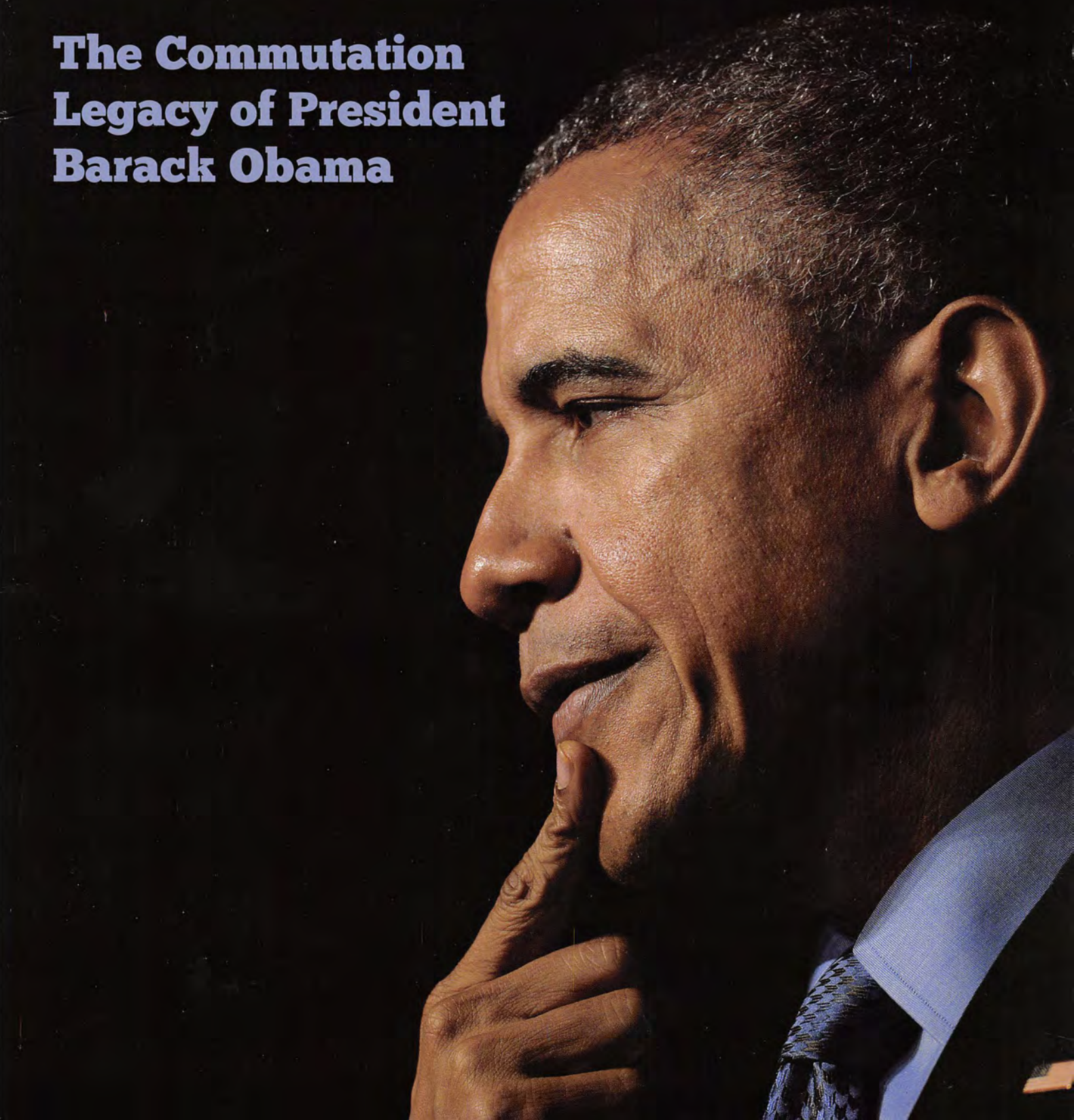
THE National Association of Criminal Defense Lawyers®
CHAMPION®
December 2016 WWW.NACDL.ORG

The Commutation Legacy of President Barack Obama



©Melpomene | AdobeStock

Cloud Computing for Criminal Lawyers: It's Not the Future Anymore

For many criminal lawyers, "the cloud" — a place where digital data is remotely created, stored, or shared using the internet — is a distant, dark, and foreboding place. Civil lawyers, with their abundant resources, staff and consultants, may choose to ascend there. But criminal practitioners are often more comfortable with their feet resting on familiar terra firma, and their hands clutching well-worn paper files and expandable folders.

This must change. And it already has. Whether they realize it or not, criminal lawyers spend much of their personal and professional lives in the cloud. They get movies from Netflix, not Blockbuster. They read case law on Fastcase, not in the *Federal Reporter*. They file motions through PACER/ECF, not court runners. They let Google, not their fingers, do the walking for contact information.

But criminal lawyers — indeed all lawyers — can and should do so much more in the cloud. Rather than conservatively clinging to past practices and deeply-engrained workflows, lawyers can and should use cloud-based resources not only to be better practitioners, but also to be better businesspeople. Through the cloud, lawyers can better find and protect client information. Through the cloud, lawyers can better collaborate and communicate with clients, co-counsel, and staff. Through the cloud, lawyers can make better use of their time, money, and limited resources.

So why the hesitancy to go there? Well, there is inertia: it is always easier to keep doing the same thing rather than making a change. Then, there are the bogeymen: the hackers, the NSA, and the ethics rules. And finally, there is the uncertainty: what cloud-based resources are available and which of those resources should a lawyer use?

Overcoming Inertia

In the short term, it is always easier to change nothing. Why would a lawyer learn a new skill, a new device, or a new process when the existing ones work fine? Typically, three things spur change: saving money, saving time, or improving quality. The cloud can do all three things for lawyers.

As to money, the cloud saves it. Paper is expensive, and not just when buying it in reams. Consider paper's secondary costs: the printers, copiers, and ink/toner cartridges to produce images on it; the clips, staplers, binders, and tabs to assemble it; the hole punches to punch it; the file folders to file it; the file cabinets to hold the file folders; the file rooms to hold the file cabinets; and, the file clerks to organize the file rooms. Walk into any Office Depot and look around. Take a good look. It is a bazaar for all things paper.

For lawyers, paper is a means to an end. Lawyers, unlike origami-ists, do not process paper for a living.

BY DANE S. CIOLINO

They process information — the facts, laws, people, and issues bearing on their matters. Lawyers who shift their information processing and storage to the cloud need less paper and fewer of its expensive accoutrements. Although the cloud holds lots of information, it cannot hold even one sheet of paper.

As to time, the cloud gives lawyers more of it. Paper information storage is not only expensive, but it is also inconvenient. To store information contained in paper, it takes time to punch holes in the document and put it into a file. To retrieve information contained in paper, it takes time go to the office, pull the file from the file cabinet, flip through the pages, and find the document. In contrast, when information is stored in the cloud, a lawyer can get it through a simple search wherever the lawyer is and whenever necessary. No trips to the office. No retrieving the file. No flipping through pages.

As to quality, the cloud improves it. Since lawyers are in the information analysis and advice business, anything that helps a lawyer to obtain, store, retrieve, and process matter-related information will improve the quality and timeliness of the lawyer's advice. The cloud allows lawyers to do all of these things more quickly and thoroughly.

Exposing the Bogeymen

"But I can't use the cloud, it's not safe there. The hackers and the NSA would see my confidential information. And the ethics rules don't allow that."

True, lions and tigers and bears are lurking about in the cloud. No one using the internet is safe from an attack — not Target, not the Democratic National Committee, and not lawyers. But the risk, although real, is overblown by the cloud's naysayers.

First, the cloud is probably more secure than most lawyers' current file storage systems. Do most lawyers know the security measures used by the file-storage facility where they store their closed records? Do most lawyers know who saw the files on their desks when their waste baskets were emptied last night? Do most lawyers know everyone who has a key to their offices? Do most lawyers back up their paper files with photocopy duplicates stored offsite in case of disaster? The answer to all or most of these questions is "no." Most lawyers are vulnerable *now* to unknown security and meteorological threats. And most slept fine last night.

Second, no offense, but hackers and the NSA really do not care much about lawyers. Remember the Matthew Broderick kid in *War Games*? He hacked into NORAD's ballistic-missile computers — not into a debt collection lawyer's cache of interrogatory answers. Hackers want credit card and deposit account numbers from financial institutions and merchants. They want embarrassing information about celebrities. The NSA wants ISIS. They are not interested in lawyers.

Third, virtually all lawyers are already using the cloud to transmit confidential information by email. Many use cloud storage facilities like Dropbox, Box, Google Drive or Microsoft OneDrive. Now.

Fourth, there are ways to be safe. Using basic internet hygiene and common-sense prophylactic measures can keep the digital intercourse between lawyers' local computers and cloud resources contagion free. *See infra* Security.

Finally, the "ethics rules" undoubtedly permit lawyers to store confidential information in the cloud. At least 20 bar associations have issued advisory opinions providing that cloud storage does not breach Rule 1.6, which requires a lawyer to exercise reasonable care to safeguard the confidentiality of client information.[1]

So much for those excuses.

Considering that there is no ethical impediment to using the cloud-based resources, which resources should lawyers use? The answer, it seems, is always "it depends." Although the answer does indeed depend on the nature of each lawyer's practice, each lawyer's financial wherewithal, and each lawyer's technological know-how, here are a few suggestions.

Moving to the Cloud

Having committed to use the cloud, how should lawyers get their practices up there? Not by operating their own cloud-connected servers. They should outsource instead. Lawyers practice law; they do not run servers. Lawyers would not try to build photocopiers for their own offices. Instead of running their own servers, lawyers should use Gmail, Google, Amazon, Dropbox, and other cloud-service providers that know what they are doing.

When outsourcing, lawyers should prefer industry leaders. Mom-and-pop and specialized providers will come and go. Gmail, Google, Amazon, and Dropbox are bent on (digital) world domination. They are here to stay.

After lawyers are in the cloud, they should remember that they are there for a reason and not for everything. Lawyers should prefer cloud-based solutions when they make life easier. Some tasks can be done locally, some can be done in the cloud, and others can be done either way. For example, a lawyer can draft a document in the cloud using Google Docs or draft it locally using Microsoft Word. In most instances, it will be easier to draft the document locally — as lawyers have done for decades. But, if a lawyer is working collaboratively with a client or another lawyer, it is far more efficient for everyone to work on a single, current version of the document in the cloud. When the collaboration is finished, *then* the lawyer can work locally to fine-tune the formatting and to finalize the document. Lawyers need to think about what they are doing and why they are doing it. Then, they need to do whatever is the easiest and most efficient way.

The most important thing lawyers will do in the cloud is store and retrieve documents, including Portable Document Files (PDF), Word files, and the like. Where and how should lawyers do this?

While there are dozens of reputable document-storage providers,[2] the industry leader is Dropbox. It is reasonably priced, reasonably secure, extremely reliable, cross-platform (that is, it runs on Windows, Mac, iOS, Android), and it plays nicely with other software and cloud-service providers.

Although document management is the most important thing lawyers will do in the cloud, they should consider doing other things. For example, several cloud-service providers offer total law practice management solutions, including the top three services, Clio, MyCase, and Rocket Matter. These services manage contacts, calendars, case documents, time tracking, and invoicing, among other things. All have robust security, backup, and integrations with other services such as Dropbox and Quickbooks.

Time, billing, and online payment are also readily available in the cloud. The industry leader for this service is Quickbooks Online. It allows lawyers to track billable time and expenses, and then to generate invoices based on hourly fees, fixed fees, or contingent fees. Most significantly, lawyers can use Quickbooks Online to email invoices directly to clients, who can pay with a credit card or checking account by clicking an online payment button in the email. Thereafter, they can quickly fol-

low up with statements to clients who do not pay timely. Finally, lawyers can do "back office" accounting in the same program to balance checking accounts, do trust accounting, and produce firm balance sheets and income statements.

Having decided on which cloud resources to use, how should lawyers transition into the cloud? Here are eight fundamental digital workflow principles for the transitioning lawyer.

First, lawyers need to keep digital documents digital. They should not print them.

Second, lawyers need to make paper documents digital. They should do it within hours of receipt if possible. Otherwise, the paper will pile up and digital files will be incomplete. For this, every lawyer needs a scanner. The only desktop scanner to buy is a Fujitsu Scansnap ix500. Trust me.

Third, as to those people who send paper that needs to be scanned, lawyers should ask them to send digital files in the future. Many will. The others are annoying.

Fourth, lawyers should have a thoughtful document management protocol. All PDF documents should be scanned and stored in black and white (not gray scale or color), and at a resolution of no greater than 300 x 300 dpi. Otherwise, the stored files will be unnecessarily large. Make every document a single PDF file; do not *in globo* scan multiple documents unless a compelling reason exists for doing so. Also, name documents with the date (YYYY-MM-DD), the author's last name, and a detailed description of the document. For example, if a lawyer named Ciolino created a document-management memorandum on Jan. 28, 2017, name it "2017-01-28 Ciolino Electronic Document Management Protocol." This naming methodology allows documents to be sorted chronologically or reverse chronologically in the lawyer's file-management system. And it is a lot easier to identify the file that Ciolino wrote about document management when it has that name rather than the name "89kd82445kd8a99.pdf."

Fifth, lawyers should keep a PDF of just about everything. Lawyers will have PowerPoint files, Word files, Excel files, and other "native" files in their systems. But lawyers should create duplicate PDFs when they are "done" in order to have a permanent file for storage and sharing.

Sixth, lawyers should send their clients copies of everything that they receive or create. Since everything will be in PDF, it is simple and costless to send the copies via email.

Seventh, lawyers should send all digital documents to the cloud for immediate version control, backup, and synchronization with their other devices. And they should assure that it happens automatically in the background using Dropbox or a similar provider.

Finally, lawyers should destroy all paper (unless an original is absolutely necessary), and then keep their PDFs forever. Digital storage is cheap; it costs virtually nothing to store documents indefinitely. Sorry, Iron Mountain.

Security

Last, but first, lawyers should not transition into the cloud without adequate security. That which common sense suggests, lawyer-conduct standards require. Rule 1.6(c) of the ABA Model Rules of Professional Conduct provides that a "lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Thus, a lawyer who stores and communicates confidential information using the cloud must take security seriously.

That being said, lawyers need not implement über-security measures. On the contrary, lawyers must implement

only "reasonable" measures. According to a comment to Model Rule 1.6, some factors to consider in evaluating the reasonableness of a lawyer's security efforts include the following:

- the sensitivity and importance of the information disclosed
- the likelihood of disclosure if more protective measures are not employed
- the cost and difficulty of employing additional safeguards
- the extent to which the safeguards "adversely affect the lawyer's ability to represent clients (such as, by making a device or important piece of software excessively difficult to use)"[3]

So what would a "reasonable" lawyer do? Every security measure that a lawyer implements makes life a little more complicated and a little more difficult; unfortunately, security without complication and difficulty is not security. To be "reasonable" with regard to security, a lawyer must trade off and balance convenience with inconvenience. Here's how lawyers should strike the balance.

First, lawyers should use cryptographically strong passwords. "ABC123" is nice as a song but not as a password. Use at least 12 characters. Use both capital letters and lowercase letters. Use numbers. Use symbols. Use different passwords on different sites. Change passwords regularly.

Second, lawyers should use firewalls, anti-virus software, and malware protection. Windows Defender is baked into Windows 10, but commercial software by providers such as AVG, Avast, and Panda are worthy of consideration. Google "anti-virus software" and see what might work best.

Third, lawyers should regularly update operating system software and applications. It typically happens automatically. Lawyers just need to make sure they have not done something to get in the way.

Fourth, lawyers should use two-factor authentication whenever it is available. Two-factor authentication, or 2FA, requires not only a password to access a site, but also requires the entry of a short-term code obtained from a text message or smartphone app at the time of login. 2FA makes it nearly impossible for an unfriendly to hack into password-protected accounts because doing so requires more than a password.

Fifth, lawyers should not be stupid. That email from the Nigerian prince who wants help reclaiming his lost 10,000,000 in Nigerian Nairas is a hacker. Click the bait and be phished. Instead, be smart. Lawyers need to avoid hooks in their mouths and malware in their machines.

Professor Dane Ciolino says he discounted the importance of 2FA until his Gmail account was hacked. Now he uses 2FA whenever he can, including for Gmail, Quickbooks Online, and Dropbox, among other providers. A list of who offers 2FA is available at **https://twofactorauth.org**.

Sixth, lawyers should physically secure all of their computer devices — with old-fashioned keys and locks and safes. Granted, this is low-tech advice, but if a lawyer's phone, tablet or computer is stolen, the data inside is vulnerable. If, God forbid, it happens, a lawyer should make every effort to remotely wipe the data on the godforsaken device. This functionality is already under the hood of some cloud-based services such as Dropbox Pro.

Seventh, lawyers should consider using more aggressive security measures if a client or the circumstances demand it. A lawyer may want to encrypt files on his or her computer before sending them to Dropbox (using a service such as Viivo or Sookasa). A lawyer may want to store encrypted files at a site that has a "zero knowledge" policy so only the lawyer can unencrypt the data (using a site such as Spideroak). A lawyer may want to consider communicating through a secure client portal (using a service such as Smartvault, Sharefile, or Clio). A lawyer may want to consider using a secure Virtual Private Network (VPN) to access the internet when using public Wi-Fi (using a service such as TunnelBear). A lawyer may want to consider encrypting email. Of course all of these hypervigilant security measures are inconvenient and annoying. Thus, lawyers should think long and hard before annoying themselves and their clients with them.

Finally, in case these security efforts fail, lawyers should make sure that they have at least three copies of their data. They should have one copy on their principal computers; one backup copy on a local hard drive; one copy in the cloud (for example, at Dropbox); and, maybe, one more copy somewhere else.

Thanks to Ernie Svenson at smallfirmbootcamp.com for the years of paperless collaboration and evangelism that led to this article.

Notes

1. *See* Wisconsin State Bar Association, Formal Ethics Opinion No. EF-15-01 (2015); Connecticut Bar Association, Informal Op. No. 2013-07 (2013); Maine Board of Bar Overseers, Op. No. 207 (2013); Ohio State Bar Association, Informal Advisory Op. 2013-03 (2013); Virginia State Bar, Legal Ethics Op. 1872 (2013); Florida State Bar, Op. No. 12-3 (2012); Massachusetts Bar Association, Ethics Op. 12-03 (2012); New Hampshire Ethics Comm. Advisory Opinion, No. 2012-13/4 (2012); Washington State Bar Association, Advisory Op. 2215 (2012); North Carolina State Bar, Formal Ethics Op. 2011-6 (2012); Oregon State Bar Formal Opinion No. 2011-188 (2011); Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility, Formal Opinion No. 2011-200 (2011); Iowa Committee on Practice Ethics and Guidelines, Ethics Opinion No. 11-01 (2011); Alabama State Bar, Formal Op. 2010-02 (2010); California State Bar Association, Ethics Op. 2010-179 (2010); New York State Bar Association's Committee on Professional Ethics Op. 842 (2010); Vermont, Op. 2010-6 (2010); Arizona State Bar, Op. No. 09-04 (2009); New Jersey Supreme Court, Advisory Committee on Professional Ethics, Ethics Op. 701 (2006); Nevada Bar Association, Standing Comm. on Ethics, Formal Op. No. 33 (2006); Arizona State Bar Association, Ethics Op. 09-04 (2004).

2. Other reputable providers include Google Drive, Box, Microsoft OneDrive, and SugarSync.

3. ABA MODEL RULE 1.6, cmt. 18.

About the Author

Dane S. Ciolino is the Alvin R. Christovich Distinguished Professor of Law at Loyola University New Orleans College of Law. He also handles criminal cases, including capital trials, as a member of the CJA Panel of the U.S. District Court for the Eastern District of Louisiana.

Professor Dane S. Ciolino
Loyola University New Orleans
College of Law
New Orleans, Louisiana
504-975-3263
WEBSITE www.daneciolino.com
TWITTER @dciolino
E-MAIL dane@daneciolino.com