Mobile and Cloud Computing:
Trends, Advice and Ethical Considerations

Stewart Whaley, Esq.
stewart@logicurrent.com
http://logicurrent.com/cle

Agenda

I. Why are cloud and mobile computing important?
II. What are cloud and mobile computing?
III. What are the ethical issues for lawyers?
IV. How to evaluate vendors and technology.

“We are now in the 5th major technology cycle of the past half century.”
- Mary Meeker, Kleiner Perkins

“By 2016 there will be over 10 billion mobile-connected devices.”

“In all professional functions a lawyer should be competent...”
- Preamble, Arkansas Model Rules of Professional Conduct

I. Why are cloud and mobile computing important?

The Internet ran out of room, unable to meet the demand for connected devices...seriously.


Internet Protocol Version 4 (IPv4) = 4.29 billion IP addresses (4,290,000,000)
Internet Protocol Version 6 (IPv6) = 340 undecillion IP addresses

340,282,366,920,938,463,463,374,607,431,768,211,456 address available
Practically ALL devices will be connected to the internet in the near future, facilitated by mobile and cloud computing technologies.

Technology has become thoroughly entrenched in substantive law. (Who doesn’t love e-Discovery?)

Technical competence is a recurring theme in legal ethics opinions across the country and more important as society moves further into mobile, cloud and social computing.

Converging technology is creating a “mobile-first web,” and mobile devices are now MORE important than desktops.

Mobile devices are now used more than desktops for internet-based activity and many “traditional” computing tasks.

Common misconceptions:

• Mobile usage in rural states is not important or widespread.

• Low-income clients aren't mobile/tech savvy.

    AR is among the rural leaders in mobile adoption.

    Often there is one device for all computing, telephony, and internet needs.

Addressing technology issues engrained in client legal issues and your practice management is quickly becoming the norm.

The ethical analysis and compliance required when address these issues is largely driven by:

    Rule 1.1 Competence

    A lawyer shall provide competent representation to a client.

    Rule 1.6 Confidentiality of Information

    (a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent

II. Cloud / Mobile Computing Defined

    Mobile computing: human–computer interaction by which a computer is expected to be transported during normal usage.

Components

    I. mobile communication
       a. Cellular data services like 3G, 4G within cell tower range
b. WI-FI via public/private networks up to +/-1000 ft.
   i. public WI-FI is generally unsecure and a recurring topic in ethical opinions)
c. Satellite access to fill in the gaps

II. mobile hardware
   a. Variety of devices that provide a platform for mobile computing
      i. Cell phones, tablets, laptops
   b. Augmented reality glasses and contacts in 2014

III. mobile software
   a. Provides basic device functionality (cellular connection, GPS, etc.)
   b. May include additional vendor and 3rd party applications

Mobile computing is bringing a massive disruption in the delivery of goods and services.

Mobile commerce (mCommerce) driven by “app stores” and in-app purchasing is accelerating at a much greater rate than eCommerce.

Consumers are growing accustomed to on-demand goods and services delivered to mobile devices.

Cloud computing: the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices:

   a. as a utility (like the electricity grid)
   b. over a network (typically the internet).

Cloud computing offers many benefits to desktop/stationary users but the accessibility, cost and power make mobile computing significantly more effective and appealing.

Cloud computing is about how the service or software is delivered, not what you are doing.

Software as a Service (SaaS):

sometimes referred to as "on-demand software", is a software delivery model in which software and associated data are centrally hosted on the cloud. SaaS is typically accessed by users using a thin client via a web browser


Google Docs is a good example. The spreadsheet resources are coming from a Google web farm in South Dakota or failover site offshore. Your device (desktop PC, iPad, phone) is just a terminal.

I. Three components of the cloud
a. **Infrastructure**
   i. Raw computing power or storage online for free/pennies/dollars
   ii. Let the experts deal with upgrades and maintenance (ex. Amazon Web Services)
   iii. We all deal with this to some extent when we are use the internet but generally won’t interact directly with vendors at this level
   iv. **WARNING:** It is critical to assess the security and privacy policies of these vendors, even if they are a downstream service used by YOUR cloud vendor

b. **Platforms**
   i. Allow developers to build applications that run on the platform provider’s infrastructure. (ex. Windows Azure, force.com, Google app engine, Facebook)
   ii. The platform can even be offered inside a company’s primary business. For example, Facebook has a massive platform that allows developers to build games and applications inside the Facebook environment.

c. **Applications**
   i. Applications developed and hosted on cloud infrastructure and platforms.
      1. **eMail:** Google Mail, Hotmail
      2. **Research:** LexusNexus, FastCase
      3. **Practice mgmt:** MyCase, Clio, Rocket Matter, Kemps
      4. **File mgmt:** Dropbox, Box, SugarSync,
      5. **Backup:** SOS, Mozy
   ii. Subscription fees, free or low up-front cost, latest versions.
   iii. Low-cost access to amazing computing and storage.
      1. Analyze on a case-by-case basis
      2. Overall cost or privacy and security issues may limit or exclude vendors
   iv. Solo and small firms can access IT resources equal to the largest firms

Cloud vendors must scale to peak capacity and redundancy for massive volume and an array of worst-case scenarios. Your firm will never have the in-house resources for that kind of “what-if” scenario. **NOTE:** Cloud computing is not a magic bullet or necessarily good for YOUR situation.

Ross Kodner’s CLE materials offer practical, real world examples of the cost-benefit analysis for a small practice. He finds the “low cost” theory doesn’t always pan out in practice: [http://www.microlaw.com/cle-downloads.html](http://www.microlaw.com/cle-downloads.html)

III. What are the ethical issues?

   **Rule 1.1 Competence**
A lawyer shall provide competent representation to a client.

**Rule 1.6. Confidentiality of Information**

(a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent

Cloud/mobile opinions generally favor cloud and mobile computing if the attorney acts “reasonably,” but lack clear guidance for assessment.

**Below is a list of relevant, opinions worthy of review.**

In particular, the first three opinions offer guidance and analysis that is very useful. These will serve as our primary guide for the remainder of this CLE.

1. North Carolina 2011 Formal Ethics Opinion 6 (Cloud computing, Saas)
2. Pennsylvania Formal Opinion 2011-200 (Cloud computing, SaaS)
4. Iowa State Bar Assoc. Ethics Opinion 11-01 (Cloud computing and SaaS);
5. Oregon State Bar Assoc. Ethics Opinion 2011-188 (Third-party cloud vendor)
6. New York State Bar Association Ethics: Opinion 842 (Cloud storage)
7. Maine State Bar Professional Ethics Commission Opinion 194 (Third-party cloud vendor)
8. ABA Commission on Ethics 20/20 (multiple)

How do we determine what the risks are and what actions to take?

1. Rules of Professional Conduct
2. State Bar Opinions

How do we guard against

1. inadvertent disclosure
2. hacking
3. vendor response to subpoenas
4. other issues

The primary concerns in all of these opinions are competence and confidentiality.

**Rule 1.1 Competence**

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

**Maintaining Competence**
[6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

**Rule 1.6 Confidentiality of Information**

(a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

[1] …disclosure by a lawyer of information relating to the representation of a client…see 1.18 prospective client; 1.9(c)(2) prior representation; 1.8(b) and 1.9(c)(1) use of information

[2] A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation.

For our purposes, application of Rule 1.1 and Rule 1.6, applies to storage and transmission of client data.

Conundrum for lawyers:

  Am I revealing client information when using cloud services (SaaS), storage, mobile devices? How do I determine if the data is being safeguarded?

**North Carolina 2011 Formal Ethics Opinion 6**

Evaluating vendors in regards to **RULE 5.3 RESPONSIBILITIES REGARDING NONLAWYER ASSISTANTS**

Inquiry #1: Given [the] duties and needs [of Rule 5.3], may a law firm use SaaS?

Inquiry #2: Are there measures that a lawyer or law firm should consider when assessing a SaaS vendor or seeking to minimize the security risks of SaaS? (Software as a Service)

When reviewing SaaS contracts look for:

1. Inclusion in the SaaS vendor’s Terms of Service or in a separate agreement, detail on how the vendor will handle confidential client information
2. Look for terms that describe what occurs if the lawyer
   a. terminates use of the SaaS product
   b. the SaaS vendor goes out of business, or
   c. the service otherwise has a break in continuity,
      i. If any of the above occur, the law firm will have a method for:
         1. retrieving the data,
         2. the data will be available in a non-proprietary format or
         3. the law firm has access to the vendor’s software or source code
3. Vendor is contractually required to return or destroy the hosted data promptly at the request of the law firm.

Does an attorney violate the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties?

In accordance with the duties of confidentiality and competence, an attorney should consider the following before using a specific technology:

a) The attorney’s ability to assess the level of security afforded by the technology, including without limitation:
   - How the technology differs from other media.
     (Consider security issues of traditional mail versus email)
   - Whether reasonable precautions will increase security.
     (Placing privileged mail in desk outbox versus carrying it to post office)
   - Limitation on who is permitted to monitor the technology, to what extent and on what grounds.
     (Is a vendor or subcontractors required to interact with confidential information as part of their service?)

b) Legal ramifications to third parties of intercepting, accessing or exceeding authorized use of another person’s electronic information.
   - Generally an intentional example would be illegal or unethical, right?

This is kind of a ‘boogey-man’ topic to dissuade cloud usage in the legal industry.

   a. Hackers don’t really care about your legal/client data
   b. Adverse parties are barred by law and ethics.

However, for the mobile and WI-FI issues addressed in this opinion it is very important.

c) The degree of sensitivity of the information. The greater the sensitivity of the information, the less risk an attorney should take with technology.

d) Possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product, including possible waiver of the privileges.
Generally we feel protected by privilege, but what about Federal Rule 502(b)(2)?

... (2) the holder of the privilege or protection took reasonable steps to prevent disclosure.

e) The urgency of the situation. If use of the technology is necessary to address an imminent situation or exigent circumstances and other alternatives are not reasonably available, it may be reasonable in limited cases for the attorney to do so without taking additional precautions.

Consider New Orleans and Katrina or Little Rock’s Quapaw tornado in 1999, etc.

A solution like DropBox is not appropriate for privileged client files...or is it?

During Katrina, a fully vetted tape backup vendor located three blocks away is probably destroyed just like your firm’s office.

Moving client files to redundant DropBox servers just prior to disaster doesn’t look so bad.

f) Client instructions and circumstances.

Obviously, if client instructs you not to use certain technology you avoid it. If a particular client is a technophobe you might consider avoiding cloud storage, etc.

If you are aware that others have access to the client’s (or your) electronic devices or accounts or might intercept or be exposed to client information, you should avoid its use.

The California opinion above is highly attuned to the sensitivity of client information, but pales in comparison to Pennsylvania’s (Pennsylvania Formal Opinion 2011-200).

Pennsylvania also discusses client instructions and circumstances (“f” above) in great detail.

The opinion lists 30 bullet points (with 50 sub-bullets) covering how an attorney might exercise “reasonable care” when storing client information in “the cloud.”

IV. How do we evaluate vendors and technology?

Brief aside: Avoiding Malpractice

We have a good idea of the pros and cons of using cloud and mobile computing now.

But remember that many malpractice issues still trace back to two things

a. calendar/scheduling issues

b. client contact
Mobile and cloud vendors offer numerous opportunities to address both of these. If you never use any other cloud technology, please explore the possibilities in these two areas.

Some malpractice insurance providers offer discounts for electronic calendar synchronization.

Back to the main point, how do we evaluate?

If you don’t feel comfortable, ask for help from:

a. another attorney
b. a technology partner, or
b. the vendor

Areas of concern

I. Security
a. Physical security
   i. Location of data center: geological or weather issues, location secrecy, redundancy
   ii. employee access to servers or premises
   iii. Auditing and certifications
      1. SAS 70
         Statement on Auditing Standards (SAS) No. 70
      2. HIPPA
         Health Insurance Portability and Accountability Act
b. Application security
   i. SSL encryption
   ii. strong passwords
   iii. multi-step authentication
   iv. who are the vendor’s vendors?
   v. who are their customers?

Examine the vendor’s documentation and call them if anything is unclear. What are their physical and application security policies and practices?

For example, does the application force users to use security features? (free Google docs vs. enterprise Google docs)

II. Privacy
a. What will the vendor do with your data?
i. Google is notorious for various scanning, and processing of data for targeted ads and usage statistics.

b. Terms of Use
   i. Ensure the vendor doesn’t make any claims on your data or the clients.
   ii. Change in ownership of the vendor.
   iii. What happens to the data if services terminated?
       1. Immediately deleted?
       2. Escrow options
       3. Data extracts in useable format?
   iv. Response to subpoenas
       1. Will the vendor notify you of a subpoena prior to action so you can gain a protective order? <unlikely>
       2. Is there ANY right to notification if the vendor responds? <unlikely>
   v. Enterprise vs. consumer services
       1. Contract terms may differ between offerings of same vendor.
   vi. Agreements to store data in specific jurisdictions
   vii. Service level agreements for availability
       1. Down time hours
       2. contiguous or cumulative
       3. Who bears the cost and how are credits applied?

Generally, the large vendors (Amazon, Google) will not negotiate terms.

Vendor and product examples

File sharing, syncing, backup
- DropBox
- Box
- SugarSync
- EverNote
- Mozy
- SOS Backup

Cloud-based practice management (Software as a Service)

All 3 of these vendors announced Application Programming Interfaces (API’s) in May 2012. API’s allow the applications to “talk” with other applications by passing data and instructions.

Expect significant integration between multiple vendors in the future. If starting a new practice, these are very interesting options due to price and future expansion via third-party developers.

- Clio
- MyCase
- RocketMatter
Mobile

Lookout http://mylookout.com

Mobile device security for Android and Apple phones

-Wipe data, backups, security, location

Prey

Similar to Lookout, but runs undetected in “stealth mode”

-Virtually impossible for thieves to detect its presence

Notes on WI-FI security

Public WI-FI is very susceptible to security breach and many public WI-FI networks are very unsecure. “Hacking WI-FI” yields +8.7 million Google hits

WI-FI is easy to hack because of:

1. Known exploits in encryption standards
2. Known exploits in hardware
3. Human tendency

Things you can do:

1. Don’t risk exposing confidential data to a WI-FI network.
   a. Don’t use it
   b. Or use a secondary device that doesn’t contain sensitive information
2. Hide your network name
3. Change your default router SSID
   a. A default network name of “LinkSys” is a good indication that you don’t take security seriously.
   b. A hacker immediately knows exactly what brand of hardware you have, too.
4. Use strong passwords
   a. Mixed case
   b. Mixed character
   c. Digits
   d. Long (at least 8 characters)
      Many hacks don’t even attempt to crack long passwords due to the exponential increase in resources and time.

How You Get Hacked:

1. HashTables and Rainbow tables
   a. Pre-compiled and processed lists of the most common router
SSID’s (device identification numbers) and derivations of the most commonly used passwords (p@ssw0rd, nimdA, etc.) can be found all over the internet.

b. These generally DON’T contain many long password combinations because of file size and processing time.

2. Device specific exploits
   a. Certain routers store information or “seed” their encryption keys in particular ways (for example, based off their default SSID)
   b. This information is also freely available online (Google)

3. Rent cloud-based hacking resources.
   a. Seriously.
   b. An NSA level encryption algorithm was broken in 49 minutes by a German hacker using rented Amazon cloud processors
   c. Cost = $2.10 per hour.
   d. When interviewed he stated that he did not try any passwords over 6 characters, so his processing time was kept to a minimum.
   e. This security flaw has been common industry knowledge for a couple of years. HOWEVER, it is still in widespread use, embedded in various hardware and software.