Cloud Technology: Ethical Issues for Lawyers

Compiled by Daniel Vincent, 2015 J.D. Candidate, BYU J. Reuben Clark Law School, 2015 M. Acc. Candidate, BYU Marriott School of Management

State Ethics Opinions

A more thorough summary of the ethics opinions issued from state bar associations below may be found at http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html

All of these opinions permit the use of cloud technology and reflect a "reasonable care" standard. Summary requirements are outlined below (taken from ABA website). Common threads between the states seem to include:

(1) Consulting an expert on data security if the lawyer is not an expert;
(2) Periodically reviewing security measures and best practices;
(3) Thoroughly reviewing a provider's security measures before contracting with it (due diligence); and
(4) Determining the client's specific security needs and desires.

Alabama

Opinion 2010-02 (2010)

- Know how provider handles storage/security of data.
- Reasonably ensure confidentiality agreement is followed.
- Stay abreast of best practices regarding data safeguards.

Arizona

Opinion 09-04 (2009)

- "Reasonable security precautions," including password protection, encryption, etc.
- Develop or consult someone with competence in online computer security.
- Periodically review security measures.

California

Formal Opinion 2010-179 (2010)

- Evaluate the nature of the technology, available security precautions, and limitations on third-party access.
- Consult an expert if lawyer's technology expertise is lacking.
- Weigh the sensitivity of the data, the impact of disclosure on the client, the urgency of the situation, and the client's instructions.

Connecticut

Informal Opinion 2013-07 (2013)

- Lawyer's ownership and access to the data must not be hindered.
- Security policies and processes should segregate the lawyer's data to prevent unauthorized access to the data, including by the cloud service provider.

Florida

Opinion 12-3 (2012)

- Ensure provider has enforceable obligation to preserve confidentiality and security, and will provide notice if served with process.
- Investigate provider's security measures
- Guard against reasonably foreseeable attempts to infiltrate data.

Iowa

Opinion 11-01 (2011)

- Ensure unfettered access to your data when it is needed, including removing it upon termination of the service.
- Determine the degree of protection afforded to the data residing within the cloud service.

Maine

Opinion 207

- Ensure firm technology in general meets professional responsibility constraints.
- Review provider's terms of service and/or service level agreements.
- Review provider's technology, specifically focusing on security and backup.

Massachusetts

Opinion 12-03 (2012)

- Review (and periodically revisit) terms of service, restrictions on access to data, data portability, and vendor's security practices.
- Follow clients' express instructions regarding use of cloud technology to store or transmit data.
- For particularly sensitive client information, obtain client approval before storing/transmitting via the internet.

New Hampshire

Opinion #2012-13/4

- Have a basic understanding of technology and stay abreast of changes, including privacy laws and regulations.
- Consider obtaining client's informed consent when storing highly confidential information.
- Delete data from the cloud and return it to the client at the conclusion of representation or when the file must no longer be preserved.
- Make a reasonable effort to ensure cloud providers understand and act in a manner compatible with a lawyer's professional responsibilities.

New Jersey

Opinion 701 (2006)

- Vendor must have an enforceable obligation to preserve confidentiality and security.
- Use available technology to guard against foreseeable attempts to infiltrate data.

New York

Opinion 842 (2010)

- Vendor must have an enforceable obligation to preserve confidentiality and security, and should notify lawyer if served with process for client data.
- Use available technology to guard against foreseeable attempts to infiltrate data.
- Investigate vendor security practices and periodically review to be sure they remain up-to-date.
- Investigate any potential security breaches or lapses by vendor to ensure client data was not compromised.

Nevada

Opinion 33 (2006)

- Chose a vendor that can be reasonably relied upon to keep client information confidential.
- Instruct and require the vendor to keep client information confidential.

North Carolina

2011 Formal Ethics Opinion 6 (2012)

- Review terms and policies, and if necessary re-negotiate, to ensure they're consistent with ethical obligations.
- Evaluate vendor's security measures and backup strategy.
- Ensure data can be retrieved if vendor shuts down or lawyer wishes to cancel service.

Ohio

Informal Advisory Opinion 2013-03 (2013)

- Competently select appropriate vendor.
- Preserve confidentiality and safeguard client property.
- Provide reasonable supervision of cloud vendor.
- Communicate with the client as appropriate.

Oregon

Formal Opinion 2011-188 (2011)

- Ensure service agreement requires vendor to preserve confidentiality and security.
- Require notice in the event that lawyer's data is accessed by a non-authorized party.
- Ensure adequate backup.
- Re-evaluate precautionary steps periodically in light of advances in technology.

Pennsylvania

Formal Opinion 2011-200 (2011)

- Exercise reasonable care to ensure materials stored in the cloud remain confidential.
- Employ reasonable safeguards to protect data from breach, data loss, and other risk.
- See full opinion for 15 point list of possible safeguards.

Vermont

Opinion 2010-6 (2010) (scroll down)

- Take reasonable precautions to ensure client data is secure and accessible.
- Consider whether certain types of data (e.g. wills) must be retained in original paper format.
- Discuss appropriateness of cloud storage with client if data is especially sensitive (e.g. trade secrets).

Virginia

Legal Ethics Opinion 1872 (2013)

- Exercise care in selection of the vendor.
- Have a reasonable expectation the vendor will keep data confidential and inaccessible.
- Instruct the vendor to preserve the confidentiality of information.

Washington

Advisory Opinion 2215 (2012)

- Conduct a due diligence investigation of any potential provider.
- Stay abreast of changes in technology.
- Review provider's security procedures periodically.

Best Practices Articles

Cloud Computing by Judge Herbert B. Dixon Jr. 51 No. 2 Judges J. 36 (2012)
This brief article provides a description of cloud computing and lists a few of the more prominent services then available.

Navigate the Cloud by James N. Kunick 210 Managing Intell. Prop. 58 (June 2011)
While focused on ways that IP lawyers can advise business clients that are considering moving to cloud-based systems, the principles are applicable to attorneys making the same considerations as well. Considerations include:

- Having a robust written contract addressing:
    - Compliance with all relevant data security laws as well as law firm standards
    - Maintenance protections against loss or destruction of data
    - Who will bear the costs of remedying a data breach
- Monitoring compliance with audits
- Maintain insurance in case of data breach
- Ensure appropriate rights regarding termination and suspension of service

Flying Safely in the Cloud by Brett Burney Law Practice Magazine, Volume 37 Number 2 (March/April 2011)
This article discusses the need for "reasonable care" in selecting a cloud provider as well as what parameters constitute "reasonable precautions" as determined by various jurisdictions

Cloud Computing/Software as a Service for Lawyers (ABA LRTC)
This article provides the basics of cloud computing, geared toward someone who is unfamiliar with the idea and may want to consider using it for her firm. Below are some questions for consideration:

- Questions to consider regarding availability/access:
  - How often do I need to access my legal software outside of the office?
  - Is the SaaS compatible with my preferred platform/device/web browser?
  - Do I work in an area that's prone to disaster or other business continuity threats?
  - Do I have reliable access to the Internet from work? From home? On the road?
  - Does the provider offer (or would it be willing to negotiate) a Service Level Agreement (SLA) that guarantees a certain level of service (e.g. uptime, accessibility, etc.)?
  - Are any relevant guarantees or disclaimers of liability included in the provider's Terms of Service (TOS)?
- Questions to consider regarding ethics/security:
  - How does the vendor safeguard the privacy/confidentiality of stored data?
  - 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?
  - What is the history of the vendor? Where do they derive their funding? How stable are they financially?
  - Can I get my data "off" their servers for my own offline use/backup? If I decide to cancel my subscription to the software, will I get my data? Is data supplied in a non-proprietary format that is compatible with other software?
  - Does the vendor's Terms of Service or Service Level Agreement address confidentiality and security? If not, would the vendor be willing to sign a confidentiality agreement in keeping with your professional responsibilities?
- Cost questions to consider:
  - What are the monthly costs for the SaaS option, and are discounted rates available for non-lawyer employees like paralegals, legal assistants, and law clerks?
  - Does the vendor require a contractual agreement to maintain service for a certain amount of time (e.g. 12 months, 24 months)?
  - How does the cost of the SaaS solution compare over a two or three year period to the cost of a comparable traditional software license?
  - What's the pricing history of the SaaS solution? How often are monthly rates increased?
  - Are there any incidental costs for the SaaS solution, like data backup or support?

The Ethics of Cloud Computing for Lawyers, Nicole Black, GP Solo E Report Vol. 2, No. 2

Cloud Computing for Lawyers Author(s): Nicole Black Sponsor(s): ABA Law Practice Division Publ. ISBN: 978-1-61632-884-9 Product Code: 5110724 2012, 222 pages, 7x10 $79.95.

One more question to ask: