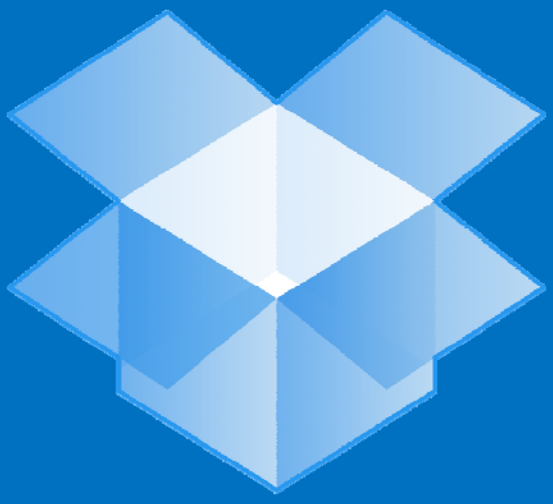
ETHICAL CONSIDERATIONS OF USING DROPBOX IN YOUR LAW FIRM



ACCELLIS TECHNOLOGY GROUP

Introduction

Lawyers have professional obligations to their clients that include a duty to keep client information confidential. Some commentators have questioned whether storage of information on the cloud is consistent with this duty.

The purpose of this whitepaper is to contemplate whether or not it is ethical for attorneys to use Dropbox.

Generally, the ethics of using Dropbox are formalized in ethics opinions, bar association rules, and local, state, and national laws. Whether or not you may use it comes down to where you practice, what you practice, and even your financial partners.

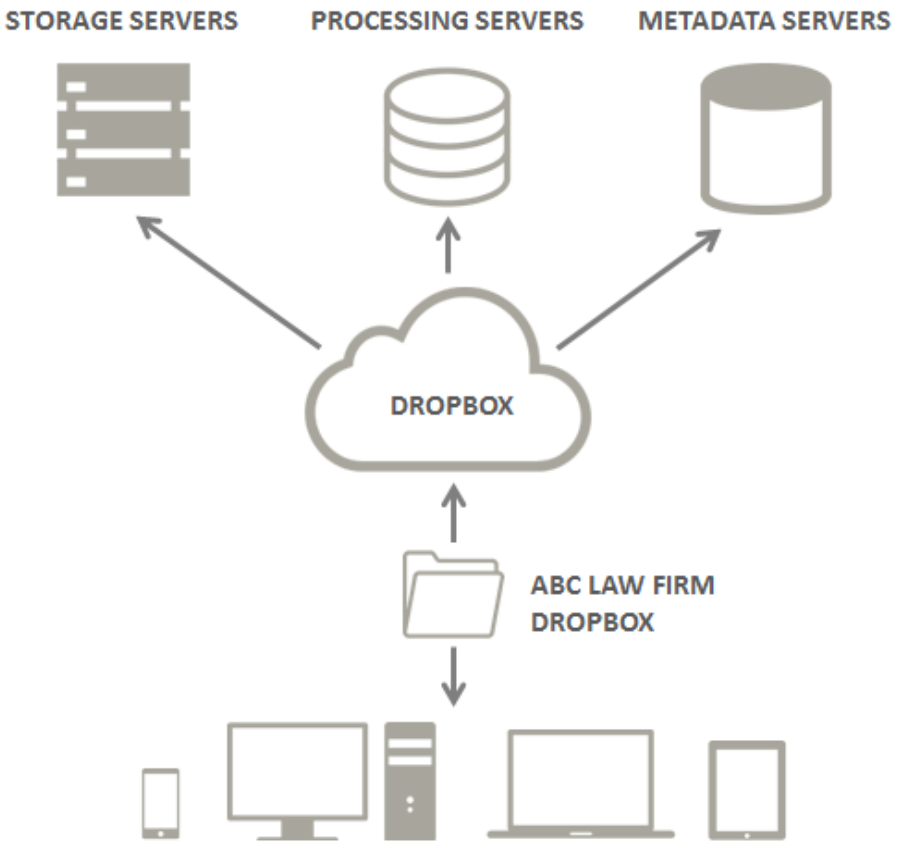
This whitepaper will review what those opinions, rules, and laws have to say about the matter, and whether or not an attorney or a law firm should condone the use of Dropbox in the workplace.

What is Dropbox?

Dropbox is a file hosting service that allows firm users to access all firm data files either locally (by PC or laptop while in the office) or via the cloud (by web browser from anywhere in the world). Dropbox also serves as a firm-wide Data Backup and Disaster Recovery Policy since, in concert with local backups, it provides 100% data security against data loss or Acts of God.

Thus Dropbox is best characterized as: the storage, hosting, delivery, backup, and DR associated with all of your digital files. If you are in the office, you work with files locally. Once saved, they are automatically synced to the cloud. When out of the office, users can access that cloud from mobile phones, tablets, laptops, and other peripherals, giving them 24x7 access to firm documents.

So, quite simply (and ideally), here is how information in your Dropbox is stored and delivered, however, as you continue reading, you'll find out why it's much more complex than this:



What Dropbox DOES NOT Do

Dropbox alone is insufficient for your firm's data backup and DR needs. It backs up your files only, not your server system state, profiles, databases (i.e., Exchange, SQL), etc. Thus, if you use *only* Dropbox for your backup needs, and you need to recover your data, you'll only get the files, not all the other residual engineering work that went into programming your PC's and servers. To ensure the firm's *entire* data store is backed up, including databases, system state and the like, you must use Dropbox *in concert with* local backup procedures – including backup media (i.e., hard drives, tapes, etc.) and backup software (i.e., Symantec Backup Exec)."

Also, Dropbox is NOT a document management system, like Worldox or NetDocuments. It's simply your storage, hosting, and backup repository. For instance, there is no document profiling (saving a document in the Client/Matter/DocType schema). You can profile documents, but this is done manually by creating folders and subfolders. In Worldox or NetDocuments, this would be automated.

What You Should Know When Considering Dropbox

There are numerous considerations that affect whether or not a lawyer or a law firm may use Dropbox. Here we outline some of those variables and provide numerous resources for you to use in making that determination.

1. The Dropbox Business Agreement

While the Dropbox Business Agreement is often ignored, its importance must be stressed when contemplating the use of Dropbox in your firm.

The following statement is of paramount concern and, often, is the only objection to Dropbox:

> *1(b): "Customer agrees that Dropbox may transfer, store, and process Customer Data in location other than Customer's country."*

Generally, if you check with that particular jurisdiction (out of country) where the data is known to flow, and make sure the security and compliance laws are equivalent or greater to local, state, and federal laws, then you will be fine to use Dropbox (see: PA Ethics Opinion 2011-200). That said, if you work with banks,

insurance companies, or healthcare organizations, you are most likely forbidden from offshore data storage – categorically.

> *5(a): "…this Agreement does not grant (i) Dropbox any Intellectual Property Rights in Customer Data…"*

Some providers were making the claim that anything they host for you gives them the authority to license and or make use of that intellectual property. After some publicity and outrage, most have drawn back from that hard stance.

> *5(b): "Customer grants Dropbox only the limited rights that are reasonably necessary for Dropbox…to offer the Services…this permission also extends to trusted third parties…(e.g., payment provider used to process payment of fees)…"*
>
> *10(a): "…neither customer nor Dropbox and its affiliates, suppliers, and distributors will be liable…even if the party knew or should have known that such damages were possible and even if a remedy fails of its essential purpose."*
>
> *11(b): "Customer and Dropbox agree to resolve any claims relating to this Agreement…through final and binding arbitration…the arbitration will be held in San Francisco (CA), or any other location both parties agree to in writing."*

These clauses are noncontroversial for most firms. Dropbox does need certain rights in order to administer the service; involved in that is some general level of immunity or indemnification; and for conflicts that arise therein, Dropbox pushes you into arbitration.

Some argue the rise of arbitration clauses (e.g., as found in employment agreements) are anti-consumer insofar as they unduly truncate due process:

> *"The presence and proliferation of arbitration in the United States is impossible to ignore. We must therefore understand how arbitration differs from mediation, and, perhaps more importantly, how it differs from a case decided by a judge in a court of law." ("The Rise of Arbitration Legislation" and "Arbitration Vs. Litigation". National Paralegal College, 2014)*

Though there are real concerns with mandatory arbitration, there aren't any alternatives available to you other than hosting your own cloud. Further, we don't know of any ethics opinions or rules that arbitration might violate. Most major software companies are embedding arbitration clauses into their contracts and the trend is accelerating.

Another potential factor is the jurisdiction in which a lawyer may seek relief; this will be restricted to California. As with arbitration, we have found no evidence that this affects your ethical duties. Here's how it reads:

> *11(c): "Either party may bring a lawsuit in the federal or state courts of San Francisco County…solely for injunctive relief to stop unauthorized use or abuse of the Services or infringement of Intellectual Property Rights…"*

2. The Dropbox Privacy Policy

> *"We may share information…but we won't sell it to advertisers or other third-parties."*
>
> *"To provide you with the Services, we may store, process and transmit information in locations around the world - including those outside your country. Information may also be stored locally on the devices you use to access the Services."*

Regarding the sharing of information, the Privacy Policy limits data sharing to others working for Dropbox, your firm users, third-party applications you authorize (i.e., integration with Amicus Cloud or Clio), and for purposes of law and order such as, a) compliance with law, b) protect persons from death or serious bodily injury, c) prevent fraud or abuse, or d) protect Dropbox's property rights. What is important is that they will not sell it.

The second quote is of significant concern for two reasons: 1) as already mentioned, moving data overseas can be a problem, and 2) if data is saved to local devices (i.e., phones, tablets, laptops, PC's) those devices become security and privacy failure points for the firm. See *section 6* for more on "local data" and why this presents problems for some law firms.

3. State & National Bar Association Rulings

Bar Association rulings and opinions shape the privacy conversation and provide the necessary scrutiny for or against using Dropbox, depending on those variables common to your firm. Generally, cloud computing is completely valid and ethical.

The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility, Formal Opinion 2011-200, rendered an opinion on the ethical obligations of attorneys using cloud computing while fulfilling the duties of confidentiality and preservation of client property:

> *"In response to this question, this Committee concludes: Yes. An attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks."*

This opinion translates to: you may use the cloud, but only if you, the attorney, take "reasonable care" to assure confidentiality and security.

"Reasonable care" is defined in the same opinion as ensuring, 1) backing up of data, 2) installing/use a firewall, 3) limiting info provided to others to what is required, needed, or requested, 4) avoid inadvertent disclosure, 5) verify identify of individuals to whom attorney provides confidential info, 6) refusing to disclose confidential information to unauthorized individuals, 7) protecting electronic records containing confidential data, including backups, via encryption, and 8) implementing electronic audit trail procedures.

In ABA Formal Opinion 99-413 (March 10, 1999), the American Bar Association concluded that using e-mail for professional correspondence is acceptable; it also concluded that unencrypted email poses no greater risks than other communication modes commonly relied upon, but this assessment is qualified with, "if the method affords a reasonable expectation of privacy."

In ABA Formal Opinion 08-451 (August 5, 2008), the American Bar Association concluded that the ABA Model Rules generally allow for outsourcing of legal and non-legal support services if the attorney ensures compliance with competency, confidentiality, and supervision ("Locked Down: information security for law firms". Nelson, Sharon D. American Bar Association, 2012. ISBN: 978-1-61438-364-2)

In the Illinois State Bar Association Ethics Opinion 10-01 (July 2009) we read a continuation of the trend that outsourced services are ethical:

> *"[a] law firm's use of an off-site network administrator to assist in the operation of its law practice will not violate the Illinois Rules of Professional Conduct…"*

4. State Laws

Most states have general security laws, breach notice laws, and secure disposal laws for *personally identifiable information* (or "PII") that outline a lawyer's obligations to secure and protect PII. These complement and at times overlap with other local and national laws, and with bar association rules, guidelines, and opinions.

General Security

General security laws can govern physical security requirements, like alarms systems, UPS (backup power), surveillance cameras, penetration auditing, incident response plans and disaster recovery plans. They can also consider authentication, patching, encryption, backup, browsing, and other IT imperatives. They may dictate compliance with certain email security standards; or certain best-practices for dealing with mobile peripherals; or they might specify a particular way to manage or secure VPN, wi-fi, or other networks.

> "If Dropbox gets breached, and your customer's PII is stolen, who's liable: the firm or Dropbox?"

Breach Notification

In instances where you or your provider (i.e., Dropbox) suffers data loss, always immediately notify your client. As a client of Dropbox, they will immediately notify you. This is important because consumers, including you, need to take immediate action in order to re-secure accounts, passwords, and other information.

Secure Disposal

Machines used to house PII that are decommissioned by the firm can be required by law to be "wiped" to some satisfactory level (usually guided to some standard by noncommittal terms like "reasonableness" or "competency"). This involves incineration, a well-placed sledgehammer, or wiping data through the use of powerful magnets. Regardless of how, you can't simply throw away a PC or server and consider the job done.

Secure disposal laws also beg the question: what if I want to leave Dropbox, or what if Dropbox goes bankrupt, or what if Dropbox moves my data from one server to another; do any or all of the hard drives (that once housed your PII) have to be forcibly destroyed? Does Dropbox have to prove this to you?

Questions like these may be very difficult to answer. What if Dropbox gets breached, and your customer's PII is stolen? Who's liable: the firm or Dropbox? Dropbox includes indemnification in its agreement but the lawyer, too, has indemnification if

the due diligence was performed and documented (i.e., if "reasonable care" was taken).

State laws strengthen consumer rights and increase the burden on lawyers to keep data reasonably safe and secure, especially when that data contains personal information. But remember that since the pace of technology is fast, a lot of questions like these don't have highly formalized answers yet.

> "Any time a document is accessed remotely (that's to say, not 'locally') via some peripheral device, that device stores data. This means you are now walking around with PII."

5. National Laws

National laws, too, help outline your ethical responsibilities and provision to individuals certain rights, including that privacy be understood as a right within its own domain.

The U.S. Supreme Court established an individual right to privacy in *Griswold v. Connecticut* (1965), finding privacy predicate to exercise of the fundamental freedoms guaranteed by the Constitution (further noting the first Eight Amendments are not an exhaustive list).

Individuals have protections established in Fair Credit Reporting Act, the Privacy Act, the Electronic Communications Privacy Act, and Health Insurance Portability and Accountability Act [McFarland, p.66].

These acts aim to simplify the equation and set of the following standards for privacy of *personal information*: collect only the data you need, minimize cross database "matching", keep data safe, keep data up to date and accurate, and provide the same access to those individuals whom the data references [see: *The Privacy Act*, 1974, enacted in the wake of Watergate].

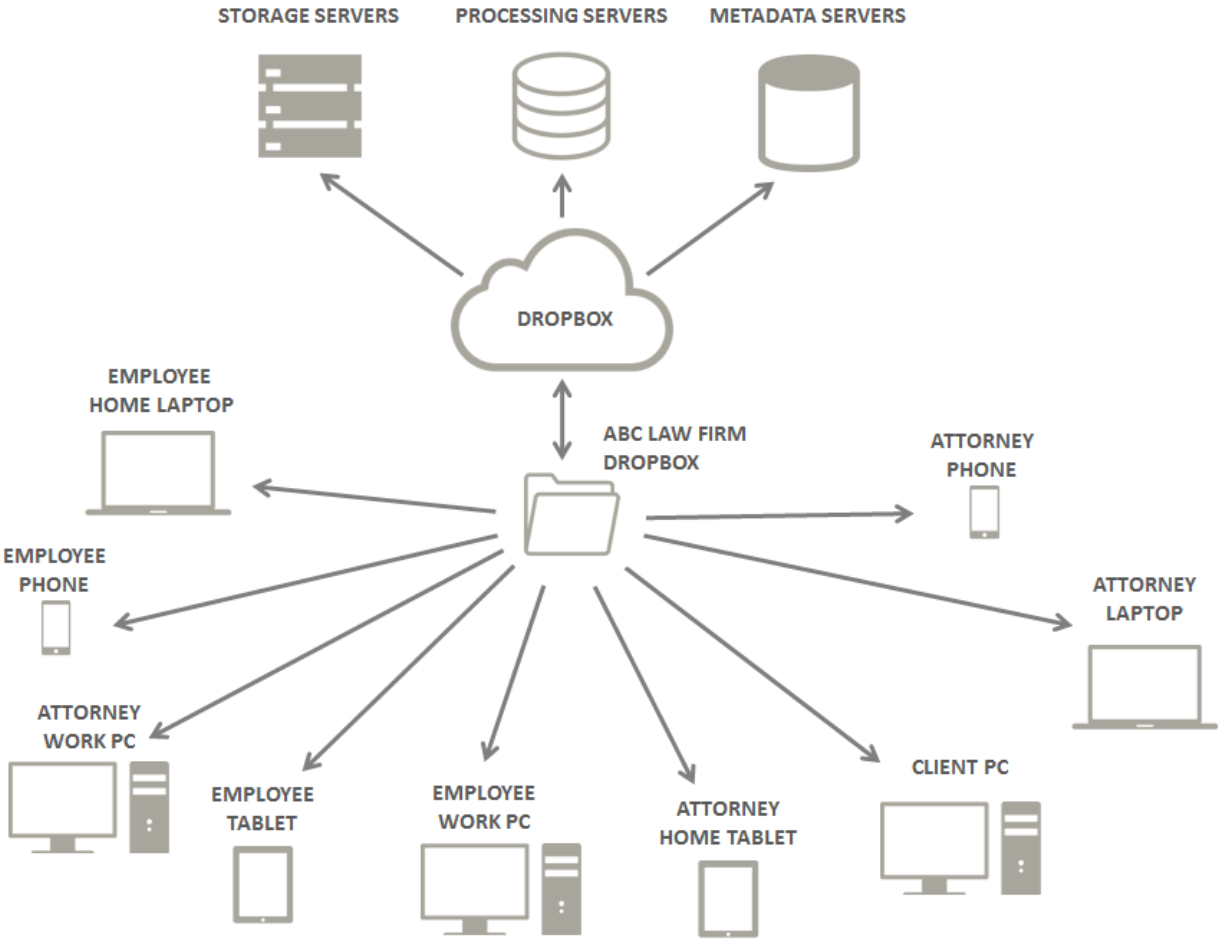
6. Local Data

One important piece of this puzzle, already hinted at, is that Dropbox does a great job at making all your IP accessible. In fact, it does this so well, that you should be concerned.

Any time a document is accessed remotely via some peripheral device, that device stores data. This means you are now walking around with PII. Thus, if you enable all firm members to access any document from any device, you are increasing the likelihood of a security event. It could be that, instead of worrying about ten PC's at

your office housing PII, you now have to worry about an additional ten home PC's, ten laptops, ten tablets, and or ten mobile phones.

So our illustration from page 3 describing how your information is stored and shared on Dropbox actually looks more like this:



Since lawyers have an ethical obligation to secure PII, any device (i.e., phone, tablet, laptop, PC, server, VM, Chromebook, netbook, or other) that accesses Dropbox will absolutely require: 1) password protection (ideally, a "strong" password), 2) periodic password expiration, 3) remote locate, lock, and wipe capabilities, 4) antivirus and antispam, and 5) should be included in your IT management schema for all hardware and software assets; this might include the need for content filtering for categories of websites, and or outright rejection of certain mobile or desktop applications.

Dropbox for Business

While firms should remain skeptical of storing sensitive content on someone else's servers, that's not to say that they should abandon the idea all together. Dropbox for Business offers robust security controls for firms that still want to use it to help improve productivity and organization. A firm that is insistent on using Dropbox should choose the Business version.

Dropbox for Business is different from a personal Dropbox account, but includes more security features such as administrative logging, remote wipe, sharing controls and even an Events page where you can see just about every action any user has taken in the account including uploading, changing, sharing and deleting documents. Firm administrators can also see sign-ons, password changes, and devices linked. Dropbox for Business also uses strong cipher encryption in transit and at rest, as well as file segmentation and hashing to anonymize stored data. Administrators can secure accounts even further with authentication features like single sign-on (SSO) support and two-step verification.

	Dropbox	Dropbox Pro	Dropbox for Business
Price	Free	$9.99 / user / month	$15 / user / month –or– $795 / year (for 5 users)
Storage	2 GB	1 TB	As much as you need
Core Dropbox Features			
Best-in-class sync and file sharing	✓	✓	✓
256-bit AES and SSL encryption	✓	✓	✓
2-step verification and mobile passcodes	✓	✓	✓
Enhanced Security			
Version history and deletion recovery	30 days	Up to 1 year	Unlimited
Remote wipe	X	✓	✓
Sharing permissions on links & folders	X	✓	✓
Account transfer	X	X	✓
Prevent sharing outside of the team	X	X	✓
Team Management			
Track logins, devices and locations	X	X	✓
Centralized team billing	X	X	✓
Easily add and remove members	X	X	✓
SSO and Active Directory	X	X	✓
Support			
Priority email support	X	✓	✓
Live support	X	X	✓

7. Additional Resources

- "Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology" (September 20, 2010)
- September 2011 revised proposals for amendments to the Model Rules concerning Outsourcing, Technology and Confidentiality, and Technology and Client Development: https://tinyurl.com/3op6tx3
- R. Acello, "Get Your Head in the Cloud," ABA Journal (April 2010)
- D. Kawairamani, "Cloud Computing: Ethical Shades of Gray," New York Law Journal (March 22, 2011)
- J. McCauley, "Cloud Computing – A Silver Lining or Ethical Thunderstorm for Lawyers?" Virginia Lawyer (February 2011)
- Sam Glover, "Is File Sync (Dropbox, et al.) Safe?," Lawyerist (February 9, 2013) http://lawyerist.com/q-is-file-sync-dropbox-et-al-safe/

The Verdict: Is Dropbox Ethical?

Verdict: It is ethical to use Dropbox, provided you have taken the necessary precautions to meet your ethical and professional obligations to protect client information.

That said, all firms need to fully research local, state, and national rules and guidelines, precedent, and other firm-specific nuances such as compliance with financial partners. Certain banks or insurance companies will categorically reject your use of Dropbox. This means Dropbox will be okay for some firms, but not okay for others.

Remember: You need to be as vigilant now as ever. Terms and conditions change over time (often quite silently); companies flop; people get sued and lose; and what was once a no-brainer yesterday, may be a colossal mistake today. As with the employment of any technology, you must stay attune to the changing legal, ethical, and business landscapes that guide whether or not this technology is good fit for your business.

**This is not a legal opinion.*

About Accellis Technology Group

Accellis Technology Group is one of the nation's leading providers of IT Consulting & Managed Services for the legal industry. We help law firms of all sizes reduce their day-to-day administrative tasks so they can focus on growing their business. Whether you need quicker access to help desk support, proactive IT management, improved security, or custom software solutions, Accellis can provide the expertise and direction to meet your goals. Our unique approach often saves clients thousands every month, while improving support, network security and efficiency.

Additional whitepapers and articles by Accellis Technology Group can be found at http://accellis.com/blog/, including:

- The Law Firm Cyber Security Threat Matrix
- 10 Mistakes Law Firms Make With Their Practice Management Software
- A Complete Guide to Managed Services for Law Firms

Contact information:

Michael O'Neill
Accellis Technology Group
Phone: 216-662-3200
Email: moneill@accellis.com
Website: www.accellis.com