7-1-2010

Privacy and consumer risks in cloud computing

Dan Svantesson
Bond University, Dan_Svantesson@bond.edu.au

Roger Clarke

Privacy and consumer risks in cloud computing

Dan Svantesson and Roger Clarke

Abstract:

cloud computing – consumers – transborder privacy –Privacy Act 1988 (Cth) *– personal information – Google Docs – privacy policy*

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.

---

[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.

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 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

[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>.

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:

---

[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: An Enterprise Perspective 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>.

> 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.

---

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

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, is only applicable if the transfer is to a third-person. Similarly, while the details are unclear, it seems that any future Australian privacy principle that regulates transborder data flows will not be applicable where the data is transferred across borders but within the same organisation.[11]

In the situation outlined above, any privacy protection will be provided through an extraterritorial application of the relevant privacy legislation. In other words, the relevant legislation is applied to the conduct of a foreign actor, to its acts carried out outside the territory of the country in question. Continuing using Australian law as an example, we can note that the jurisdictional scope of the *Privacy Act 1988* (Cth) extends in an extraterritorial manner. Section 5B makes clear that the Act is applicable in relation to an act done, or practice engaged in, outside Australia by an organisation, provided that certain requirements are met. Those requirements relate both to the organisation in question and the data subject.

---

[11] See first stage Government response to the ALRC report: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2009) <http://www.dpmc.gov.au/privacy/alrc_docs/stage1_aus_govt_response.doc> at 18 January 2010.

First, the Act only has extraterritorial effect where the act or practice relates to personal information about an Australian citizen or another person whose continued presence in Australia is not subject to a limitation as to time imposed by law.[12] Second, the extraterritorial effect is limited to situations where the organisation in question has a strong link with Australia, for example, by carrying on business in Australia.[13]

Even leaving aside these limitations, extraterritorial application of privacy laws risk being ineffective due to the difficulties associated with cross-border enforcement.[14] While the Organisation for Economic Co-operation and Development (OECD) is currently carrying out important work to strengthen cross-border cooperation in relation to the enforcement of privacy laws,[15] the simple fact is that today, it is extremely difficult for victims of privacy violations to obtain redress where the violation has occurred outside the victim's home country.

Further, like any extraterritorial claim of jurisdiction, the extraterritorial application of privacy laws is not entirely uncontroversial. As a result extraterritorial claim of jurisdiction, providers of cloud computing products are exposing themselves to the laws of all countries from which the products are used – potentially a heavy burden indeed. Consider, for example, the legal situation of cloud computing services such as Google Docs or Microsoft's Hotmail. Both these services are being utilised by individuals virtually globally, and due to the threat of extraterritorial application of the laws of the countries from which those individuals access the services, Google and Microsoft need to take account of the laws of all the countries from which they have users. This may seem unreasonable. On the other hand, it can also be argued that where an organisation is seeking to profit from a marketplace, it is reasonable that the organisation abides by the laws of that marketplace. The controversy obviously stems from the fact that we are here dealing with a virtually global marketplace.

---

[12] *Privacy Act 1988* (Cth), s. 5B(1)(a).
[13] *Privacy Act 1988* (Cth), s. 5B(3)(b).
[14] Dan Svantesson, 'Protecting Privacy on the "Borderless" Internet – Some Thoughts on Extraterritoriality and Transborder Data Flow' (2007) 19(1) *Bond Law Review* 168. <http://epublications.bond.edu.au/blr/vol19/iss1/7>.
[15] See further: <http://www.oecd.org/document/25/0,3343,en_2649_34255_37571993_1_1_1_1,00.html>.

However, these issues are neither new, nor uniquely associated with cloud computing. In fact, the same dilemma has been the object of intense debate for many years in the context of globally accessible websites.[16]

Where a cloud computing user uses a transborder cloud computing product in relation to customer information, it will have to abide by regulations aimed at restricting the instances where transborder data flows are allowed. Thus, for example, where a health care provider uses a transborder cloud computing product to store and/or process patient data,[17] they would have to ensure that the transfer is permitted under the relevant privacy law.

Perhaps the most well-known example of such regulation is found in EU Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article 25 of that Directive makes clear that:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

This type of provision severely limits the circumstances and manner in which transborder cloud computing can be used, as it necessitates that the users of cloud computing products are able to ascertain the cloud's geographical location. Indeed, this highlights a fundamental tension between the law's focus on geographical locations and the ubiquitous nature of cloud computing. This tension may very well represent the largest obstacle to a widespread adoption of cloud computing.

Imagine, for example, that a European company is considering adopting a cloud computing product such as Google Docs. To assess whether the company could do so, it would need to know in which country, or countries, its data would be stored – it would need to know the location of the cloud. Only then could it assess whether the country/ies in which the cloud is located provide(s) an adequate level of protection, and thereby satisfy the requirement of Article 25 outlined above.

---

[16] Dan Svantesson,'Borders On, Or Border Around – The Future of the Internet' (2006) 16(2) *Albany Law Journal of Science & Technology* 343 <http://epublications.bond.edu.au/law_pubs/16>.
[17] Kim Zetter, *Medical Records: Stored in the Cloud, Sold on the Open Market* (2009) Wired <http://www.wired.com/threatlevel/2009/10/medicalrecords/>.

The question is then whether the provider of the cloud computing product (1) is able to limit the location the data will be stored with sufficient specificity, and (2) is willing to do so. If the company wishing to start using the cloud computing product is sufficiently large, it may be able to negotiate these matters with the provider. However, it is unlikely that cloud computing providers would be inclined to negotiate each contract individually.

It cannot be expected that the law will change so as to remove the requirement expressed in Article 25, and indeed, provisions such as Article 25 play a crucially important role in privacy protection. Consequently, the way forward seems to be for cloud computing providers to develop products that are geographically limited. Continuing using the example above, Google should make it possible for the European company to opt to have its data stored on servers within the European Union only.

Furthermore, cloud computing is an interesting setting to observe the interaction between the law and technological developments. On the one hand, regulations such as these, while aimed at sound goals, will inevitably restrict the development of technologies such as cloud computing. On the other hand, technologies such as cloud computing may highlight needs for modernisation of this type of regulation. For example, Article 25 of EU Directive 95/46 is focused on transfer to a third *country*. This opens the door for clouds over international spaces – cloud computing products located in international spaces beyond individual countries' control, such as the high seas. While the idea of data havens in intentional spaces may seem far-fetched, attempts have in fact already been made to establish hosting facilities beyond the reach of any country's jurisdiction.[18] Further, Google is pursuing the idea of offshore data storage centres.[19] Consequently, the risk is not as remote as might first be thought.

To gain an understanding of the privacy policies users of cloud computing products are exposed to, we have examined the Google Docs' Privacy Policy, which must be read in conjunction with Google's general Privacy Policy.[20] In so doing, we found several noteworthy provisions. For example:

> Google's servers automatically record certain information about your use of Google Docs. Similar to other web services, Google records information such as account activity (e.g. storage usage, number of

[18] Simson Garfinkel, *Welcome to Sealand. Now Bugger Off* (2000) Wired Issue 8.07 <http://www.wired.com/wired/archive/8.07/haven.html>.
[19] Rich Miller, *Google Planning Offshore Data Barges*, (6 September 2008) Data Centre Knowledge <http://www.datacenterknowledge.com/archives/2008/09/06/google-planning-offshore-data-barges/>.
[20] For an analysis, see: Roger Clarke, 'Evaluation of Google's Privacy Statement Against the Privacy Statement Template of 19 December 2005' (2005) <http://www.rogerclarke.com/DV/PST-Google.html>.

> log-ins, actions taken), data displayed or clicked on (e.g., UI elements, links), and other log information (e.g. browser type, IP address, date and time of access, cookie ID, and referrer URL).[21]

While details are provided about some types of data being collected, the reference to 'certain information about your use of Google Docs' being recorded is very vague, and it is not clear whether the specified types of data are the only types of data collected, or merely examples of the types of data being collected. Another vague part of the Google Docs Privacy Policy relates to third-party providers: 'Some features (e.g. gadgets) are provided by third parties, who may receive and process your data. When you use one of these features, you may be sharing data with the third party, including allowing the third party to process your data.'[22] This statement may work as a warning, but due to its vagueness, it does not equip users with the information necessary to understand the threats to their privacy, nor with the tools needed to take steps to protect it.

Furthermore, Google makes clear that they may combine the information that consumers submit under their accounts with information from other Google services or third parties. This means that Google can construct user profiles of extraordinary precision and detail. This is all the more serious when taking account of the fact that Google shares personal information with other companies and individuals outside of Google in certain circumstances.[23]

Interestingly, Google takes the view that, 'information that is already available elsewhere on the Internet or in public records' is not to be regarded as private or confidential.[24] While Google's approach to information available in public records is conventional, and in line with privacy laws of many countries, the fact that Google treats information available elsewhere on the Internet in the same manner is problematic, as not all content on the Internet is meant to be accessed by the public.

Finally, it is worth noting that:

---

[21] Google Docs Privacy Policy (version of 30 October 2009) <http://www.google.com/google-d-s/intl/en/privacy.html> at15 January 2010.
[22] Ibid.
[23] Privacy Policy (version of 11 March 2009) <http://www.google.com/privacypolicy.html> at 15 January 2010.
[24] Privacy and Security: Program Policies (no version number available) <http://docs.google.com/support/bin/answer.py?hl=en&answer=148505> at 15 January 2010.

- Google is registered with the U.S. Department of Commerce's Safe Harbor Program, and 'adheres to the US Safe Harbor Privacy Principles of Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement';[25]

- Consumers must be aware that their data may remain in Google's possession even after the consumer has deleted the files: 'residual copies of your files may take up to 30 days to be deleted from our active servers and may remain in our offline backup systems for up to an additional 60 days.';[26] and

- Google's Privacy Policy may change from time to time, and Google does not undertake to notify users where changes take place.[27] The legality of this approach is discussed in detail below.

Our analysis of Google Docs' Privacy Policy and related documents show that a user can gain only a very limited understanding of how her/his personal information may be used by Google and of where the data might reside. While the vague language used by Google is easily understandable from a commercial perspective, it seriously undermines the legitimate privacy rights of individual users.

3. Consumer Risks

This section considers the risks to consumers that arise from the use of a cloud computing service. Drawing upon relevant parts of the normative template previously developed and applied by the authors,[28] it also examines the legal issues that are associated with those risks.

Bearing in mind that cloud computing is associated with some rather obvious risks, as mentioned above, the first step for consumers wishing to use a particular cloud computing product is to

[25] Above, n 24.
[26] Above, n 25.
[27] Above, n 24.
[28] Dan Svantesson and Roger Clarke,'A Best Practice Model for eConsumer Protection' (2010) 26(1) *Computer Law & Security Review* 31; Roger Clarke, 'B2C Distrust Factors in the Prosumer Era' (Proc. CollECTeR Iberoamerica, Madrid, 25-28 June 2008) <http://www.rogerclarke.com/EC/Collecter08.html> and Roger Clarke, 'A Major Impediment to B2C Success is ... the Concept "B2C"' (Proc. ICEC '06, Fredericton NB, Canada, 14-16 August 2006) <http://www.rogerclarke.com/EC/ICEC06.html>.

familiarise themselves with the product. They must make sure that the product is suitable for their needs, and that the risks of use are understood.

At the same time, consumers cannot possibly predict all the risks they take in using cloud computing products. While the relevant privacy risks are discussed in more detail in the preceding section, a privacy example is illustrative of this point. Currently, it is unclear whether a person in Europe, who uploads personal information about another individual onto her/his *Facebook* page, violates EU Directive 95/46 if the person who uploads the information has 'friends' outside the EU.[29] The law is simply not clear enough for anyone to know the legal status of such an act, and consumers must understand that such 'hidden risks' exist.

Like virtually all other consumer products on the Internet, the supply of consumer cloud computing products is typically governed by contracts drafted exclusively by the providers with no input from consumers. There are several practical reasons for this approach, but to provide some balance between the parties, the law often places some restrictions on such contracts.

For example, such restrictions include laws relating to mandatory information disclosure about the product and/or provider,[30] misleading and deceptive conduct,[31] and misrepresentations.[32] Others relate to the circumstances of contract formation, such as laws relating to mistake,[33] undue influence,[34] duress,[35] illegality,[36]capacity,[37] and unconscionable conduct.[38] Yet other such restrictions relate to the content of the contract, and the interpretation of that content, such as laws relating to:

---

[29] Dan Svantesson, 'Privacy, the Internet and Transborder Data Flows – An Australian Perspective' (Cyberspace 2009: Masaryk University, Brno, Czech Rep).
[30] See e.g. Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Articles 5 and 6.
[31] See e.g. *Trade Practices Act 1974* (Cth), s. 52.
[32] Ibid s. 53.
[33] See e.g. Dan Svantesson, *Svantesson on the Law of Obligations* (2nd ed, 2009), 146-160.
[34] Ibid 175-183.
[35] Ibid 161-168.
[36] Ibid 242-261.
[37] See e.g. Willmott et al., *Contract Law* (3rd ed, 2009), 331-359.
[38] Above n 32, s. 51AB.

- Unfair contractual provisions;[39]
- Implied or imposed terms;[40]
- *Contra proferentem* and *contra stipulatorem* rules;[41] and
- Unconscionability.[42]

All of these consumer protection measures affect providers of consumer cloud computing products.

A particularly interesting issue arising in this context is the extent to which cloud computing providers will/should be liable for issues such as service outages and loss of data. There can be little doubt that providers of cloud services will seek to exclude liability for such events, howsoever caused. However, many countries have taken a protective approach towards consumers, with the result that attempts to exclude such liability may be ineffective. For example, Australian law imposes[43] a term into Business-to-Consumer (B2C) contracts to the effect that a service must be rendered with due care and skill.[44] Further, where a consumer makes known any particular purpose for which the services are required, or results that the services ought to achieve, there is an implied warranty that the services will be reasonably fit for that purpose or are of such a nature and quality that they might reasonably be expected to achieve that result.[45] While consumers cannot contract out of these rights[46] and thereby enjoy a relatively good level of protection, they may encounter difficulties when trying to identify the responsible party in the cloud, in order to enforce the imposed term.

[39] See e.g. Council Directive 93/13/EEC on unfair terms in consumer contracts.
[40] Above n 32, ss. 69, 70, 71, 72 and 74.
[41] See e.g. *Maye v CML* (1924) 35 CLR 14.
[42] Above n 39.
[43] The term 'implies' is more commonly used, but as the parties to the contract cannot contract out of the provisions in question, the term 'impose' is more accurate.
[44] Above n 32, s. 74(1).
[45] Ibid s. 74(2).
[46] Ibid, s.68.

Another matter that is likely to be a source of disputes in relation to consumer cloud computing products is where the provider seeks to vary the terms on which the product is provided. Such changes may not be permitted where they are unilateral.[47]

Furthermore, it can be expected that there will be clashes between the contractual terms prepared by the providers of consumer cloud computing products on the one hand, and limitations placed on choice of forum and choice of law clauses imposed by some law makers on the other hand. For example, European consumers enjoy the right to always take action against a business in their home jurisdiction[48] and under the laws of home jurisdiction.[49] This undermines choices made by the provider in the contract.

While we, above, encouraged consumers to familiarise themselves with the cloud computing product they wish to use, we also acknowledge that doing so is not always an easy undertaking. For example, when considering using *Google Docs*, one ought to read at least Google's:

- Universal Terms of Service;
- Additional Terms;
- Program Policies;
- Privacy Policy; and
- Copyright Notices.

Together, those documents are approximately as long as this paper. In addition they provide links to further materials that a prudent consumer ought to take into account. Few consumers will take the necessary time to familiarise themselves with this wealth of information.

We have, however, examined the documents listed immediately above in order to gain an understanding of the consumer policies users of cloud computing products are exposed to (our privacy-specific observations are outlined above). Several interesting features became apparent from

[47] See e.g.: Council Directive 93/13/EEC on unfair terms in consumer contracts.
[48] Brussels I Regulation 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.
[49] Rome I Regulation 593/2008 on the law applicable to contractual obligations.

the examination. First, to use any of Google's services, a consumer has to agree to be bound by a range of terms unilaterally decided by Google,[50] and those Terms may be unilaterally changed by Google without specific notification.[51] In the same vein, Google also makes clear that they, without giving prior notice, may change[52] or stop providing[53] their services. As discussed above, it is uncertain whether this type of contractual provision is effective in light of laws regulating unfair contractual terms.

Somewhat similarly, despite the legal uncertainty as to the validity of the approach, Google states that they will treat a consumer's use of their services as an acceptance of the terms included in Google's contract.[54] In other words, while most consumers will not have read the terms, may not even be aware of the terms, and have not signalled their agreement to the terms, Google argues that consumers are bound by the terms.

Furthermore, contrary to the EU approach to choice of law and choice of forum in consumer contracts, users of Google Docs are informed that their contract with Google is 'governed by the laws of the State of California',[55] and that the courts within the county of Santa Clara, California, will have exclusive jurisdiction.[56]

The Terms for Google Docs also make clear that:

> By submitting, posting or displaying the Content you give Google a worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through the Service for the sole purpose of enabling Google to provide you with the Service in accordance with its Privacy Policy.[57]

---

[50] Google Terms of Service, 2.1 (version of 16 April 2007) <http://www.google.com/accounts/TOS> at 15 January 2010.
[51] Ibid 19.1 and 19.
[52] Ibid 4.2.
[53] Ibid 4.3
[54] Ibid 2.2(B).
[55] Ibid 20.7.
[56] Ibid.
[57] Additional Terms for Google Docs (no version number available) <http://www.google.com/google-d-s/intl/en/addlterms.html> at 15 January 2010.

This far-reaching provision may perhaps surprise some users. Another far-reaching provision makes clear that consumers agree to be 'solely responsible to Google for all activities that occur under' their account.[58] This may or may not be reasonable depending on how tightly Google ensures the security of the accounts.

Further, we note that:

- Where Google disables access to a consumer's account, the consumer may be prevented from accessing files and other content contained in the account.[59] This is particularly serious in relation to services such as Google Docs;

- Consumers undertake to indemnify, and even defend, Google if claims arise due to some specified forms of use of Google Docs;[60]

- Google states that consumers are not allowed to use their services unless they are 'of legal age to form a binding contract with Google.'[61] This provision means that a relatively large section of those who use Google's services are in fact in violation of the Terms of Service;

- Google reserves the right to target advertisement to consumers using their services, based on the 'information stored on the Services, queries made through the Services or other information'.[62] The reference to unspecified 'other information' is particularly concerning, and may in fact be contrary to the privacy laws of some jurisdictions; and

- In using Google's services, consumers must abide by any applicable law, 'including any laws regarding the export of data'.[63] As discussed below, for consumers to familiarise themselves with complex areas of law, such as the laws regarding the export of data, may be a considerable burden, and may not be possible.

---

[58] Above n 51, 6.2.
[59] Ibid 4.4.
[60] Above n 58.
[61] Above n 51, 2.3.
[62] Ibid 17.1.
[63] Ibid 5.2.

Finally, and not surprisingly, Google excludes liability to the extent allowed under the law of the consumer's jurisdiction.[64]

Overall, it is clear that users of Google Docs, knowingly or unknowingly, agree to a range of terms that may have serious consequences. The legality of some of those terms is questionable.

4. Concluding remarks

This article has highlighted that so-called cloud computing is associated with serious risks to privacy and consumer rights, and that current privacy law may struggle to address some of those risks. It has also highlighted that consumers using cloud computing products, like other cloud computing users, need to be cautious. The article should also have sent a warning that providers of cloud computing products would do well to familiarise themselves with applicable consumer protection and privacy laws – a very difficult task where they are marketing, or otherwise making available, their products globally and thereby expose themselves to the diverse laws of multiple countries.

Finally, in the article we have also highlighted that the tension between the law's focus on geographical locations and the ubiquitous nature of cloud computing may represent the largest obstacle to a widespread adoption of cloud computing.

About the authors

Dr Dan Svantesson is an Associate Professor, Faculty of Law Bond University, Gold Coast Queensland 4229 Australia, Ph: +61 7 5595 1418, E-mail: Dan_Svantesson@bond.edu.au, (www.svantesson.org).

Dr Roger Clarke is principal of Xamax Consultancy Pty Ltd, Canberra. He is also a Visiting Professor in the Cyberspace Law & Policy Centre at the University of N.S.W., and a Visiting Professor in the Department of Computer Science at the Australian National University.

---

[64] Ibid 14 - 15 14 – 15 (version of 16 April 2007, http://www.google.com/accounts/TOS last accessed 15 January 2010).