TIPS FOR SAFEGUARDING CONFIDENTIALITY & PRIVACY OF CLIENT INFORMATION IN COMPLIANCE WITH PROFESSIONAL RULES, HIPAA, & OTHER STATUTORY REQUIREMENTS

General Practice, Solo & Small Firm Section Program

Al Harrison
Harrison Law Office, P.C.
411 Fannin Street, Suite 350
Houston, Texas 77002
(713) 223-4034
Patent.Trademark.Lawyer@hlopc.com

Co-Author:

Randy Claridge
Harrison Law Office, P.C.
Randy.Claridge@hlopc.com

Thursday, June 10, 2010
9:30 a.m. – 10:00 a.m.
Biographical Sketch of Al Harrison; Harrison Law Office, P.C.; Houston
(Patent.Trademark.Lawyer@hlopc.com)

Al Harrison is a patent attorney who practices intellectual property law in Houston under
the banner of Harrison Law Office, P.C. Prior to practicing law, he worked as an engineer and as
a computer programmer/analyst/designer.

He received an engineering undergraduate degree from City College of the City
University of New York (1967); a masters degree in Operations Research from New York
University (1970); and his law degree from the University of Houston Law Center (1983).

Al is a past chair of the State Bar Computer & Technology Section, and continues to
serve as a council member. He is a council member of the GP-Solos-Small Firm Section and is a
past chair of the Computer Law Committee of the Intellectual Property Law Section. Al is also
presently a member of the State Bar Law Practice Management Committee. He has been a board

Al is a member of the Houston Bar Association, where has served as chair of each of the
Law Practice Management and Cyberlaw Sections, and also serves on the editorial board of The
Houston Lawyer magazine and has been a guest editor of special issues. He is a past president of
the HAL-PC computer user group in Houston.

Al speaks regularly on substantive intellectual property and computer law issues, and on
technology-related issues under the auspices of the State Bar, the Texas Center for the Judiciary,
the Houston Bar Association, and other independent organizations. He frequently participates on
panels and 10-Minute Mentor presentations for State Bar webcasts and podcasts.
Randy Claridge  
Harrison Law Office, P.C.  
411 Fannin Street #350  
Houston, Texas 77002  
713-223-4034  
FAX: 713-224-7950  
Randy.Claridge@hlopc.com

**BIOGRAPHICAL INFORMATION**

**EDUCATION**  
B.S. in Industrial Engineering, Texas A&M University  
J.D., South Texas College of Law

**PROFESSIONAL ACTIVITIES**  
Harrison Law Office, Houston, TX – Intellectual Property Attorney  
El Paso Corporation, Houston, TX – Senior Risk Analyst  
Futron Corporation, Houston, TX – Systems Engineer

**PUBLICATIONS AND PRESENTATIONS**  
Speaker, Houston Bar Association, “Billing and Collection” 2009  
Co-Author, The Practice Manager, “E-Book Review: Spam-Proof Your E-mail Address” 2008  
Speaker, Simulations Solution Symposium, “Robust Modeling Design” 2001
Safeguarding Confidentiality and Privacy of Client Information in Compliance with Professional Rules

Al Harrison & Randy Claridge
Harrison Law Office, P.C.
Houston, Texas
# Table of Contents

I. Safeguarding Client Information .................................................................................................................. 3
II. Retention of Client Information .................................................................................................................... 3
   A. Current Client Files .................................................................................................................................. 3
   B. Inactive Client Files .................................................................................................................................. 3
   C. Former Clients .......................................................................................................................................... 4
III. How to Protect Client Information with Encryption .................................................................................... 4
IV. Procedural Tips for Protecting Client Information .......................................................................................... 5
   A. Security Prerequisites for Laptops and Handhelds .................................................................................... 5
   B. Password Logistics ................................................................................................................................... 5
   C. Laptop, Handheld & Other Portable Device Longevity .............................................................................. 5
V. Online Services ............................................................................................................................................. 5
   A. Primary Storage ........................................................................................................................................ 7
      i. Google Docs ......................................................................................................................................... 8
      ii. Microsoft Office Live .......................................................................................................................... 8
      iii. Clio ..................................................................................................................................................... 9
   B. Backup Storage ........................................................................................................................................ 9
      i. Carbonite ............................................................................................................................................. 9
      ii. Mozy .................................................................................................................................................... 9
   C. Remote Access ......................................................................................................................................... 10
      i. LogMeIn ............................................................................................................................................. 10
      ii. GoToMyPC ......................................................................................................................................... 10
VI. Final Thoughts .......................................................................................................................................... 10
I. Safeguarding Client Information

The confidentiality standards of the attorney-client relationship enable an open and honest discussion between clients and their respective counsel, and generally promote resolution of clients' legal matters. Except as otherwise permitted or required, a lawyer shall not knowingly "[r]eveal confidential information of a client or a former client to: (i) a person that the client has instructed is not to receive the information; or (ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer’s law firm.” Tex. Disciplinary R. Prof'l Conduct 1.05(b) (2005).

A common issue arises when dealing with routine duplication and transport of confidential client information. Specifically, if a third-party is provided access to confidential client information for the purpose of providing a service to the lawyer, has a breach of Rule 1.05 occurred?

The Supreme Court of Texas Professional Ethics Committee Opinion Number 572, June 2006, addresses the use of an independent contractor, such as a copy service, hired by the lawyer to perform services in connection with the lawyer’s representation of the client. The Committee concluded:

that a lawyer's delivery of materials containing privileged information to an independent contractor providing a service, such as copying, to facilitate the lawyer's representation of a client (and not for the purpose of disclosing information to others) does not constitute "revealing" such privileged information within the meaning of Rule 1.05, provided that the lawyer reasonably expects that the independent contractor will not disclose or use such items or their contents except as directed by the lawyer and will otherwise respect the confidential character of the information. In these circumstances, the independent contractor owes a duty of confidentiality both to the lawyer and to the lawyer's client.

Although not explicitly addressed by the Committee, use of independent contractors in the form of Internet-based services would not necessarily constitute revealing of privileged client information. However, as will be hereinafter described, attaining a reasonable expectation that Internet-based service providers will neither disclose nor use such privileged information, except as directed by the lawyer, may prove problematic.

II. Retention of Client Information

A. Current Client Files

Files associated with current clients are perhaps the most straight forward to maintain. After all, legal services are currently being performed on behalf of the client. But, what about long-standing or large clients which implicate numerous matters corresponding to comparably numerous files? Original documents including wills, deeds, securities, and signed contracts should be retained indefinitely. When space or protection of sensitive information is an issue, formal delivery of client files should be scheduled for each matter which has concluded, e.g., final settlement or judgment, attaining federal Trademark Registration or a Patent Grant, thereby relieving the attorney of the burden of storing physical copies. For record-keeping purposes of the attorney, electronic copies of the original documents should preferably be created. The Texas Business & Commerce Code §72.003 (2009) contemplates satisfying business record retention requirements via reproduction of the original records.

B. Inactive Client Files

There is no bright line rule regarding retention of client files. Each type of document contained within a client file may require a different retention term. A business record may be destroyed as soon as the third anniversary of the date the record was created. Tex. Bus. & Comm. Code §72.002. The Health Insurance Portability and Accountability Act (HIPAA) requires retention of policies and procedures for a period of six years from the date of creation or the date when last was in effect, whichever is later. 45 CFR §164.316(b)(2)(i) (2009). Estate planning files should be retained until the client’s death plus four years. Records related to intellectual property including evidence of ownership of patents and trademarks – and supporting documents, should preferably be retained in perpetuity.

Attorneys often retain original client files as a courtesy to the client and at the client’s request thereby facilitating expeditious access to client history. Unfortunately, the duty to maintain attorney-client confidentiality and to safeguard client property can easily result in an attorney spending significant time and money to take reasonable precautions regarding the clients’ files. A preferable approach is to implement a formal, matter-specific, disengagement process wherein a client’s file for a particular matter is
surrendered and wherein the attorney creates a duplicate copy for the attorney’s own record-keeping purposes.

C. Former Clients
Confidentiality of client information survives termination of representation, i.e., applies to former clients. Tex. Disciplinary R. Prof’l Conduct Rule 1.05 (2005). The duty to maintain confidentiality, however, is not a duty to maintain former client records in perpetuity. Whenever termination of representation occurs, the client files should be surrendered and property to which the client is entitled turned over to the client. Tex. Disciplinary R. Prof’l Conduct Rule 1.15(d). The attorney should preferably create a duplicate of the file contents for internal record-keeping purposes, at the attorney's own expense.

As a practical guide, there is a two-year limitation period during which a person must bring a suit for matters such as legal malpractice. See Texas Civ. Prac. & Remedies Code Sect. 16.003. Due to the possibility of tolling of the two-year limitation period, retention of duplicated former client files should be determined on a case-by-case basis including factors such as minority, mental incompetence, bankruptcy, and ongoing incarceration. In the case of safekeeping client property, “[c]omplete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of five years after termination of the representation.” Tex. Disciplinary R. Prof’l Conduct Rule 1.14(a).

III. How to Protect Client Information with Encryption
Encryption refers to a process of converting information into a form which is unusable, unreadable, and indecipherable to parties not possessing the requisite decryption algorithm. There currently exist several popular encryption paradigms including: file or folder encryption, full-disk encryption, and encrypted communications to and from networked computers. Regardless of the approach taken, encryption is quickly becoming a standard requirement of the contemporary law office because the loss of an encrypted computer or encrypted data file often does not trigger notification rules thereby potentially protecting attorneys and clients from the expenses and other ramifications associated with a breach of client confidentiality.

Individual file or folder encryption is perhaps the first form of encryption adopted by many attorneys using software programs such as Adobe Acrobat Professional (Acrobat). Using Acrobat, a Portable Document Format (PDF) file or set of PDF files (PDFs) can be converted to a form that renders the file(s) unreadable to anyone lacking a corresponding password or digital certificate. An encrypted file may then be stored on a computer network or e-mailed to a client without fear of inadvertent disclosure of confidential information.

Although easily implemented, individual file encryption poses a significant challenge when dealing with numerous clients and client matters, which implicate multiple passwords. If the password required for a particular file were destroyed or otherwise were to become unavailable, the contents of the encrypted file would be in all likelihood lost and thus effectively digitally “shredded.”

Another encryption approach, typically implemented on business-class laptops, is full-disk encryption (FDE), either hardware-based or software-based. With FDE the contents of the entire hard drive are stored in an encrypted state. In a hardware-based implementation of FDE, a decryption key is stored within the circuitry of the hard drive and data is seamlessly decoded following initial, boot-time entry of a password by the user. In a software-based implementation of FDE, pre-installed software such as the open-source program TrueCrypt (http://www.truecrypt.com), PGP Whole Disk Encryption (http://www.pgp.com), and Windows proprietary BitLocker (http://www.microsoft.com/windows/windows-7/features/bitlocker.aspx) serve as boot-time gatekeepers requiring password entry prior to decoding of user data. The ease of FDE is readily apparent; however, care should be taken following initial password entry because data is automatically decoded until the system is turned off or rebooted.

Unlike individual file encryption, FDE does not require password entry beyond a single boot-time entry. A single password can be used for each computer which stores confidential client information thereby rendering the information unreadable should the computer be stolen or otherwise misplaced.

In addition to secure storage of client information on internal office computers, electronic communications with client should also be encrypted. Fortunately, most Internet services, including e-mail, e-commerce, and document storage incorporate the Secure Sockets Layer (SSL) protocol specified within the settings of an e-mail software application or identifiable by “https://” preceding a website address. If “https://” does not precede a website address, then the communications to and from that website are not
encrypted and are potentially readable by unknown third-parties.

IV. Procedural Tips for Protecting Client Information

A. Security Prerequisites for Laptops and Handhelds

Recommended security prerequisites for laptops and handhelds: (1) password protected with an inherently strong password; (2) relatively short laptop or handheld inactivity or emplacement of handheld in holster causes timeout that blanks screen, or shuts down hard drive, deactivates keys or touch screen, and requires password for reactivation; (3) email should preferably be encrypted in transit to and from user; (4) stored files encrypted - text, images; (5) all data should preferably be remotely purged if laptop or handheld has gone missing.

B. Password Logistics

The propriety of passwords must be assured and sustained or else the integrity of the safeguarding protocol is undermined. This is a very serious and crucial aspect of safeguarding client data. While inconvenient and introducing another level of complexity to the law firm environment, password protocol must be carefully established and rigorously practiced and enforced.

Recommended password protocol: (1) Don't keep passwords posted in plain view near computers, e.g., using Post-It notes, stickies, etc.; (2) Don't print a list of passwords and store the list adjacent computer on desktop, in file drawer, etc.; (3) Don't generously share core or private passwords; being very discriminating which personnel, if any, have access to such core information; (4) Consider invoking an encrypted password or key manager [RoboForm, Keepass, Sxipper for Firefox] or a unique encoding schema; (5) Don't construct passwords from repeated characters or numbers, or sequences of characters or numbers; (6) Don't rely upon pedestrian data [based upon biographical or family information]; (7) Preferably use association protocol for remembering passwords or keys, and encode password from combinations of associated words or terms; write down encoded sequence(s) constituting password(s) or key(s).

C. Laptop, Handheld & Other Portable Device Longevity

Be "religious" about properly caring for each and every storage device containing proprietary and confidential client information — both in the office and contained on a portable electronic device or storage medium. Pattern established that no more than 5% of stolen laptops are typically recovered. Laptop thefts during 2009 and continuing into 2010 are expected to grow exponentially. According to the FBI’s National Crime Information Center, the number of reported laptop thefts rose about 50% during the two-year time horizon from 2007 - 2008, i.e., from about 74,000 to about 109,000 laptop thefts.

The number of reported cell and smartphone thefts soared 33% during this same 2007 - 2008 time frame — from about 60,000 to about 80,000 thefts. Similarly, during the past 3 years, reported thefts of Apple iPods and other digital music players surged 90% — from about 9,000 to more than 17,000. These disappearances of valuable portable electronic devices are attributable to not only pick-pocketing or the like, but also to commercial thefts. Moreover, the actual numbers of losses and thefts are even higher because of a significant number of unreported occurrences.

Obviously, the costs associated with laptop and device theft are staggering. The Computer Security Institute’s 2008 Computer Crime & Security Survey found that information breaches cost companies an average of about $300,000 a year. It should be noted with great interest that about 40% of about 70 large corporations surveyed suffered the consequences of laptop theft. Incredibly, the most prevalent venue for laptop losses to occur are U.S. airports: as many 12,000 laptops are lost or stolen weekly at domestic airports, as estimated by the Ponemon Institute. This Institute has also guesstimated that as many as 800,000 memory devices — laptops, smartphones, thumb drive memory sticks — are lost or stolen annually; and that major corporations are inflicted by annual robberies devolving to about 600 laptops, 2000 USB thumb drive memory sticks, 1000 smartphones, and 1,500 other portable electronic data storage devices.

Clearly, caution should be exercised in virtually every venue the attorneys visit or travel, not just airports and train stations, but also coffee shops, government buildings and offices, clients’ offices and sites. It appears that contemporary criminals have adopted the protocol for stealing or demanding popular, easily liquidated electronic devices besides cash money. Laptops and netbooks should be held securely to prevent thieves from engaging in a snatch-and-run maneuver at an attorney’s expense. Similarly, smartphones, iPods, and the like should not be conspicuous to attract the attention of lingering thieves.

A recent fail-safe application to be considered by law firms is Remote Laptop Security ("RLS") corresponding to a procedure that enables users to
control access to files on a laptop even if the laptop has gone missing. Proprietary files for safeguarding are selected a priori and are implicated in a protocol for either restoring or terminating the account that owns the data files. The designated administrator selects which files to be safeguarded using the RLS application. Duly safeguarded files are then converted and encrypted to permit only authorized access. For a laptop which has gone missing, access to secured files is unequivocally denied. There are RLS tools dependent upon Internet or WiFi connections, and even cellular access. In the abundance of caution, RLS applications should periodically authenticate user identity. Of course, under circumstances in which access to proprietary files on a particular laptop has been deactivated, that laptop ceases to be authenticated.

V. Online Services

Many businesses, including law firms, are beginning to explore the benefits of “Cloud Computing,” wherein ownership of computer hardware and software is maintained by a third-party and businesses are granted access to use the third-party’s computer resources on a subscription basis.

Although analogous to using an independent contractor for document duplication and courier services, the advent of Cloud Computing, sometimes referred to as “Software as a Service” (SaaS), raises additional questions. Given the recent availability of SaaS legal applications, few State Bar Ethics Committees have had the opportunity to address the use of online services as a method of managing client files and client communications.

In response to an inquiry regarding the steps a lawyer must take to safeguard electronic client information from Internet hacking and viruses, Arizona State Bar Ethics Opinion 05-04 (July 2005) provides the following guidance:

It is not unethical to store such electronic information on computer systems whether or not those same systems are used to connect to the internet. However, to comply with these ethical rules as they relate to the client’s electronic files or communications, an attorney or law firm is obligated to take competent and reasonable steps to assure that the client’s confidences are not disclosed to third parties through theft or inadvertence. In addition, an attorney or law firm is obligated to take reasonable and competent steps to assure that the client’s electronic information is not lost or destroyed. In order to do that, an attorney must either have the competence to evaluate the nature of the potential threat to the client’s electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end, or if the attorney lacks or cannot reasonably obtain that competence, to retain an expert consultant who does have such competence.

Subsequent guidance is provided in Arizona State Bar Opinion 09-04 (December 2009) regarding online file storage and retrieval systems:

Lawyers providing an online file storage and retrieval system for client access of documents must take reasonable precautions to protect the security and confidentiality of client documents and information. Lawyers should be aware of limitations in their competence regarding online security measures and take appropriate actions to ensure that a competent review of the proposed security measures is conducted. As technology advances over time, a periodic review of the reasonability of security precautions may be necessary.

The North Carolina State Bar Ethics Committee proposed providing the following preliminary guidance (in Proposed 2010 Formal Ethics Opinion 7), Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property, April 15, 2010:

[A] law firm may use SaaS if reasonable care is taken effectively to minimize the risks to the confidentiality and to the security of client information and client files. However, the law firm is not required to guarantee that the system will be invulnerable to unauthorized access. Note that no opinion is expressed on the business question of whether SaaS is suitable for a particular law firm.

The Committee further suggested the following best practices to minimize the risk of using SaaS:
The lawyer or law firm should be able to answer the following questions sufficiently to conclude that the risk to confidentiality and security of client file information is minimal:

- What is the history of the SaaS vendor? Where does it derive funding? How stable is it financially?
- Has the lawyer read the user or license agreement terms, including the security policy, and does he/she understand the meaning of the terms?
- Does the SaaS vendor’s Terms of Service or Service Level Agreement address confidentiality? If not, would the vendor be willing to sign a confidentiality agreement in keeping with the lawyer’s professional responsibilities? Would the vendor be willing to include a provision in that agreement stating that the employees at the vendor’s data center are agents of the law firm and have a fiduciary responsibility to protect client information?
- How does the SaaS vendor, or any third party data hosting company, safeguard the physical and electronic security and confidentiality of stored data? Has there been an evaluation of the vendor’s security measures including the following: firewalls, encryption techniques, socket security features, and intrusion-detection systems?
- Has the lawyer requested copies of the SaaS vendor’s security audits?
- Where is data hosted? Is it in a country with less rigorous protections against unlawful search and seizure?
- Who has access to the data besides the lawyer?
- Who owns the data—the lawyer or SaaS vendor?
- If the lawyer terminates use of the SaaS product, or the service otherwise has a break in continuity, how does the lawyer retrieve the data and what happens to the data hosted by the service provider?
- If the SaaS vendor goes out of business, will the lawyer have access to the data and the software or source code?
- Can the lawyer get data "off" the servers for the lawyer’s own offline use/backup?

If the lawyer decides to cancel the subscription to SaaS, will the lawyer get the data? Is data supplied in a non-proprietary format that is compatible with other software?

- How often is the user's data backed up? Does the vendor backup data in multiple data centers in different geographic locations to safeguard against natural disaster?
- If clients have access to shared documents, are they aware of the confidentiality risks of showing the information to others?
- Does the law firm have a back-up for shared document software in case something goes wrong, such as an outside server going down?

As can be seen from the best practices suggested by the North Carolina State Bar Ethics Committee, safeguarding client information using an online service provider preferably requires more diligence than merely subscribing to an available service.

A. Primary Storage

Google started offering a free e-mail service (GMail) to consumers on a limited basis in 2004. Since then, the company has transformed the consumer and, to a lesser extent, business users' expectations regarding e-mail storage and retrieval.

Prior to GMail, most e-mail providers operated using the standard Post Office Protocol (POP) to download messages from the service provider’s computer to the end-users' computer. A key benefit of the POP approach was that e-mail service providers were not required to allocate a substantial amount of disk space for client files because the files were removed from the e-mail service provider’s mail-server when the user checked their e-mail. With the offering of Internet Message Access Protocol (IMAP), GMail allowed users to check their e-mail, but contrary to POP, the e-mail remained on the GMail mail-servers and could be accessed from multiple computers wherein changes made from any one computer would be visible to all other computers which had authority to access the same e-mail account. Thus, through the introduction of IMAP (in free, consumer-oriented e-mail accounts) Google convinced millions of users to start storing all of their e-mail communications in the “cloud.” It should be noted that Google did not invent IMAP, but rather Google invested heavily in computer storage, thereby enabling users to permanently store their e-
mail messages on Google’s GMail servers.

As computer storage prices continue to fall and Internet connectivity becomes nearly universal – whether through office networks, home broadband, or cell phone data plans – the potential to access data from virtually any Internet-connected device possessing an Internet browser such as Firefox, Internet Explorer, Chrome, Safari, Opera, or other proprietary Internet browsers available on some advanced cell phones, is creating data management possibilities previously reserved for only the largest and wealthiest corporations.

For the small or solo law practice, “Cloud Computing” not only is convenience, but also affords a competitive advantage. Unfortunately, as will be seen in the following privacy policy excerpts, it may be somewhat difficult to achieve an acceptable expectation that independent contractors providing Internet-based services will sufficiently safeguard confidential client information.

i. Google Docs

Google Docs (http://docs.google.com) is an online file storage and dissemination service provided by Google. The main purpose of Google Docs is to provide online storage of customer files and to enable customers to collaborate in the development of such documents. Both a free and a paid version of Google Docs is currently available. The paid version may offer greater protection of confidential information as a privity of contract would then exist.

According to the Google Docs Privacy Policy dated October 20, 2009:

“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. Access to your data by these third parties is not governed by this Privacy Policy.”

The broader Google Privacy Policy effective March 11, 2009 states:

“Google processes personal information on our servers in the United States of America and in other countries. In some cases, we process personal information on a server outside your own country. We may process personal information to provide our own services. In some cases, we may process personal information on behalf of and according to the instructions of a third party, such as our advertising partners.

***

Google only shares personal information with other companies or individuals outside of Google in the following limited circumstances:

• We have your consent. We require opt-in consent for the sharing of any sensitive personal information.

• We provide such information to our subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf. We require that these parties agree to process such information based on our instructions and in compliance with this Privacy Policy and any other appropriate confidentiality and security measures.

• We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.”

Although one of the better privacy policies available today, the Google privacy policy still does not eliminate some potentially troubling scenarios. Will a “gadget” developed by a party other than Google compromise client information stored in Google Docs? As a result of Google storing information on servers outside of the United States, is confidential client information unreasonably susceptible to unauthorized search and seizure? Does the provision allowing Google to access user information to “(d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law” pose a conflict of interest when dealing with client matters involving technology?
ii. **Microsoft Office Live**


The Microsoft Privacy Policy effective October 2009 states in relevant part:

> We may access or disclose information about you, including the content of your communications, in order to: (a) comply with the law or respond to lawful requests or legal process; (b) protect the rights or property of Microsoft or our customers, including the enforcement of our agreements or policies governing your use of the services; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers or the public. We may also disclose personal information as part of a corporate transaction such as a merger or sale of assets.

***

Personal information collected on Microsoft sites and services may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries or service providers maintain facilities.

As with *Google Docs*, potentially troubling scenarios still exist. Microsoft introduces the additional possibility that personal information may be disclosed “as part of a corporate transaction such as a merger or a sale of assets.”

iii. **Clio**

*Clio* ([http://www.goclio.com](http://www.goclio.com)) is a web-based law practice management service providing document management, scheduling, time tracking, and billing features. Electronic documents can be shared with clients by way of encrypted client login. The *Clio* Privacy Policy effective October 2008 states in relevant part:

> We reserve the right to disclose your personally identifiable information as required by law and when we believe that disclosure is necessary to protect our rights and/or to comply with a judicial proceeding, court order, subpoena, or legal process served on our Web site.

Although seemingly protected to a higher degree than that stated in the Google and Microsoft privacy policies, the issue of potential conflicts between *Clio* and attorneys' clients may still exist.

B. **Backup Storage**

i. **Carbonite**

*Carbonite* ([http://www.carbonite.com](http://www.carbonite.com)) is a popular online backup service whereby an installed application continuously monitors an individual's computer for new and changed files that should be backed up.

The *Carbonite* Privacy Policy effective November 19, 2009 includes in relevant part:

> Carbonite may disclose your Personal Information to third parties if we believe that such action is necessary to (1) comply with a law, regulation, or governmental or judicial warrant, rule, or order; (2) protect and defend the rights or property of Carbonite; (3) enforce the Carbonite Terms and Conditions of Use and/or this Privacy Policy. Carbonite may also provide access to your Backup Data to government authorities if Carbonite suspects or believes that the data contain child pornography or other prohibited data, or that the data or the Carbonite Products or Services are being used for illegal purposes. Carbonite will provide access to your Backup Data to your surviving spouse and/or your executor upon presentation of a death certificate and identification which Carbonite reasonably believes to be valid and sufficient, or in response to a court order, warrant, subpoena or other judicial or administrative legal process.

Again, as with most general online backup services, there exist several scenarios wherein *Carbonite* could conceivably divulge confidential client information without requiring an enforceable government request such as a warrant.

ii. **Mozy**

*Mozy* ([http://www.mozy.com](http://www.mozy.com)), a product of the Decho Corporation, is another popular online backup service. The Decho Corporation Privacy Policy effective May 14, 2009 states in relevant part:
By registering to use the Service, you agree (1) to comply with the terms and conditions of this Privacy Policy and (2) Decho may process (i.e., collect, use, etc.) your Personal Data as described in this Privacy Policy or the User Agreement. Personal Data may be processed by Decho in the country where it was collected as well as other countries (including the United States) where laws regarding processing of Personal Data may be less stringent.

Decho does not disclose Personal Data, including the data you back up with the Service, unless disclosure is necessary to comply with an enforceable government request such as a warrant.

Mozy appears to offer a very strong commitment to protecting the confidentiality of data short of an enforceable government request; nevertheless, storage of data in jurisdictions outside of the United States may still be of concern because those locations may have less stringent requirements regarding attainment of an enforceable government request.

C. Remote Access

In some circumstances, it may be preferable to merely access secure law-office computers remotely rather than storing confidential client information on the Internet. This approach has the benefit of keeping confidential client information solely on the attorney's computers. Fortunately, nearly every remote access option currently available incorporates communication encryption. Notwithstanding, attorneys should exercise care when relying upon a third-party to provide remote access.

i. LogMeIn

LogMeIn (http://www.logmein.com) provides remote access to computers without requiring substantial user knowledge (computer-specific configuration settings) or IT support. LogMeIn has proven to be a robust and readily available means of remote access to law-office computers.

The LogMeIn Privacy Policy as of May 2010 states in relevant part:

[W]e may transfer your personal information without your consent to the extent required to do so by law or in the
good faith belief that such action is necessary to: a. conform to the edicts of law or comply with legal process served on LogMeIn or the site; b. protect or defend the rights or property of LogMeIn, c. act in urgent circumstances to protect the personal safety, property, or privacy of LogMeIn's employees, users of LogMeIn's products or service, or members of the public, or d. effect a transaction, restructuring or proceeding that transfers to a third party the assets or line of business to which the information pertains.

Although containing language similar to other online service providers, remote access services such as LogMeIn may actually pose less of a threat to client information because remote access merely provides access to a remote computer's login screen.

ii. GoToMyPC

GoToMyPC (http://www.gotomypc.com) offers a remote access service comparable to LogMeIn. The GoToMyPC Privacy Policy effective May 27, 2009 states in relevant part:

Occasionally we send offers to selected groups of GoToMyPC customers on behalf of other businesses. When we do this, we do not give the businesses your name and address. Except in the limited instances as stated above, we will never voluntarily share personally identifiable information with any third party without the user's express consent or unless compelled by applicable state and federal laws. We reserve the right to disclose your personally identifiable information as required by law and when we believe that disclosure is necessary to protect our rights and/or to comply with a judicial proceeding, court order, or legal process served on our Web site.

Citrix Online does not control the practices of our affiliates. If you have questions about how affiliates use the information gathered when you link to them, please read their privacy policies.

As with LogMeIn, GoToMyPC reserves a right to disclose information in circumstances other than solely in response to a court order. Fortunately, secure login
passwords and/or other security measures on the remote computer may serve as an effective barrier to unauthorized intrusion by a remote access service provider.

VI. Final Thoughts

As a practical matter, storage of confidential client information on the Internet by way of a third-party service provider is inevitable. The benefits far outweigh the challenges. With online storage services, a small or solo law practice need not lose a single client file. If a computer is lost or stolen or otherwise destroyed by a natural disaster such as fire or flood, the purchase of a new computer will readily restore access to the client information.

Safeguarding client information requires more than merely securing reliable access to such information. Preferable safeguarding protocols should also include effective use of encryption, adoption of SaaS having adequate privacy policies, and implementation of other protective measures, e.g., firewalls, anti-virus, anti-malware, and computer access policies.

Attorneys still have a duty not to knowingly “[r]eveal confidential information of a client or a former client to: (i) a person that the client has instructed is not to receive the information; or (ii) anyone else, other than the client, the client’s representatives, or the members, associates, or employees of the lawyer’s law firm.” Tex. Disciplinary R. Prof’l Conduct 1.05(b) (2005).