LIQUID LITIGATION MANAGEMENT, INC.

Every Cloud Has a Silver Lining:

Protecting Privileged Data in a Hosted World

By Lindsay Stevens, Vice President Technology

As litigation and e-discovery continue to rise, more legal departments are turning to cloud computing for its advantages, which include greater efficiency through ease of accessibility and collaboration opportunities as well as cost-effectiveness from scalability and lack of infrastructure costs — all without sacrificing quality or security.[1] But what are the risks of reaching for the cloud and can the waiver of attorney-client privilege be one of them? What follows is an exploration of the contemporary concern, what's being done to address it and steps counsel can take to ascend to the cloud with confidence.

CLOUD AND E-DISCOVERY CONCERNS

In his 2012 article on balancing cloud convenience with client confidentiality, R. Eric Hutz asserts that there are both cloud and e-discovery concerns worth counsel's consideration. Counsel can either address them with the service provider or at least be aware of them at the time of engagement.

CLOUD:[2]

- A client's consent to use a cloud-computing platform and transmit confidential information
- Unauthorized access by hackers or vendor employees
- What jurisdiction would govern the company and vendor's respective businesses and the servers' location in a dispute
- Who would ensure software licenses in third-party programs permit cloud computing
- Data backup and encryption, data destruction policies and audit accessibility

E-DISCOVERY:[3]

- Whether the company owns or controls the data in the cloud
- If there is easy access to data, especially for pending discovery requests
- How the vendor would respond to third-party requests like a subpoena
- If the vendor is required to inform the company prior to production
- The storage of confidential information on servers in countries with less legal protection of electronically stored information (ESI)
- How information would be handled to comply with the company's obligation to produce relevant ESI in a reasonable and defensible manner

In addition to this comprehensive list, Hutz advises that the protection of privileged communication within the overall cloud computing process and the review and production of ESI stored in the cloud must also be carefully considered.[4]

Furthermore, since cloud-computing services are outsourced to a third party and utilize servers in an external location, it raises ethical and privilege obligation issues.[5]

ETHICAL OBLIGATIONS

According to a cloud-computing article by Louise L. Hill, there is a wide range of ethical obligations associated with a lawyer's use of cloud computing and the privacy and security of client information. A lawyer's duty of competence requires the protection of client information that is accessible from a cloud-computing platform, the selection of the appropriate model, and understanding the risks and benefits associated with the use of such technology.[6]

ATTORNEY-CLIENT PRIVILEGE

Hill also states that in addition to a lawyer's ethical duty to maintain client confidences, the law of confidentiality in this country recognizes the doctrine of attorney-client privilege, which protects against compelled disclosure of confidential communications exchanged between lawyer and client.[7] It is a rule of evidence that limits "the extent to which a party in litigation can force from an unwitting witness a statement or document that is protected as confidential."8 She continues that a lawyer's ethical duty to maintain client confidences also applies in all representational contexts.[9] Each state has its own privilege rules, while federal courts follow Rule 501 of the Federal Rules of Evidence. Abroad, attorney-client privilege depends on the country.[10]

Attorney-client privilege can be waived and is absolute. In Hall's reference to work by J. Triplett Mackintosh and Kristen M. Angus, a waiver can result from intentional voluntary disclosure and inadvertent disclosure.[11] At issue is whether the waiver is triggered when confidential information is turned over to a cloud service provider. In Hall's reference to an article by Janine Anthony Brown, in such a situation, not only is a lawyer entrusting protected information to a third party, but also, in the cloud environment, it is possible for the same information to be stored in multiple locations at the same time.[12] Because data in the cloud may be moved geographically to servers in different states or different countries, which jurisdiction or country's laws are applicable may have an impact on the privileged nature of underlying communications.[13] With respect to voluntary waiver, and again through Hill's reference to work by Mackintosh and Angus, it's the client, not counsel, who can waive privilege.[14]

Hill addresses whether turning confidential information over to a cloud service provider results in the waiver of attorney-client privilege. She states that a lawyer must assess the degree of protection needed to safeguard client information and act accordingly.[15] If counsel allows a cloud vendor to store a client's confidential information without being aware of security measures and location, he or she may end up breaching ethical obligations, resulting in an inadvertent waiver and the loss of confidential information's privileged status.[16]

Additionally, a lawyer must know what will happen to the data if the cloud provider is acquired, files for bankruptcy, or goes out of business, and that failure to do so could have ethical implications and the loss of privilege through an inadvertent waiver.

INTERNATIONAL CONSIDERATIONS

It is imperative that lawyers are aware where their cloud providers are physically storing their data, particularly in this global information and business climate. Physical storage locations may determine what country's law is applicable, thus having an impact on the security, confidentiality and privileged nature of the information.

In some countries, like Switzerland and Germany, only documents in a lawyer's possession are protected.[17] Documents in a client's possession, like a legal advice letter from counsel, may not be protected.[18] Other countries like Japan, Romania and Brazil have similar laws.[19] In Spain, however, documents in a client's possession "continue to benefit from confidentiality," and in Italy they are "generally protected from disclosure."[20] Understanding the local legal issues will help counsel know when and what to expect with privilege and legal protection of communications in the cloud.

In many countries, the legal profession is bifurcated and the attorney-client privilege does not extend to in-house lawyers. The ability of in-house lawyers to claim the attorney-client privilege or legal profession privilege in Europe typically divides along the lines of countries originating from English common law versus civil law.[21] The United Kingdom and Canada allow privilege protection between in-house counsel and their clients. The Netherlands, Germany and Belgium offer some level of protection but require that counsel makes some steps to ensure impartiality. Other European Union nations like France do not necessarily extend this to in-house counsel. In addition, the EU's court system, including the European Court of Justice, does not as re-affirmed in Akzo Nobel Chemicals Ltd. and Akcros Chemicals Ltd. v. European Commission. Beyond Europe, India does not extend privilege to in-house counsel while, in general, China is rather silent on privilege.[22]

India is worth a closer examination. Compared to other developed nations, it has not had much exposure to attorney-client privilege in the cloud, and laws regarding cloud computing and privacy issues continue to evolve.[23]

India's Information Technology Act, 2000 states that government "has the authority to monitor and decrypt any information shared through a computer resource in the cloud."[24] The government has used these acts to prevent companies or threaten companies to get access to communication traffic, for example when Blackberry maker Research in Motion agreed to hand over its encryption keys to India in 2012.[25]

These are real concerns for cloud-computing providers and their clients; as a result, India is not often included in security and confidentiality assurances from cloud providers. Considering these risks, counsel should ensure that their data is not going to be stored in countries where the security of any of their data is at risk, not just to privileged data. Overall, being aware of jurisdictional issues and security issues where the communications are going and being stored is key and will influence cloud usage. Counsel may also protect against unforeseen risk and avoid any pitfalls by defining within contracts where or where not data may be stored. This includes both primary data storage locations and failover locations used for high availability and disaster recovery situations.

DOMESTIC JURISDICTIONS

Bar associations and individual jurisdictions have addressed a number of ethical issues associated with cloud computing, with the primary goal of preserving security and confidentiality.[26] What follows are examples from opposite sides of the country.

NEW YORK

According to the Committee on Professional Ethics of the New York State Bar, a lawyer may use cloud computing provided by an online service to backup file storage, provided that reasonable care was taken to ensure system security and the maintenance of client confidentiality. The Committee also advised lawyers that as technology advances, counsel should reconfirm that the provider's security measures are still effective and also monitor changes in law related to confidential communication.

CALIFORNIA

The Standing Committee on Professional Responsibility and Conduct of the State Bar of California determined that an attorney's violation of confidentiality and competence when using technology to transmit or store confidential data depends on the type of technology and use circumstances.[27] Prior to use, lawyers are to consider the technology's level of security, the information's sensitivity, the urgency of the matter, the possible effect inadvertent disclosure or unauthorized interception could pose to a client or third party, and client instructions and circumstances.[28]

CLOUD SECURITY

The adage "you get what you pay for" certainly applies to cloud computing. When one pays more, one may experience higher levels of confidentiality, integrity and availability (CIA). With a private cloud, one can control the perimeter and access whereas with a public cloud, access levels have little differentiation and cannot be customized or, more important, restricted. In addition to security, a cloud-computing client can have a higher expectation for integrity and availability from a private cloud, plus a more efficient resource, which allows for better scalability at a lower cost.

RECOMMENDATIONS

In his article on the impact of technology on attorney-client privilege, Philip Favro recommends that if a company is considering utilizing the cloud for its ESI storage needs, it should require that the vendor "offer measures to preserve the confidentiality of privileged messages." This could include specific confidentiality terms or a separate confidentiality agreement as well as encryption functionality — like secure sockets layer connection, password hashing and encryption key storage — to prevent unauthorized access in the cloud and better preserve confidentiality.[29] With regard to the confidentiality agreement, the company and cloud vendor want to be sure to include that confidentiality will be maintained by putting the parameters discussed in place and that the client neither waives nor intends to waive any applicable privilege by allowing the cloud vendor to host its data.

FINAL WORDS: ENJOYING CLOUD COMPUTING TO THE FULLEST

Cloud computing is a powerful tool that offers increased efficiency and cost-savings for both counsel and clients. The total cost of ownership for corporations is staggeringly less than bringing software in-house to handle legal-related matters, which makes it a more attractive option to an increasing number of businesses. Furthermore, attorney-client privilege can be preserved through attorneys' understanding of the evolving technology, applicable and changing laws, and ensuring proper safeguards are in place like encryption functionality and precise agreements. Attorneys who follow the recommended standards for reasonable care and perform their due diligence on the cloud provider for security, confidentiality and data storage can safely benefit from the many advantages of cloud computing and working with a proven service provider.

• END •

REFERENCES

[1] Steven Hunter, E-Discovery: *Ascending to the Cloud Creates Negligible E-Discovery Risk,* Inside Counsel (July 6, 2011), *available at* http://www.insidecounsel.com/2011/07/06/e-discovery-ascending-to-the-cloud-creates-negligi.

[2] R. Eric Hutz, *E-Discovery: The Relationship Between Cloud Computing, E-Discovery and Privilege,* Inside Counsel (May 22, 2012), *available at* http://www.insidecounsel.com/2012/05/22/e-discovery-the-relationship-between-cloud-computi.

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] Louise L. Hill, *Cloud Nine or Cloud Nein? Cloud Computing and Its Impact on Lawyers' Ethical Obligations and Privileged Communications,* Journal of the Professional Lawyer (2013), at 4.

[7] *Id.* at 6.

[8] *Id.*

[9] *Id.*

[10] *Id.* at 7.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] Louise L. Hill, *Disparate Positions on Confidentiality and Privilege Across National Boundaries Create Danger and Uncertainty for In-House Counsel and Their Clients, Legal Ethic s for In-House Corporate Counsel (2007),* at 4, *available at* http://works.bepress.com/louise_hill/4.

[18] *Id.*

[19] http://uk.practicallaw.com/2-103-2508?service=crossborder.

[20] *Id.*

[21] Jordan W. Cowman & Ausra Laurusa, *Attorney-Client Privilege Across Borders: In-House Counsel* (Feb. 2011), *available at* http://www.dallasbar.org/content/attorney-client-privilege-across-bordershouse-counsel.

[22] Sam Widdoes, *Privilege in a Global Landscape Part II: International In-House Counsel, available at* http://www.acc.com/legalresources/quickcounsel/piaglpt.cfm.

[23] Kasturika Sen, *India: Privacy Issues in Cloud Computing* (Dec. 4, 2013), *available at* http://www.mondaq.com/india/x/279070/Data+Protection+Privacy/Privacy+Issues+In+Cloud+Computing+With+Reference+To+India.

[24] *Id.*

[25] Joji Thomas Philip, *BlackBerry Maker Research in Motino Agress to Hand over Its Encryption Keys to India* (Aug. 2, 2012), *available at* http://articles.economictimes.indiatimes.com/2012-08-02/news/33001399_1_blackberry-enterprise-encryption-keyscorporate-emails.

[26] *Supra* note 8 at 8.

[27] *Id.* at 10.

[28] *Id.*

[29] Philip Favro, *Technology: The Impact of Digital Age Innovations on the Attorney-Client Privilege* (Oct. 25, 2013), *available at* http://www.insidecounsel.com/2013/10/25/technology-the-impact-of-digital-age-innovations-o.