Attorney-Client Privilege in the Cloud

Cloud storage has grown in popularity over recent years, and storage is generally a third-party, off-site, Internet-accessible data store for computer files. An advantage of cloud storage is that individuals and firms can pay for only the amount of storage actually used, and can purchase additional storage without having to purchase additional hardware (such as hard drives). Further, cloud storage services may provide additional features such as data redundancy, security (*e.g.*, file encryption), and file sharing.

One example of a cloud storage service is Dropbox, which synchronizes files among a user's multiple devices such as computers and smartphones (while also storing those files online for access via a web browser). For example, when a user saves a word-processing document, that document is automatically uploaded to Dropbox's servers and is then propagated to all of the user's other devices. Further, Dropbox stores a new version of the document each time it is saved and uploaded, thereby allowing a user to quickly and easily recover previous versions of the document. Additionally, Dropbox can propagate updated documents to devices of multiple users (such as friends and coworkers), and allows those other users to also upload a modified copy of the document for propagation. Other cloud storage services, such as Apple's iDisk, Google Docs, and Windows Live Mesh, provide similar functionalities.

However, cloud storage services present concerns that would not otherwise be present if individuals and organizations stored data locally—concerns such as the ability of third parties to access sensitive data. For example, a corporate competitor might attempt to use a subpoena to force a cloud storage service to disclose sensitive files.

Any such access to attorney-client privileged data could waive the privilege. This article investigates the risk of disclosure of cloud-stored attorney-client privileged information to third parties, and concludes that the risk of disclosure is low, such that the use of cloud storage services is unlikely to result in a waiver of attorney-client privilege.

Law of Attorney-Client Privilege

An exact formulation of the elements that must be present to assert attorney- client privilege over a communication is jurisdiction-dependent, varying based on the governing case law. However, the general rule is that the attorney-client privilege applies to (1) any communication (2) made between privileged persons (such as the client and attorney) (3) in confidence (4) for the purpose of obtaining or providing legal assistance for the client.[1] Accordingly, the attorney-client privilege may apply to, for example, emails requesting legal advice,[2] invention disclosure forms,[3] emails from an inventor regarding an invention,[4] and draft patent applications.[5]

Generally, the attorney-client privilege is waived if the client or attorney provides the communication to a third party.[6] However, exceptions exist, for example, for agents of either the client or attorney

who facilitate communication and for agents of the attorney who facilitate the representation.[7] Yet, for either exception to apply, the client or attorney communicating the privileged information must reasonably believe that no third parties other than the agent will learn the contents of the communication.[8]

Third-Party Access to Attorney-Client Privileged Files Stored in the Cloud

Cloud storage services do present some risk of inadvertent disclosure of attorney-client privileged information to third parties. However, this risk is small.

Security

Nearly all cloud storage services employ security measures to prevent unauthorized access to data. For example, Dropbox employs various security measures to prevent disclosure of information to hackers. All information stored on Dropbox's servers is encrypted using "the same encryption standard used by banks to secure customer data."[9] Dropbox also encrypts all data transmissions to and from their servers "using 256-bit SSL (Secure Sockets Layer) encryption, the standard for secure Internet network connections."[10] Moreover, Dropbox uses "military grade perimeter control berms, video surveillance, and professional security staff to keep their data centers physically secure."[11]

On the other hand, Dropbox and most other cloud storage services do not implement advanced security measures such as two-factor authentication. Since data stored by Dropbox is encrypted using only a password, hackers need only obtain a user's password to have complete access to that user's files. Because Internet users often use the same username and password for multiple services (such as Facebook, Google, and Amazon), hackers often only need to obtain a password for one of these services, perhaps by targeting the least-secure service.[12] Further, hackers may use "social engineering" to obtain a password, perhaps by emailing an unsuspecting user and posing as a system administrator asking for a password to provide a free upgrade to the service.[13] Since many websites allow a user to reset a password using information such as a birthday or birthplace, hackers may be able to reset a user's password by obtaining this information via a social network such as Facebook. Advanced security measures not currently offered by Dropbox could prevent these exploits.[14]

However, these security issues are not unique to Dropbox or cloud storage services generally. In a recent survey, only 15 percent of law firms employed two-factor authentication for Microsoft Outlook web access.[15] The other 85 percent offered the same password security that Dropbox offers. Therefore, the same methods for obtaining a user's Dropbox password would apply equally to obtaining the user's Outlook password. Yet law firms trust and rely upon password security to protect attorney-client privileged information.

Further, according to the same survey, only 10 percent of law firms automatically encrypted outgoing emails.[16] In contrast, Dropbox provides automatic end-to-end encryption for file transfers. By these measures, cloud storage services provide stronger security measures than those currently provided by many law firms.

Therefore, the security measures adopted by Dropbox (and other cloud storage services) will generally preserve the attorney-client privilege of files stored on Dropbox servers. Law firms would not adopt these measures unless they reasonably believed that no third parties would learn the contents of the communication (a belief that is necessary for the attorney-client privilege to apply).[17] The security measures provided by cloud storage services are at least as secure as, if not more than, those provided by law firms. For example, Google (which provides Google Docs and Gmail) offers two-factor authentication, an advanced security measure offered by few law firms.[18] Therefore, a client or attorney could reasonably believe that no third party would learn the contents of files stored on Dropbox or another cloud storage service.

e-Discovery

Another concern regarding cloud storage services is the potential for corporate competitors to obtain attorney-client privileged files from those cloud storage services via a subpoena. Such a subpoena may allow (and indeed require) the cloud storage service to turn over such sensitive information.

For example, Dropbox's privacy policy explicitly allows Dropbox to turn over files and information in response to a subpoena.[19] Moreover, before turning those files over in response to a subpoena, Dropbox will decrypt the encrypted files.[20] Dropbox is able to decrypt the files because it also stores the information necessary to decrypt that information.[21]

However, because only the party that holds the attorney-client privilege (*i.e.*, the client) may waive the privilege,[22] subpoenas to cloud storage services should not pose a threat of waiver. Indeed, courts have held that the attorney-client privilege is not waived, even if third parties obtain the privileged information via a subpoena, so long as the communicating party reasonably believed that the information was safe from access by third parties.[23] In fact, some parties have been sanctioned for attempting to subpoena information known to be protected by the attorney-client privilege.[24] Further, assuming that attorneys are complying with their obligation to disclose relevant, non-privileged documents during discovery,[25] the volume of non-privileged documents that may be relied upon during litigation should be the same regardless of whether the documents are obtained via a cloud storage service (*e.g.*, Dropbox) or via the production of documents possessed by the client or attorney.

Therefore, the storage of attorney-client privileged files on cloud storage services presents little risk of waiving that privilege. At a minimum, such storage presents little (if any) additional risk of waiver as compared to storing files locally on a hard drive.

Conclusion

Dropbox and other cloud storage services present little (if any) additional risk of disclosure to third parties than do other methods of communicating or storing information, and may present even less of a risk than other methods of communication. For example, in contrast to Dropbox's policy of not inspecting user information, FedEx's policy explicitly provides that they "may, at our sole discretion, open and inspect any shipment without notice."[26] Such unfettered access to attorney-client privileged information by FedEx could arguably negate a reasonable belief by a client or attorney that such information is inaccessible by third parties. In any case, clients and attorneys can safely store files, including attorney-client privileged files, using cloud storage services, without fear that the privilege will be waived, so long as the client and attorney reasonably believe that no other third parties will be able to access the files.

Alan W. Krantz, an MBHB associate, prepares and prosecutes patent applications, conducts legal research, and provides technological advice in support of validity, infringement, and patentability analyses, patent application preparation and prosecution, and litigation matters in the computing field.
krantz@mbhb.com

Endnotes

1. Restatement (Third) of the Law Governing Lawyers § 68 (1998).
2. *E.g.*, *McCook Metals L.L.C. v. Alcoa Inc.*, 192 F.R.D. 242, 252-53 (N.D. Ill. 2000).
3. *In re Spalding Sports Worldwide, Inc.*, 203 F.3d 800, 805-06 (Fed. Cir. 2000).
4. *E.g.*, *McCook Metals*, 192 F.R.D. at 253.
5. *E.g.*, *id.* at 252-53.
6. "A communication is in confidence... if, at the time and in the circumstances of the communication, the communicating person reasonably believes that no one will learn the contents of the communication except a privileged person as defined in § 70 or another person with whom communications are protected under a similar privilege." Restatement (Third) of the Law Governing Lawyers § 71 (1998).
7. "Privileged persons within the meaning of § 68 are the client (including a prospective client), the client's lawyer, agents of either who facilitate communications between them, and agents of the lawyer who facilitate the representation." *Id.* § 70.
8. *Id.* § 71.
9. Dropbox, Security Overview, http://www. dropbox.com/security/ (last visited Aug. 7, 2011) [hereinafter "Dropbox Security"].
10. *Id.*
11. *Id.*
12. Symantec, *Social Engineering*
13. *Fundamentals, Part I: Hacker Tactics* (Nov. 3, 2010), *available at* http://www. symantec.com/connect/articles/socialengineering-fundamentals-part-i-hackertactics.
    Id.
14. Further, Dropbox recently suffered a severe security lapse when a software bug allowed anyone to log in to any account using any password over a period of four hours. *See* Arash Ferdowsi, The Dropbox Blog, *Yesterday's Authentication Bug* (June 20, 2011), *available at* http://blog.dropbox. com/?p=821.
15. Int'l Legal Tech. Ass'n, 2010 Technology Survey: Analysis and Results 52 (2010), *available at* http://iltanet.org/MainMenuCategory/PublicationsWhitePap ersandSurveys/2010-Technology-Survey. aspx.
16. *Id.*
17. *See* Restatement (Third) of the Law Governing Lawyers § 71 (1998).
18. Google, Getting Started with 2-Step Verification, http://www.google.com/ support/accounts/bin/answer.py?answer =180744 (last visited Aug. 7, 2011).
19. "We may disclose to parties outside Dropbox files stored in your Dropbox and information about you that we collect when we

have a good faith belief that disclosure is reasonably necessary to (a) comply with a law, regulation or compulsory legal request....” Dropbox, Privacy Policy (July 2, 2011), *available at* http://www.dropbox. com/privacy/ [hereinafter Dropbox Privacy Policy].

20. “If we provide your Dropbox files to a law enforcement agency as set forth above, we will remove Dropbox’s encryption from the files before providing them to law enforcement.” *Id.*
21. “[W]e manage the encryption keys.” Dropbox Security, *supra* note 9.
22. *See Advertising to Women, Inc. v. Gianni Versace S.p.A*, No. 98 C 1553, 1999 WL 608711, at *4 n.3 (N.D. Ill. Aug. 4, 1999) (quoting *Southwire v. Essex Group, Inc.*, 570 F. Supp. 643, 645 (N.D. Ill. 1983)).
23. *E.g.*, *Am. Int’l Life Assurance Co. of NY v. Vazquez*, No. 02 Civ. 141(HB), 2003 WL 548736, at *3 (S.D.N.Y. Feb. 25, 2003).
24. *Id.*; *see also* Fed. R. Civ. P. 45(c)(3)(A)(iii) (“On timely motion, the issuing court must quash or modify a subpoena that... requires disclosure of privileged or other protected matter, if no exception or waiver applies...”).
25. Fed. R. Civ. P. 26(b)(1) (“Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party’s claim or defense...”); *Bristol-Myers Squibb Co. v. Rhone-Poulenc Rorer, Inc.*, 188 F.R.D. 189, 199 (S.D.N.Y. 1999) (“Court process can, however, require disclosure of [attorney-client confidential] information unless it is subject to the attorney-client privilege.”).
26. FedEx, Express Terms and Conditions 7 (July 14, 2011), *available at* http://fedex. com/us/service-guide/terms/expressground/.