwise to store other individuals' personal information, this should involve undertaking a PIA before adopting cloud computing techniques. Cloud computing products must not be used for such purposes unless the user of the product can ensure that privacy and security risks are satisfactorily addressed and privacy laws are complied with. As has been noted in a briefing paper by the Organisation for Economic Co-operation and development:

Companies that wish to provide Cloud services globally must adopt leading-edge security and auditing technologies and best-in-class practices. If they fail to earn the trust of their customers by adopting clear and transparent policies on how their customers' data will be used, stored, and protected, governments will come under increasing pressure to regulate privacy in the Cloud.[10]

To provide a useful discussion of the specific privacy issues that arise from cloud computing, it is necessary to separate two distinct cloud structures:

- Domestic clouds; and
- Transborder clouds.

Where the entire cloud is physically located within one and the same jurisdiction, we can talk of a domestic cloud. Domestic clouds will obviously not give rise to any cross-border issues. However, such clouds can still give rise to privacy issues such as:

- Whether the collection of data is carried out in an appropriate manner;
- Whether the data is used appropriately;
- Whether the data is disclosed only where disclosure is appropriate;
- Whether the data is stored and transmitted safely;
- How long the data will be retained for;
- The circumstances under which the data subject can access and correct the data; and
- Whether the data subject is sufficiently and appropriately informed about these matters.

These matters must be considered in all cloud computing situations, whether the cloud is domestic or not.

Transborder clouds are associated with additional privacy issues, and in approaching those privacy issues, it is useful to draw a distinction between:

- Issues associated with transborder cloud operators (such as, for example, Google); and
- Issues associated with transborder cloud users (such as, for example, a bank using a transborder cloud computing product in relation to customer information).

While the legal issues facing cloud operators and cloud users stem from the fact that personal data is transferred across jurisdictional borders, applicable privacy regulation typically draws a line between data being transferred *within* an organisation, and data being transferred *between* organisations.

Where a cloud operator transfers data across borders, the data remains in the cloud operator's control and is not transferred to any third party. This is, for example, the case where an individual uses *Google Docs* to store her/his documents in the cloud.

In such a situation, privacy principles regulating transborder data flows may not be applicable as they typically require the transfer to be to another organisation. For example, National Privacy Principle 9, which is Australia's current privacy provision dealing with transborder data flows,

[2] A Cavoukian, *Privacy in the Clouds: A White Paper on Privacy and Digital Identity*, Information and Privacy Commissioner of Ontario 2009, at <http://www.ipc.on.ca/images/Resources/privacyintheclouds.pdf>.

[3] R Gellman, 'Cloud Computing and Privacy' (Presented at the World Privacy Forum, 2009) at <http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf>.

[4] Leslie Harris, *Perils in the Privacy Cloud* (2009) ABC News, 15 Sep 2009 <http://abcnews.go.com/Technology/AheadoftheCurve/privacy-evaporates-computing-cloud/Story?id=8573715&page=1>.

[5] Microsoft, *Privacy in the Cloud Computing Era - A Microsoft Perspective* (2009) Microsoft Trustworthy Computing <http://download.microsoft.com/download/3/9/1/3912E37E-5D7A-4775-B677-B7C2BAF10807/cloud_privacy_wp_102809.pdf>.

[6] Tim Mather, Subra Kumaraswamy and Shahed Latif, Cloud Security and Privacy: AnEnterprisePerspective on Risks and Compliance (2009).

[7] Electronic Privacy Information Centre (EPIC), *Resources on Cloud Computing* (2009), <http://epic.org/privacy/cloudcomputing/>.

[8] Australian Privacy Foundation (APF) *Policy Statement re Cloud Computing* (2009) <http://www.privacy.org.au/Papers/CloudComp-0911.html>.

[9] Roger Clarke, 'Privacy Impact Assessment: Its Origins and Development' (2009) 25(2) *Computer Law & Security Review* 123 <http://www.rogerclarke.com/DV/PIAHist-08.html>. See also Roger Clarke, 'Privacy Impact Assessments' (1999) <http://www.rogerclarke.com/DV/PIA.html>.

[10] OECD (2009) Briefing Paper for the ICCP Technology Foresight Forum (14 October 2009) <http://www.oecd.org/dataoecd/39/47/43933771.pdf>.