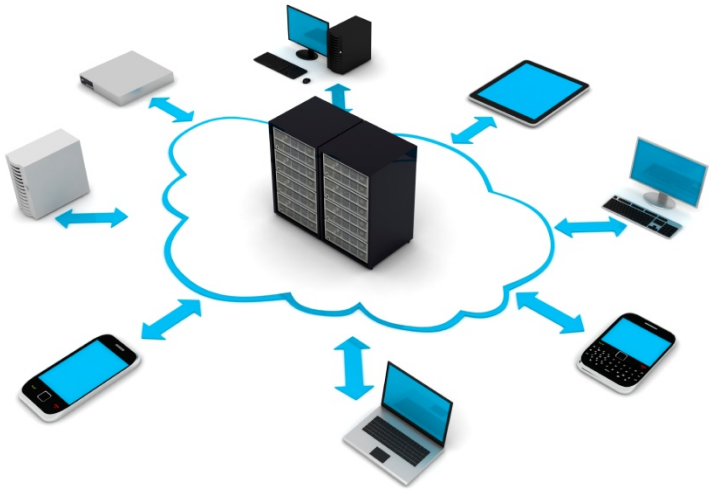
LAW SOCIETY
OF SOUTH AFRICA

LSSA Guidelines on the Use of Internet-Based Technologies in Legal Practice



Drafted for the Law Society of South Africa by the LSSA E-Law Committee

Use of Internet-Based Technologies in Legal Practice

LSSA Guidelines

Version 1.0

6 March 2015

Foreword

Please read this foreword carefully

This guideline has been compiled to provide background information and to serve as a tool to assist attorneys in South Africa.

The views, conclusions and recommendations contained in this guideline are not to be regarded or construed as legal advice or as establishing any standard or legal obligation.

Reliance on the contents of this document is at the reader's own will. Neither the LSSA, any of its [employees?], or any member of the E-Law Committee shall be liable for any loss or damage arising in any way from use of or reliance on the contents on this whitepaper.

LSSA GUIDELINES ON THE USE OF INTERNET-BASED TECHNOLOGIES IN LEGAL PRACTICE

EXECUTIVE SUMMARY

When making use of Internet-based technologies in legal practice, lawyers should exercise due diligence before utilising a third-party service provider for purposes of storing or processing confidential information offsite. In addition, a written agreement should be concluded that requires the service provider to establish and maintain measures that ensure the security of any personal information stored by the service provider as well as the protection and integrity of any confidential or privileged client information.

Introduction

"Cloud computing" is an expression used to describe a variety of different computing models that involve a number of computers connected via the Internet. The term is generally used to describe third party hosted services that run server-based software from a remote location.

Cloud computing is not new to the legal field. It has been around for a number of years and many lawyers would already be familiar with a number of cloud computing service providers, including web-based email service providers. Cloud computing offers flexible, affordable technologies that directly addresses a company's objectives and goals by providing required functionality, reducing overhead expenditure and increasing mobility and convenience.

While cloud computing offers many benefits, it also introduces several new risks that lawyers must take into consideration since cloud computing often means entrusting data to a third party.

Many foreign law societies and bar associations around the world have determined that lawyers may use cloud computing technologies in their law practice without compromising their ethical duties towards their clients, "*as long as the lawyer takes reasonable steps or reasonable protective measures to ensure that sensitive client information remains confidential*"[1].

[1] See for example the New Hampshire Bar Association, Ethics Committee Advisory Opinion #2012-13/4 "The Use of Cloud Computing in the Practice of Law" found at http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp

The general consensus internationally is that the use of cloud computing does not violate any ethical duty (and in many instances may go some way towards upholding them) provided that reasonable care is taken effectively to minimize any risks pertaining to the confidentiality and security of client information and client files[2] with the onus of evaluating a cloud provider's security infrastructure placed on the law firm or practitioner.[3]

In determining whether or not a lawyer has taken 'reasonable steps' or put into place 'reasonable protective measures', the facts and circumstances of each case should be taken into account, however guidance can be obtained from the Law Society of South Africa's previously published guides on information security and the protection of personal information[4].

Ethical Duties and Responsibilities Impacting on the Use of Cloud Computing

A number of ethical duties and responsibilities have been identified internationally that impact on the use of cloud computing technologies. Many of these follow on or support the main duty of a lawyer to take 'reasonable steps' to protect confidential client data. A summary of some of these internationally identified duties (and the law society which identified it) is set out below, including some ethical duties previously identified by the LSSA:

- To understand and guard against the risks inherent in the cloud by remaining aware of how and where data is stored and what the service agreement says, i.e. the duty of competence- (New Hampshire Bar Association)[5];
- To keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology - (American Bar Association)[6];

[2] See North Carolina State Bar, Proposed 2010 Formal Ethics Opinion 7, found at http://www.rocketmatter.com/blog/wp-content/uploads/2010/05/NC-Bar-Ethics-Decision-on-Cloud-Computing.pdf
[3] See the recently published opinions by the Florida Bar at http://tinyurl.com/ckp8mfp and the New Hampshire Bar Association at http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp
[4] "Information Security Guidelines for Law Firms" located at http://www.lssa.org.za/upload/Information%20Security%20Guideline%202011.pdf
[5] See note 1 above.
[6] See American Bar Association, revised comment to Model Rule 1.1 of the Model Rules of Professional Conduct, located at http://www.catalystsecure.com/blog/2013/03/latest-ethics-opinion-on-cloud-computing-emphasizes-duty-of-competence/

- To have a reasonable understanding of the technology and using it, or by seeking assistance from others who have the necessary proficiency – (Canadian Bar Association)[7];
- To keep abreast of, and understand, any advances in technology that genuinely relate to competent performance of the lawyer's duties to a client – (American Bar Association)[8];
- To engage in due diligence when using a third party service provider or technology for data storage and/or processing -(Law Society of British Columbia, Canada)[9];
- To ensure that the service provider and technology they use support the lawyer's professional obligations, including compliance with the Law Society's regulatory processes - (Law Society of British Columbia, Canada and New Hampshire Bar Association)[10];
- To conclude an agreement with the provider/operator of the services, where the information to be processed is personal information, to ensure that appropriate security for the protection of personal information is established and maintained – (Law Society of South Africa), once the Protection of Personal Information Bill has been enacted[11];
- To implement and provide appropriate information security for the information and communications processed by the lawyer – (Law Society of South Africa), once the Protection of Personal Information Bill has been enacted[12].

Duty of Competence

Lawyers have access to high volumes of information and what is undeniably an obligation of every lawyer today is the proper governance of such information.[13] We have moved from a paper and text environment to one of electronic records and communications and the proper governance of

[7] See Canadian Bar Association "Guidelines for Practicing Ethically with New Information Technology", a supplement to its "Code of Professional Conduct" located at http://www.cba.org/cba/activities/pdf/guidelines-eng.pdf
[8] See American Bar Association Commission on Ethics 20/20, Comment [6] to Rule 1.1 of the Model Rules located at http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac2013/sac_2013/36_the_ethical.authcheckdam.pdf
[9] See Law Society of British Columbia, Report of the Cloud Computing Working Group, January 2012 located at http://www.lawsociety.bc.ca/docs/publications/reports/CloudComputing_2012.pdf
[10] See note 8 above.
[11] "An Introduction to Cloud Computing" found at http://www.lssa.org.za/upload/LSSA%20Guidelines_Introduction%20to%20Cloud%20Computing%20-%20Legal%20Implications%202012.pdf.
[12] See note 11 above.
[13] See note 4 above.

maintaining confidentiality in electronic records and communications is hugely different to what is necessary in the text and paper environment.[14]

In a guidance note written by the Canadian Bar Association entitled "*Practicing Ethically with New Information Technology", a supplement to its "Code of Professional Conduct*", the following comment is pertinently made:

> "*To meet the ethical obligation for competence in Rule 2 (i.e. to perform any legal services undertaken on a client's behalf competently) lawyers must be able to recognise when the use of technology may be necessary to perform a legal service on that client's behalf and must use the technology responsibly and ethically.*
>
> *Lawyers must satisfy this duty by personally having a reasonable understanding of the technology and using it, or by seeking assistance from others who have the necessary proficiency"* [15].

The Law Society of South Africa has previously stated that *"attorneys are required to act reasonably and diligently in fulfilling their professional obligations"*[16]. The LSSA has stated further that *"one of these obligations must be that in using modern technology they do not compromise the rights of their clients arising from the attorney/client relationship"*.[17]

The LSSA has also previously clarified that it will likely not only be confidential legal data that is stored in the cloud but personal information too. Therefore, in accordance with the principles and objectives of the Protection of Personal Information Bill, there should be a written agreement concluded between the lawyer and the provider of the cloud computing services that requires the service provider to "establish and maintain measures that ensure that security of the personal information and protect the integrity and confidentiality of information"[18].[19]

[14] See note 4 above.
[15] See note 7 above.
[16] See note 4 above.
[17] See note 4 above.
[18] Section 21(2) of the Protection of Personal Information Bill.
[19] See note 11 above.

Hosting Information within South Africa

There are five key points of consideration when contemplating making use of a service provider to store and/or host electronic information.

1. **Inadvertent Waiver of Privilege**

   Discovery for litigation is becoming increasingly more efficient when electronic discovery platforms and service providers are used to manage and review the large numbers of the documents for pre-trial preparation. It is important to note that placing documents by a service provider on a database system for review does not amount to waiver of privilege, but sharing access to that database with opposing counsel may be a waiver of privilege if privileged documents are disclosed to opposing counsel.

   In *ThornCreek Apartments III, LLC v Village of Park Forest ND* Ill Aug 9 2011 the court applied the rules contained in the amended Federal Rule of Evidence Rule 502(b) which states that a disclosure of privileged information does not operate as a waiver if three elements are met:"*(1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error*". The court found that privilege had been waived where the vendor had produced privileged documents upon disclosure to the opposing counsel, and after holding that the attorney's procedures for privileged review were completely ineffective and the court had little confidence in the reasonableness of the attorney's precautions regarding disclosure.

   Lawyers need to be aware of the importance of taking reasonable steps to protect against inadvertent disclosure and to perform due diligence on potential service providers to ensure against inadvertent disclosure. A crucial point to take into consideration is that if documents are provided to a third party service provider who does not have in place the requisite security protocols, then inadvertent disclosure could also lead to an inadvertent waiver of privilege.

2. Hosting with a South African Service Provider

The use of cloud computing technologies is not inconsistent with a lawyers ethical duties provided that lawyers should exercise due diligence before utilising a third-party service provider for confidential data storage or information processing in the cloud. In addition, a written agreement should be concluded that requires the service provider to establish and maintain measures that ensure the security of any personal information stored by the service provider as well as the protection of the integrity and confidentiality of client information.

A South African lawyer should therefore look towards a SA hosted solution when considering the use of cloud computing services, for both their own and their client's needs, due to the advantages of hosting data with a South African headquartered company with South Africa servers which can offer clients a solution that avoids the reach of any extra territorial data seizures.

3. Foreign Jurisdiction (Safe Harbour – EU)

When using a cloud service provider not domiciled in South Africa, it is key to be aware of any foreign law which may be applicable under the circumstances for the use and storage of information electronically within that jurisdiction and when using a cloud service provider.

For example, the "European Union Directive on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data"[20] acts as a guideline for EU member states and requires that these states enact local data protection laws adopting the principles of data protection and privacy which are laid out in the Directive. As part of this formalised system of data privacy legislation, companies operating in the EU are not permitted to send personal data to countries outside of the member states[21] unless that state can guarantee that its local laws comply with the levels of data protection laid out in the Directive.

[20] Chapter 1, Article 4. Hereinafter referred to as the Directive. Found at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT
[21] Including countries that fall outside of the European Economic Area.

In order to assist the United States in meeting the EU data protection requirements a new framework, called the Safe Harbour Privacy Principles, has been developed and aimed at companies within the EU or US that stores customer data, in an attempt to protect such data by preventing accidental disclosure or loss of such personal information.[22] However the EU Commission conducted a review of this framework and on the 5 June 2013 adopted Opinion 06/2013[23] on open data and public sector information reuse, which in essence came to the conclusion that the Safe Harbour Privacy Principles may not be in actual fact be safe enough.

Lawyers looking to host data outside of South Africa should thus take these considerations into account and take note that your company will be subject to that particular country's laws surrounding the storing and monitoring of data. For example, Dropbox received requests for user information from the US government in relation to 164 user accounts in 2012[24].

For example, lawyers need to be aware that if they host data anywhere in the world with a US headquartered service provider then irrespective of where the data is hosted, the service provider will be obliged to disclose all data and client information upon the issuing by a federal court of a search warrant for such data in response to US investigations. This is a direct result of the judgment delivered in New York by US District Judge Loretta Preska on 31 July 2014[25], whose judgment has been stayed to allow the parties to appeal such ruling, however the implications are that data hosted with US companies is now subject to seizure by US investigators anywhere in the world.

[22] Wikipedia The Free Encyclopaedia "International Safe Harbour Privacy Principles". Found at http://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles

[23] Drafted by the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data set up by Directive 95/46/EC, having regard to Articles 29 and 30 of that Directive. Found at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf

[24] Loek Essers, "Dropbox pushes to publish spy data request details" found at http://www.pcworld.com/article/2049307/dropbox-joins-bid-to-publish-spy-data-requests.html

[25] See *In re: A Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp,* U.S. District Court, Southern District of New York, No. 13-mj-02814.

4. SARS

Lawyers need to maintain awareness of any relevant SARS ruling for electronic storage of accounting records.

For example, in Government Notice No 787[26] ("the Notice") the Commissioner for SARS prescribed that taxpayers are allowed to keep records, in terms of section 29 of the Tax Administration Act[27], in an electronic form, so long as the rules contained in the Notice are observed.

Rule 3.2 of the Notice defines an "acceptable electronic form" as a form in which '*the integrity of the electronic record satisfies the standard contained in section 14 of the Electronic Communications and Transactions Act*'. In addition, it is required that '*the person required to keep records is able to, within a reasonable period when called on by SARS, to provide SARS with an electronic copy of the records, in a format that SARS is able to readily access, read and correctly analyse, or to send the records to SARS in an electronic form that is readily accessible by SARS, or to provide SARS with a paper copy of those records*'.

Rule 4 requires that the '*records retained in electronic form must be kept and maintained at a place physically located in South Africa*'. Electronic documents may not therefore be retained outside of South Africa without a senior SARS official's authorisation and consent.

Rule 6 places a requirement on persons who keep records in an electronic format to '*ensure that measures are in place for the adequate storage of the electronic records for the duration of the period referred to in section 29 of the Act*', for a period of not less than 5 years.

[26] Found at http://www.sars.gov.za/AllDocs/LegalDoclib/SecLegis/LAPD-LSec-TAdm-PN-2012-01%20-%20Notice%20787%20GG%2035733%201%20October%202012.pdf
[27] Act 28 of 2011.

5. Conduct Vendor Due Diligence

Due diligence should be conducted on cloud service providers to actively verify the cloud vendors security standards, prior to hosting with such service provider. Such due diligence constitutes reasonable steps which a lawyer must take to ensure that sensitive client information is protected and remains confidential, and to identify whether or not the service provider and technology they use support the lawyer's professional obligations, including compliance with applicable Law Societies regulatory processes.