

2016

Baring All: Legal Ethics and Confidentiality of Electronically Stored Information in the Cloud

Whitney Morgan

Catholic University of America (Student)

Follow this and additional works at: <https://scholarship.law.edu/jlt>



Part of the [Civil Procedure Commons](#), [Communications Law Commons](#), [First Amendment Commons](#), [Intellectual Property Law Commons](#), [Internet Law Commons](#), [Legal Ethics and Professional Responsibility Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Whitney Morgan, *Baring All: Legal Ethics and Confidentiality of Electronically Stored Information in the Cloud*, 24 Cath. U. J. L. & Tech (2016).

Available at: <https://scholarship.law.edu/jlt/vol24/iss2/8>

This Notes is brought to you for free and open access by CUA Law Scholarship Repository. It has been accepted for inclusion in Catholic University Journal of Law and Technology by an authorized editor of CUA Law Scholarship Repository. For more information, please contact edinger@law.edu.

BARING ALL: LEGAL ETHICS AND CONFIDENTIALITY OF ELECTRONICALLY STORED INFORMATION IN THE CLOUD

Whitney Morgan*

I. INTRODUCTION

The proliferation of innovative information and communication technology (“ICT”) such as computers, the Internet, and e-mail has caused information to be increasingly stored solely electronically.¹ With technological advances such as tablets and smartphones, maintaining a paper copy of all client information, correspondence, and documentation is becoming increasingly difficult and time consuming to create.² The cost of maintaining these copious amounts of paper copies can be astronomical, and the space that is needed is illogical with the technological capabilities to store it digitally.³

In December of 2006, the Federal Rules of Civil Procedure were amended to include the discovery and production process of “electronically stored information.”⁴ The term “Electronically Stored Information” (“ESI”) was coined by these amendments. While not explicitly defined by the amendments nor the

* J.D. Candidate, The Catholic University of America: Columbus School of Law, 2017; B.A. in Music Performance with Elective Studies in Business Administration, Wichita State University, 2012. I would like to thank Professor Chris Savage for his patience and assistance throughout the writing process. I would also like to thank the editors and associates of the Catholic University Journal of Law and Technology for all of their hard work and input, as well as my family and friends for their continued support throughout this entire research and writing process.

¹ MICHAEL ARKFELD, PROLIFERATION OF “ELECTRONICALLY STORED INFORMATION” (ESI) AND REIMBURSABLE PRIVATE CLOUD STORAGE COMPUTING COSTS 3-4, 6 (2011), <http://bit.ly/1XX8DI0> (“ESI includes email, word-processing documents, spreadsheets, voice mail, text messaging, databases, deleted ESI and any other type of digital information.”).

² *Id.* at 4.

³ *See id.* at 12; *see also Understanding Technology Costs*, NETWORK ALL., <http://bit.ly/1r19Cr3> (last visited Feb. 1, 2016).

⁴ *See* FED. R. CIV. P. 26, 34.

accompanying Committee Notes, “[ESI] is understood to mean information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software.”⁵

In the summer of 2014, a large quantity of private digital photos, many containing nudity, of various celebrities were obtained from iCloud by a hacker and posted on the Internet.⁶ The incident became known as “Celebgate.”⁷ The photos spread like wildfire from one online imageboard,⁸ quickly making it onto every popular social network site such as Reddit, Twitter, and 4Chan.⁹ Many of these celebrities claimed to have deleted these photos years ago and were completely oblivious that they were still stored in the cloud.¹⁰

Apart from the “Celebgate,” many other malicious hacks of private and personal information have occurred in the last few years, resulting in breaches of personal information.¹¹ The casual and default use of the cloud must change. At the very least, it must change for lawyers, whom uphold ethical obligations to attorney-client privilege and safeguarding sensitive client information.¹²

More and more law firms are adopting the cloud to store this abundance of electronic information for its “mobility and financial benefits.”¹³ However, along with these technological advantages come a slew of potential risks and privacy concerns. Many lawyers use the cloud as a default for electronic storage, saving all information there for easy access anywhere on the go.¹⁴ The

⁵ Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, NW. J. OF INTELL. PROP. 171, 173 (2006).

⁶ Dayna Evans, *J-Law, Kate Upton Nudes Leak: Web Explodes over Hacked Celeb Pics*, GAWKER (Aug. 31, 2014), <http://bit.ly/1TgrBWf>.

⁷ Alex Johnson, *Almost 600 Accounts Breached in ‘Celebgate’ Nude Photo Hack, FBI Says*, NBC NEWS (June 10, 2015, 3:45 AM), <http://nbcnews.to/1SN9QQX>.

⁸ *Definition of Imageboard*, REFERENCE.ORG, <http://bit.ly/246hle9> (last visited Feb. 8, 2016) (defining an imageboard as an “internet forum” where users post images).

⁹ Evans, *supra* note 6.

¹⁰ See James Cook, *Celebrities Victimized in the iCloud Naked Photo Hack Want to Sue Google for \$100 Million*, BUS. INSIDER, (Oct. 2, 2014), <http://read.bi/1rl9OGM>; see also Adam Clark Estes, *What is the “Cloud” – And Where Is It?*, GIZMODO (Jan. 29, 2015), <http://bit.ly/1pKCnfs> (“‘Cloud’ is a buzzword that vaguely suggests the promise and convenience of being able to access files from anywhere... [I]t’s a physical infrastructure, its many computers housed in massive warehouses all over the world.”).

¹¹ See Meghan C. Lewallen, *Cloud Computing: A Lawyer’s Ethical Duty to Act with Reasonable Care when Storing Client Confidences “In the Cloud”*, 60 CLEV. ST. L. REV. 1133, 1144-45 (2013) (discussing the Dropbox glitch of 2011 that resulted in users gaining access to any Dropbox account with an arbitrary password, as well as the Google Docs glitch of 2009 which allowed access to an individual’s documents to anyone they had collaborated with previously via the cloud).

¹² See, e.g., MODEL RULES OF PROF’L CONDUCT r. 1.6, 1.15 (AM. BAR ASS’N 2013).

¹³ Lewallen, *supra* note 11, at 1137.

¹⁴ Sam Glover, *It’s Time for Lawyers to Re-Think the Cloud*, THE LAWYERIST (Oct. 17,

dangers that accompany this default use and easy access are unparalleled for professionals that have an ethical obligation to protect sensitive information. Lawyers have been battling ethical implications that accompany ESI for years, and some jurisdictions still have not issued an ethics opinion as a guideline to regulate the storage of ESI in the cloud.¹⁵

This Note will explore the use of cloud computing by law firms and the electronic storage of sensitive client information. It will compare the ramifications of notable security breaches with those that may occur within a law firm, and the measures that may be taken to prevent such breaches. To assist in outlining a balancing test for using the cloud, Part III will explore the advantages to cloud computing as well as the risks that a law firm shoulders in trusting a third party with sensitive client information. Part III will also discuss the risks associated with electronic discovery procedures that accompany a client's use of the cloud. Part IV will outline current state and federal statutes that govern ESI and e-discovery within a law firm. Also, Part IV will analyze the various ethical duties by which a law firm must abide in providing competent representation.

Part V will highlight the infamous "Celebgate" incident of 2014 as well as other notable cloud breaches. Some of these notable breaches even led to civil litigation.¹⁶ These breaches were unfortunate incidents but provide lessons not to be taken lightly by lawyers or any professional that has an ethical duty to guard sensitive client information, for that matter. Part VI will discuss and compare the existing ethics opinions from the handful of jurisdictions that have published in this area. Though only persuasive authority, ethics opinions provide general guidance for use of the cloud for storing sensitive information by law firms.¹⁷ Too many jurisdictions have not published formal ethics opinions to govern law firm use of the cloud.¹⁸ Finally, Part VII will argue for a more concrete standard to which ESI should be held or, at the very least, a demand for publication of formal ethics opinions in the remaining jurisdictions that still lack this guidance.

2014), <http://bit.ly/1SNa36E> (discussing his personal experience as a lawyer using the cloud).

¹⁵ Lewallen, *supra* note 11, at 1135-36.

¹⁶ Cook, *supra* note 10 (explaining the possibility of a \$100 million lawsuit against the alleged iCloud hacker by a Hollywood attorney that represented several of the celebrity women victimized by the famous breach).

¹⁷ See *Cloud Computing/Software as a Service for Lawyers*, AM. BAR ASS'N, <http://bit.ly/1XX8N2b> (last visited Feb. 1, 2016) (explaining "Software as a Service," a new cloud computing service model developed to store sensitive materials for law firms).

¹⁸ See *Cloud Ethics Opinions Around the U.S.*, AM. BAR ASS'N, <http://bit.ly/1WUTc4S> (last visited Feb. 1, 2016).

II. WHAT IS THE CLOUD AND CLOUD COMPUTING?

By the 1990s, the Internet was widely used, connecting users all over the planet via e-mail and messaging.¹⁹ Individuals and businesses began creating websites, posting photos, and sending or receiving data.²⁰ With an increase in bandwidth²¹ and a significant reduction in data storage costs, computing and network technology have advanced to the point where cloud computing is a possibility that did not exist nearly 20 years ago.²²

Cloud computing moves electronic data and data management off-site to a third party data center.²³ These data centers, or “cloud providers”, are essentially warehouses with multiple servers all over the world on which millions of users store their electronic information.²⁴ These cloud providers allow users to access the information they have stored in the cloud from any device that connects to the Internet at any time.²⁵ However, along with these numerous benefits of cloud computing, come major risks associated with discovery procedures during litigation, privacy, and confidentiality agreements.

III. THE BAD WITH THE GOOD: WHY USE THE CLOUD?

A. The Benefits of Cloud Computing

Enterprise data, including client ESI, is estimated to be doubling every three years.²⁶ The physical space required for maintaining paper copies of client data can be considerable.²⁷ Furthermore, law firms are generally required to retain client files for a specified amount of time, usually several years, amounting in an even larger physical space requirement to store files.²⁸ A major benefit of cloud computing that combats this physical space limitation is the scalability of

¹⁹ Dena G. McCorry, *With Cloud Technology, Who Owns Your Data?*, 8 FED. CTS. L. REV. 125, 127-28 (2014).

²⁰ *Id.* at 126, 128.

²¹ *See Bandwidth*, MERRIAM-WEBSTER, <http://bit.ly/1ST4sPj> (last visited Feb. 1, 2016) (defining bandwidth as “[a] measurement of the ability of an electronic communications device or system (such as a computer network) to send and receive information”).

²² McCorry, *supra* note 19, at 128.

²³ *Id.* at 129.

²⁴ *Id.*

²⁵ *Id.*

²⁶ Rod Smith, Int’l Bus. Machines, Internet Emerging Technology, Presentation at the Internet Summit 10, at 2 (Nov. 18, 2010), <http://ibm.co/24mLu5y>.

²⁷ ARKFELD, *supra* note 1, at 12 (noting the high power consumption, cooling requirements, installation and cooling with paper versus cloud storage).

²⁸ *Id.* at 5.

storage space with a third party technology provider.²⁹ Cloud services can be quickly scaled up or down, sometimes even automatically, to cater to evolving demands of law firms and their clients.³⁰ These capabilities can be elastically provisioned and purchased in various bundles quickly at any time.³¹

One of the most commonly known benefits to cloud computing within a law firm is the level of economic savings compared to desktop counterparts.³² Before the cloud, firms were forced to pay for servers, software installation, and updates, as well as annual licensing fees or software upgrade fees.³³ The biggest expense for law firms before cloud computing was the training and salary costs of an IT staff³⁴ to maintain servers and updates.³⁵ With a third party technology provider, the only cost is one monthly fee; the cloud computing provider hosts and updates the software at no additional cost.³⁶

The greatest benefit of cloud computing is the simplicity of it, especially for lawyers starting new firms without pre-existing knowledge of systems currently in place.³⁷ Data security, backup, disaster recovery, and IT expertise are generally the responsibilities of the cloud provider instead of the law firm.³⁸

Along with simplicity comes the accessibility of using the cloud. Data stored in the cloud can be accessed anywhere that an Internet connection is available.³⁹ Because data is stored in a remote location instead of on one desk-

²⁹ *Id.* at 9-10.

³⁰ Roland L. Trope & Sarah Jane Hughes, *Contemporary Issues in Cyberlaw: Red Skies in the Morning – Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111, 167 (2011) (citing PETER MELL & TIMOTHY GRANCE, NAT'L INST. STANDARDS & TECH, PUB. NO.800-145, THE NIST DEFINITIONS OF CLOUD COMPUTING 2 (2011), <http://1.usa.gov/21hv38K>).

³¹ *See id.* (explaining the flexibility and scalability of the amount of electronic storage offered tied to the required amount by the company. These different options can be tailored in various packages available for purchase or upgraded if the storage space required increases).

³² NICOLE BLACK, CLOUD COMPUTING FOR LAWYERS 20 (2012).

³³ *Id.*

³⁴ *What Does an Information Technology Specialist Do?* WISEGEEK, <http://bit.ly/1WUTo49> (last visited Feb. 1, 2016) (explaining that an IT Specialist works with computers and Internet systems in many different capacities and settings and is responsible for hardware servicing, network maintenance, troubleshooting, among other things); *see also* BLACK, *supra* note 32, at 21 (stating that there is often no need to hire IT staff with the emergence of cloud computing).

³⁵ BLACK, *supra* note 32, at 20; *see also Understanding Technology Costs*, *supra* note 3 (explaining costs of computers and their ongoing expenses that include security, updates, technical support and repair, and noting that firms, on average, spend \$700 per user per month on IT expenses).

³⁶ BLACK, *supra* note 32, at 20.

³⁷ *Id.* at 21.

³⁸ *Id.* at 37.

³⁹ Elijah Yip & Martin E. Hsia, *Confidentiality in the Cloud: The Ethics of Using Cloud*

top computer in a firm, that data can be synchronized to several different devices.⁴⁰ With this technology, changes can be made to a document on one device and then retrieved and edited on a completely different device in a different location.⁴¹ This is an incredibly efficient tool for lawyers in the pre-trial phases of litigation, when documents are being sent back and forth between attorney and client, for approval and edits.

Though the privacy and security risks may commonly be considered the major downfalls of cloud computing, this is actually a myth. Cloud computing provides increased security and stability.⁴² Highly capable cloud providers use the most up-to-date, sophisticated security measures.⁴³ They have adequately trained staff with the expertise to implement security measures while taking into account current technological trends.⁴⁴

E-mail security in its current practice is severely flawed and is used by most lawyers hundreds of times a day, with the average corporate user receiving 112 e-mails per day.⁴⁵ “Most e-mails are essentially no more than virtual postcards, the contents readily viewable by anyone who cares to look.”⁴⁶ However, most cloud computing platforms remedy the lack of e-mail security by including an encrypted form of client communication into their software.⁴⁷ Due to the growing trend of e-mail as a lawyer’s main medium for communication, this encrypted form of client communication alone should justify the switch to cloud computing from traditional software packages.⁴⁸

B. With Cloud Computing Comes Risk

Risks associated with cloud computing come from two different sources. There are risks that accompany a law firm storing sensitive client information in the cloud.⁴⁹ In addition, there are risks when clients possess, or store in the cloud, sensitive documents that are subject to discovery and the procedures

Services in the Practice of Law, 18 HAW. B.J., Aug. 2014, at 4, 5.

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Use of Cloud Computing in a Law Office*, IT LAW GRP., <http://bit.ly/1ST4Q0l> (last visited Sept. 25, 2015).

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ ARKFELD, *supra* note 1, at 5.

⁴⁶ BLACK, *supra* note 32, at 24.

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ Yip & Hsia, *supra* note 39, at 5-6.

that govern e-discovery.⁵⁰

No solution is risk-free when entrusting sensitive client information to a third party. Among the most paramount of concerns associated with storing client information offsite is security.⁵¹ Most sets of ethical rules today contain a duty of confidentiality, and this duty can be difficult to uphold when transferring control of personal information to a party not involved in the matter.⁵² However, by shifting the control to this third party, the duty of preventing data leaks majorly shifts to that party as well.⁵³

The attorney-client privilege is generally waived if the client voluntarily discloses private communications to anyone other than their attorney.⁵⁴ The *possibility* that a third party could potentially see the private communication does not necessarily waive the attorney-client privilege.⁵⁵ It is the general opinion of the legal field that the use of cloud computing by attorneys is permitted as long as they exercise reasonable care.⁵⁶ However, the lack of a formal ethics opinion in so many states leaves the majority of law firms with little guidance for storing client information in the cloud.

Without control of cloud computing servers, data loss may occur by no fault or knowledge of the law firm.⁵⁷ Data loss is an important risk of cloud computing, whether it is temporary or permanent data loss.⁵⁸ Temporary data loss can occur for a number of reasons including Internet outages, power outages, or if the provider's cloud computing servers go down.⁵⁹

For example, in May of 2011, Amazon.com discounted pop artist Lady Gaga's album "Born this Way" from nearly 12 dollars to 99 cents for a one-day only sale.⁶⁰ This one-day sale was initiated to promote Amazon's new "cloud drive" service that allowed users to purchase music from the Amazon website,

⁵⁰ Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) (explaining that to prevent such risks, there must be proper communication between a party and his/her lawyer).

⁵¹ Gavin Manes & Tom O'Connor, *Attorneys Beware: The Danger of Storing Information In the Cloud*, INSIDE COUNSEL (Apr. 6, 2012), <http://bit.ly/1VV1gUg>.

⁵² See, e.g., MODEL RULES OF PROF'L CONDUCT r. 1.6 (governing confidentiality of information between a lawyer and a client).

⁵³ SOLICITORS REGULATION AUTH., SILVER LININGS: CLOUD COMPUTING, LAW FIRMS, AND RISK 10 (2013), <http://bit.ly/1NDkZo6>.

⁵⁴ Yip & Hsia, *supra* note 39, at 6.

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ BLACK, *supra* note 32, at 30.

⁵⁸ Charles Babcock, *9 Worst Cloud Security Threats*, INFO. WEEK (Mar. 3, 2014, 10:25 AM), <http://ubm.io/1P8OWq3>.

⁵⁹ BLACK, *supra* note 32, at 30.

⁶⁰ Ben Sisario, *Lady Gaga Sale Stalls Amazon Servers*, N.Y. TIMES (May 23, 2011), <http://nyti.ms/24mLZwG>.

store it at a remote location, and stream it onto any music playing device.⁶¹ However, the 99 cents purchase proved to be so popular that Amazon's cloud computing servers were overwhelmed by Lady Gaga fans.⁶² The servers went down, preventing many users from completing their download or listening to the full album.⁶³ Therefore, taking potential downtime into consideration is important when considering whether to switch to cloud storage.⁶⁴

Permanent data loss may also occur in a number of ways, wiping computing servers indefinitely of all ESI. The cloud provider's servers could malfunction and "crash"⁶⁵ much like an incident in April 2011, when Amazon's huge cloud servers' crash permanently destroyed data connected with users' websites.⁶⁶ Permanent data loss could result if servers are destroyed by a natural disaster of some kind.⁶⁷ Third parties could also withhold data by refusing a company access to the cloud due to a billing dispute or other type of contractual disagreement.⁶⁸ Lastly, there is always the fear of losing data due to a provider going out of business.⁶⁹ Financial stability is never guaranteed, so it is always important to have procedures in place for such an occasion.⁷⁰ Although data loss is an important risk to bear in mind when choosing storage options for ESI, the lack of local equipment can actually result in a lesser likelihood of data loss.⁷¹

In the context of meeting discovery obligations during litigation, lawyers face major risks associated with clients having and storing sensitive documents related to discovery in the cloud.⁷² Spoliation is "the destruction or significant alteration of evidence" and includes the failure to preserve any potential evidence for future reasonably foreseeable litigation.⁷³ The authority to sanction

⁶¹ *Id.*

⁶² *Id.*

⁶³ *Id.*

⁶⁴ BLACK, *supra* note 32, at 30.

⁶⁵ See Margaret Rouse, *Definition: Crash*, WHATIS.COM, <http://bit.ly/24mM0R3> (last updated Mar. 1, 2006) (defining a crash as "the sudden failure of a software application or operating system").

⁶⁶ Henry Blodget, *Amazon's Cloud Crash Disaster Permanently Destroyed Many Customers' Data*, BUS. INSIDER (Apr. 28, 2011, 7:10 AM), <http://read.bi/1YVLNAQ>. An unexplained crash of Amazon.com's cloud server took down websites of dozens of high-profile companies for several hours, and completely deleted data from other users' websites permanently. *Id.*

⁶⁷ BLACK, *supra* note 32, at 31.

⁶⁸ *Id.*

⁶⁹ *Id.*

⁷⁰ *Id.*

⁷¹ Yip & Hsia, *supra* note 39, at 5.

⁷² *Zubulake*, 229 F.R.D. at 432.

⁷³ *Id.* at 430 (citing *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir.

litigants for spoliation arises under Fed. R. Civ. P. 37 and is confined to the sole discretion of the trial judge.⁷⁴ The decision to award sanctions is assessed on a case-by-case basis.⁷⁵

The court in *Zubulake v. UBS Warburg LLC* imposed upon counsel a duty to monitor a party's compliance with e-discovery procedures such as preservation and proper production of discovery documents.⁷⁶ If a client fails to retain and produce discovery documents, the client's lawyer faces the risk of sanctions. The main cause of this failure on the client's part is the lack of control over the cloud's operating system or data storage.⁷⁷ Clients only have access to their own data.⁷⁸ Unfortunately, courts will usually find that the responding party, the client, does have control of all information stored in the cloud, despite not having physical control over this information.⁷⁹ This results in compliance issues with discovery requests and the additional possibility of sanctions issued against the party's attorney.⁸⁰ Therefore, proper attorney-client communication is essential.⁸¹

There are always risks associated with data storage, and cloud computing presents a unique set of risks and legal issues. Risks such as security breach, duty of confidentiality breach, and data loss are significant risks that should not be taken lightly in deciding on a storage option for sensitive information. However, there are risks associated with on-site data storage and in-house IT departments as well,⁸² so it is important to compare these risks before settling on an electronic storage option. Being smart about cloud computing and taking reasonable steps to ensure that client data remains safeguarded and confidential can prevent most risks associated with data storage.

1999).

⁷⁴ FED. R. CIV. P. 37(b)(2).

⁷⁵ *Fujitsu Ltd. v. Fed. Express Corp.*, 247 F.3d 423, 436 (2d Cir. 2001).

⁷⁶ *Zubulake*, 229 F.R.D. at 432.

⁷⁷ Cindy Pham, *E-Discovery in the Cloud Era: What's a Litigant To Do?*, 5 HASTINGS SCI. & TECH. L.J. 139, 158 (2013).

⁷⁸ *Id.*

⁷⁹ *Id.* at 158 n.107.

⁸⁰ *Id.*

⁸¹ *See Zubulake*, 229 F.R.D. at 432.

⁸² *See generally Use of Cloud Computing in a Law Office*, *supra* note 42 (discussing risks in IT storage).

IV. STATUTES AFFECTING ELECTRONICALLY STORED
INFORMATION

A. December 2006 Amendments to the Federal Rules of Civil Procedure

After five years of study on Civil Rules by the Advisory Committee and the recognition of fundamental differences between paper-based document discovery and the discovery of electronic information, a package of amendments was issued to the Federal Rules of Civil Procedure in December of 2006.⁸³ The Committee Notes accompanying the 2006 amendments covered electronic discovery used in any current or potentially future mediums:

Rule 34(a)(1) is expansive and includes any type of information that is stored electronically. A common example often sought in discovery is electronic communications, such as e-mail. The rule covers—either as documents or as electronically stored information—information “stored in any medium,” to encompass future developments in computer technology. Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.⁸⁴

These amendments attempted to resolve the many conflicts arising out of electronic discovery prior to taking effect nationwide.⁸⁵ These conflicts were the result of the lack of control a client has over a cloud’s operating system or data storage.⁸⁶ Generally clients only have access to their own data in the cloud.⁸⁷ However, because of Fed. R. Civ. P. 34, courts will likely hold law firms responsible for maintaining control over this data, regardless of the cloud provider’s physical control of the information.⁸⁸ Because of this lack of control, parties often times have trouble complying with discovery requests, risking sanctions for not producing ESI under Rule 37.⁸⁹

These amendments also labeled and defined ESI for the first time.⁹⁰ However, neither cloud computing nor storage regulations for this electronic infor-

⁸³ Withers, *supra* note 5, at 171.

⁸⁴ FED. R. CIV. P. 34(a) advisory committee’s notes to 2006 amendment.

⁸⁵ See generally *Treppel v. Biovail Corp.*, 233 F.R.D. 363 (S.D.N.Y. 2006) (addressing electronic discovery issues pertaining to preservation, interrogatory questionnaire limits, and issues pertaining to scope).

⁸⁶ Pham, *supra* note 77, at 158.

⁸⁷ *Id.*

⁸⁸ *Id.* at 140-41 (citing FED. R. CIV. P. 34).

⁸⁹ *Id.* at 158 (citing FED. R. CIV. P. 37(e)).

⁹⁰ FED. R. CIV. P. 34(a) advisory committee’s notes to 2006 amendment.

mation were specifically addressed, leaving law firms with few to no guidelines regulating the use of the cloud.

B. Privacy Laws and Regulations Unique to Law Firms

Numerous state and federal laws and regulations could be applied to cloud computing.⁹¹ Turning to non-discovery cloud regulations, the biggest legal concerns are privacy laws and regulations that are unique to law firms.⁹² Privacy should be a top priority in maintaining a successful law firm.⁹³ Depending on the type of law practice, different laws may govern how client information should be transitioned to the cloud, however there are some privacy issues that lawyers may encounter more generally.⁹⁴

Law firms that store sensitive information regarding a client's medical history are subject to the Health Insurance Portability and Accountability Act ("HIPAA").⁹⁵ These law firms must follow specific regulatory requirements before the information may be given to a third party, such as a cloud computing provider.⁹⁶ Hospitals and other medical facilities are generally regulated by HIPAA, however law firms that store client information containing any medical information or history must also follow HIPAA.⁹⁷ The same procedures apply to sensitive financial information under the Gramm-Leach Bliley Act.⁹⁸ Each agreement must be narrowly tailored according to the type of information that is being stored: "Under both acts, the agreement between the law firm and the cloud-computing provider must include the specific language set forth in the applicable statute regarding the disclosure of covered data to third parties."⁹⁹

Another, more broadly sweeping concern for the regulation of cloud computing is the USA PATRIOT Act.¹⁰⁰ Under this anti-terrorist law, information

⁹¹ James Ryan, *The Uncertain Future: Privacy and Security in Cloud Computing*, 54 SANTA CLARA L. REV. 497, 506 (2014) (citing Jason Bloomberg, *Cloud Computing: Legal Quagmire*, ZAPTHINK (Jul. 5, 2011), <http://bit.ly/1VE3rLr>).

⁹² See generally *id.* at 506-10 (discussing applicable laws and regulations of cloud computing in the United States).

⁹³ See EDNA SELAN EPSTEIN, *THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK-PRODUCT DOCTRINE 2* (4th ed. 2001).

⁹⁴ BLACK, *supra* note 32, at 81.

⁹⁵ See generally Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

⁹⁶ BLACK, *supra* note 32, at 81.

⁹⁷ *Id.* at 80-81.

⁹⁸ See Gramm-Leach Bliley Act of 1999 §§ 501-502, 15 U.S.C. §§ 6801-6802 (2012).

⁹⁹ BLACK, *supra* note 32, at 81.

¹⁰⁰ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115

stored in the cloud can be turned over to the government, sometimes without notice to the customer.¹⁰¹ This presents a plethora of security concerns for the cloud computing industry.

Numerous states have passed state laws or regulations implementing security measures that must be taken by businesses storing sensitive information electronically.¹⁰² In Massachusetts and Nevada, for example, information such as social security numbers that are transmitted electronically must be done so via encrypted communications only.¹⁰³

Other regulations, in terms of visibility, include the Stored Communications Act, export regulations overseen by the Departments of Commerce and State, and consumer protection under the Federal Trade Commission.¹⁰⁴ Further state and federal laws govern ESI and cloud computing for financial institutions, hospitals, and other non-law firm businesses.¹⁰⁵ However, additional regulations are required for application, specifically to attorney-client communications, especially with present concerns surrounding recent large-scale data disclosures.¹⁰⁶

C. Ethical Implications of Cloud Computing

Ethical issues regarding cloud computing within a law firm can be divided into two sub-categories: (1) issues involving the law firm's cloud computing third party vendor choice and (2) risks in the daily use of technology after cloud computing has been incorporated into the law firm.¹⁰⁷

The American Bar Association's ("ABA") Model Rules of Professional Conduct ("MRPC")¹⁰⁸ Rule 1.6(a), the duty of confidentiality, and Rule 1.15,

Stat. 272 (2001); Ryan, *supra* note 91, at 507.

¹⁰¹ David Saleh Rauf, *PATRIOT Act Clouds Picture for Tech*, POLITICO (Nov. 29, 2011, 11:27 AM), <http://politi.co/246kyKR>.

¹⁰² BLACK, *supra* note 32, at 81.

¹⁰³ *Id.*; David Canellos, *Adopting the Cloud While Adhering to Domestic & Foreign Government Regulations*, SAFEDEV (Oct. 2, 2013), <http://bit.ly/1pKDMTj> (referring to when information is encrypted in the cloud it is unreadable until paired with the encryption key that is held by the receiving party).

¹⁰⁴ Ryan, *supra* note 91, at 506.

¹⁰⁵ *See, e.g.*, 18 U.S.C. § 1514A (2012) (defining and outlining The Sarbanes-Oxley Act that governs corporate financial reporting).

¹⁰⁶ BLACK, *supra* note 32, at 82.

¹⁰⁷ *Id.* at 35.

¹⁰⁸ The American Bar Association's Model Rules of Professional Conduct have no primary authority unless directly adopted into an individual state's model rules. Most states that have not adopted the ABA's MRPC, have incorporated their own rules of professional conduct that include or bare great resemblance to Rule 1.6(a) and Rule 1.15.

the safekeeping of client property, reach all aspects of ethical concerns for cloud computing in law practice.¹⁰⁹ These Model Rules help to form the foundation for attorney-client privilege and the protection of any information that a client deems sensitive from potential detrimental disclosure and embarrassment.¹¹⁰ Rule 1.6 provides: “A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation . . .”¹¹¹ Comment 17 to this rule adds that lawyers must take “reasonable precautions” to safeguard sensitive information and keep it from accidental disclosure to unintended parties during transmission.¹¹²

Attorneys have an ethical duty to take reasonably necessary steps to keep these client confidences secure.¹¹³ A law firm must keep this duty in mind when choosing a third party cloud computing provider with which to trust this sensitive trusted client information on a daily basis.¹¹⁴ Therefore, law firms should choose a highly capable and trustworthy outside cloud computing business to safeguard client files and keep information safe and secure.

Until 2012, these duties were merely implicit in the MRPC with regard to technology, at which point, they were updated to include technical competency requirements.¹¹⁵ The ABA Commission acknowledged “in light of the pervasive use of technology to store and transmit confidential client information, this obligation should be stated explicitly in the black letter of MRPC Rule 1.6.”¹¹⁶ With the majority of attorney-client interaction and document exchange being conducted electronically, black letter law governing confidentiality regulations for technology became a necessity in the MRPC. In August 2012, the ABA included a change to the MRPC requiring lawyers to keep pace with “relevant technology” to satisfy their obligation to provide competent representation to clients.¹¹⁷

MRPC Rules 1.1 (competency)¹¹⁸ and 1.3 (diligence)¹¹⁹ are high-ranking

¹⁰⁹ MODEL RULES OF PROF’L CONDUCT r. 1.6, 1.15.

¹¹⁰ *Id.*

¹¹¹ *Id.*

¹¹² BLACK, *supra* note 32, at 37 (citing MODEL RULES OF PROF’L CONDUCT r. 1.6(a)).

¹¹³ Lewallen, *supra* note 11, at 1143.

¹¹⁴ BLACK, *supra* note 32, at 35.

¹¹⁵ Antigone Peyton, *Kill the Dinosaurs, and Other Tips for Achieving Technical Competence in Your Law Practice*, 21 RICH. J.L. & TECH. 1, 5 (2014).

¹¹⁶ Am. Bar Ass’n Comm’n on Ethics 20/20, Initial Draft Proposals—Technology and Confidentiality 13 (2011) [hereinafter ABA Ethics 20/20 Draft Proposal], <http://bit.ly/1WUUDA5>.

¹¹⁷ Peyton, *supra* note 115, at 5-6.

¹¹⁸ MODEL RULES OF PROF’L CONDUCT r. 1.1.

¹¹⁹ *Id.* r. 1.3.

rules for consideration when selecting a technology provider for daily use cloud computing services.¹²⁰ A law firm has an ethical duty to “provide competent representation to a client.”¹²¹ This includes choosing a third party in which to entrust confidential information.¹²² This duty inherently implies a separate duty to stay abreast of current communication technologies and methodologies for electronic information storage.¹²³

A duty to stay abreast of current technologies may be controversial, but in order to recognize the risks that accompany new technology and have the ability to explain and disclose those risks to clients, it is imperative that a lawyer be able to keep up with evolving technology.¹²⁴ Additionally, when using the cloud on a day-to-day basis, a law firm cannot rely on the technology provider to maintain the cloud-based tools and to keep them up to date with current industry standards at all times.¹²⁵

Though not a necessarily binding authority, the ABA Commission on Ethics 20/20 supported this position in its Initial Draft Proposal on Technology and Confidentiality.¹²⁶ The ABA Commission’s Draft concluded that a lawyer should be up to date on the benefits and risks of evolving technology.¹²⁷ Accordingly, the Draft recommended that Comment 6 of Model Rule 1.1 be updated to the following: “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.”¹²⁸ Thus, a law firm carries the duty to keep up with evolving technology, whether it is an ethical duty stemming from the competency requirement or an implicit duty in providing clients with the best, most up to date cloud storage option.

Lastly, there is a court-imposed duty to monitor client’s e-discovery efforts to ensure the proper disclosure of ESI.¹²⁹ In *Zubulake v. UBS Warburg LLC*, the Honorable Shira Sheindlin stated: “[I]t is not sufficient to notify all employees of a litigation hold and expect that the party will then retain and pro-

¹²⁰ BLACK, *supra* note 32, at 53.

¹²¹ MODEL RULES OF PROF’L CONDUCT r. 1.1.

¹²² BLACK, *supra* note 32, at 35.

¹²³ Trope & Hughes, *supra* note 30, at 137-38.

¹²⁴ *Id.* at 138.

¹²⁵ BLACK, *supra* note 32, at 54.

¹²⁶ See ABA Ethics 20/20 Draft Proposal, *supra* note 116, at 5.

¹²⁷ *Id.*

¹²⁸ *Id.*

¹²⁹ See *Zubulake*, 229 F.R.D. at 430-31.

duce all relevant information. Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched.”¹³⁰ With the proliferation of ESI, litigation is becoming riskier and more costly.¹³¹ In many cases, courts will not and have not hesitated to impose sanctions on parties for failure to preserve or disclose electronic discovery information in their possession.¹³²

V. ALL OF THE TIMES THE CLOUD LET US DOWN

A. “Celebgate:” What Lawyers Can Learn from Jennifer Lawrence

In August 2014, a multitude of female celebrities’ iCloud accounts were hacked.¹³³ Personal photographs, many containing nudity, were published onto the Internet and spread like wildfire within minutes.¹³⁴ Some of the most famous photos among these belonged to America’s sweetheart at the time, Jennifer Lawrence.¹³⁵ This breach happened because these photos were stored as unsecured files in the cloud.¹³⁶ Several of these celebrities were unaware that these photos still existed in the cloud, having deleted them from their phones years ago.¹³⁷

This is a common oversight by many people, including lawyers who think that once an e-mail or document is deleted on their laptop or smartphone that it is gone forever.¹³⁸ What have we learned from Jennifer Lawrence? Just because a file is deleted, does not mean that it is gone.¹³⁹ The December 2006 amendments to the Federal Rules of Civil Procedure even included the phrase “deleted data” in the definition of ESI that was outlined for the first time.¹⁴⁰ Prior to these amendments, courts held that the definition of “documents” un-

¹³⁰ *Id.* at 432.

¹³¹ Pham, *supra* note 77, at 158.

¹³² ARKFELD, *supra* note 1, at 6.

¹³³ Kashmir Hill, *Please Stop Saying ‘Celebs Shouldn’t Have Taken Nude Photos in the First Place’*, FORBES (Sept. 1, 2014, 5:51 PM), <http://onforb.es/1NDICyd>.

¹³⁴ *Id.*

¹³⁵ *Id.*

¹³⁶ Jeff Bennion, *Why Jennifer Lawrence’s Leaked Nude Photos Should Be Important to Lawyers*, ABOVE THE LAW (Sept. 2, 2014, 12:13 PM), <http://bit.ly/21hvVKG>; *see also* Justin Worland, *How That Massive Celebrity Hack Might Have Happened*, TIME (Sept. 1, 2014), <http://ti.me/24mMK8U>.

¹³⁷ *See* Evans, *supra* note 6 (citing Mary E. Winstead (@M_E_Winstead), TWITTER (Aug. 31, 2014, 5:53 PM), <http://bit.ly/1XX9bxH>).

¹³⁸ Bennion, *supra* note 136.

¹³⁹ *Id.*

¹⁴⁰ ARKFELD, *supra* note 1, at 6.

der Rule 34 included “computer data” as well as “deleted data.”¹⁴¹

A law firm’s documents are just as enticing to obtain for a hacker as nude photographs of celebrities because sensitive client files can be obtained for a price.¹⁴² In some high profile cases parties would pay top dollar to get sensitive information that would win them the case.¹⁴³ Most lawyers do not know the first thing about cybersecurity, yet they unknowingly store confidential information in the cloud as a default option on a daily basis.¹⁴⁴ Many lawyers use services available through the Internet to store the most sensitive of client information despite ramifications of these default actions being plastered all over the news every day.¹⁴⁵ It is time for lawyers and law firms to change the way they store electronic information.

B. Revisiting *Zubulake v. UBS Warburg LLC*

In *Zubulake v. UBS Warburg LLC*, the plaintiff employee, in an employment discrimination suit, sued the defendant for failure to produce relevant documents and tardiness to produce similar materials.¹⁴⁶ The court-ordered sanctions related to defendant’s willful destruction of plaintiff’s relevant e-mails.¹⁴⁷ A mere understanding of e-mail was not enough for trial counsel to uphold their duty to monitor client’s obligation to preserve electronic records for discovery purposes.¹⁴⁸

Because of *Zubulake*, the court imposed this duty to monitor all clients’ electronic discovery needs to ensure disclosure upon counsel.¹⁴⁹ The *Zubulake* series of opinions set the groundwork for the notion that technical competence is necessary in providing effective legal representation and fulfilling ethical obligations to clients.¹⁵⁰ The fact that mere understanding of the way e-mail works was not enough to satisfy this court-imposed duty to monitor implies that there is indeed a duty to keep up with evolving technology.¹⁵¹

¹⁴¹ Bennion, *supra* note 136.

¹⁴² *Id.*

¹⁴³ *Id.*

¹⁴⁴ *Id.*

¹⁴⁵ *See generally id.*

¹⁴⁶ *Zubulake*, 229 F.R.D. at 424.

¹⁴⁷ *Id.*

¹⁴⁸ *Id.* at 432.

¹⁴⁹ *Id.*

¹⁵⁰ Peyton, *supra* note 115, at 3-4.

¹⁵¹ *See Zubulake*, 229 F.R.D. at 424, 432.

C. Other Cloud Security Issues

Beginning on Black Friday of 2013, Target suffered a data breach that resulted in the theft of personal credit card information of up to 110 million customers nationwide.¹⁵² The breach involved the theft of data stored on the magnetic strips of credit cards and extended to nearly every Target store in the country.¹⁵³ This was a shocking theft that occurred during the normal processing and storage of data.¹⁵⁴

There have been several reports of security breaches from businesses that have had potential to cause great harm.¹⁵⁵ In 2011, Dropbox reported a glitch that allowed users to access any Dropbox account by using an arbitrary password.¹⁵⁶ This glitch allowed potential hackers to log onto a Dropbox account and retrieve private information from another user.¹⁵⁷

In 2009, Google Docs experienced a glitch that resulted in private documents being inadvertently exposed.¹⁵⁸ The glitch shared an individual's private documents with anyone the user had shared with previously via the Cloud.¹⁵⁹ Google Docs has been identified as one of the most widely used cloud service provider by large and small law firms.¹⁶⁰ Therefore, it would make sense that a number of attorneys felt the disastrous effects of the Google Docs glitch.¹⁶¹

VI. COMPARING ETHICAL CONSIDERATIONS OF VARYING JURISDICTIONS

In response to the rise of cloud computing, the ABA is issuing formal ethics opinions to help address ethical concerns with using the cloud.¹⁶² Though only persuasive authority, formal ethics opinions give jurisdictions a basic guideline to follow when storing electronic information.¹⁶³ Unfortunately, many jurisdic-

¹⁵² Maggie McGrath, *Target Data Breach Spilled Info On As Many As 70 Million Customers*, FORBES (Jan. 10, 2014, 8:56 AM), <http://onforb.es/1qYtrUP>.

¹⁵³ *Id.*

¹⁵⁴ Babcock, *supra* note 58.

¹⁵⁵ Lewallen, *supra* note 11, at 1144.

¹⁵⁶ *Id.* at 1145; *see also* Eliu Mendez, *Dropping Dropbox in Your Law Practice to Maintain Your Duty of Confidentiality*, 36 CAMPBELL L. REV. 175, 176 (2014) ("Dropbox is a free file-hosting service that offers cloud storage and file synchronization.").

¹⁵⁷ Lewallen, *supra* note 11, at 1145.

¹⁵⁸ *Id.* at 1144.

¹⁵⁹ *Id.* at 1144-45.

¹⁶⁰ Robert Ambrogi, *Lawyers' Use of Cloud Shows Big Jump in ABA Tech Survey*, LAW SITES (Aug. 6, 2013), <http://bit.ly/1VE3yqt>.

¹⁶¹ Lewallen, *supra* note 11, at 1145.

¹⁶² *Id.* at 1146-47.

¹⁶³ *See Cloud Ethics Opinions Around the U.S.*, *supra* note 18.

tions have still not issued ethics opinions.¹⁶⁴ Law firms within these jurisdictions have little to no guidance on switching to the cloud or they must outline basic regulations for ESI all on their own.¹⁶⁵

When developing a standard to which attorneys should be held when storing clients' information in the cloud, it helps to consider other jurisdictions' ethics opinions surrounding cloud computing and ESI.¹⁶⁶ Currently approximately 19 states have issued ethics opinions that address cloud computing.¹⁶⁷

A. Arizona's Vague Ethics Standard

Arizona's state bar addressed ethical issues regarding online file storage in 2009.¹⁶⁸ The formal opinion states that a lawyer may use online file storage and retrieval systems as long as reasonable care is used to provide competent legal assistance.¹⁶⁹ Various methods for acting with reasonable care are suggested within the opinion such as the use of a firewall, which is a system designed to control incoming and outgoing traffic on a network,¹⁷⁰ or password encryption.¹⁷¹ The opinion also encourages lawyers to keep current on technological advances.¹⁷² However, overall Arizona's ethics opinion on electronic storage offers vague guidance and little help.¹⁷³

B. California's Overbroad Ethics Opinion

In 2010, California's state bar issued a slightly more detailed formal ethics opinion regarding technology in general.¹⁷⁴ The California opinion requires attorneys to evaluate several factors before using technological developments to interact with clients:

- 1) the level of security attendant to the use of that technology, including whether rea-

¹⁶⁴ See generally *id.*

¹⁶⁵ See Lewallen, *supra* note 11, at 1148.

¹⁶⁶ *Id.* at 1147.

¹⁶⁷ Peyton, *supra* note 115, at 20.

¹⁶⁸ See State Bar of Ariz. Comm. On the Rules of Prof'l Conduct, Formal Op. 09-04 (2009), <http://bit.ly/AZop0904>.

¹⁶⁹ Lewallen, *supra* note 11, at 1148.

¹⁷⁰ Margaret Rouse, *Definition: Firewall*, TECH TARGET, <http://bit.ly/1ST623M> (last visited Feb. 8, 2016).

¹⁷¹ Lewallen, *supra* note 11, at 1148.

¹⁷² See *id.*; see also *Cloud Ethics Opinions Around the U.S.*, *supra* note 18.

¹⁷³ See *id.*

¹⁷⁴ See generally State Bar of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 2010-179 (2010) [hereinafter Cal. Bar Formal Op. 2010-179], <http://bit.ly/CA2010179>.

sonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client's instructions and circumstances, such as access by others to the client's devices and communications.¹⁷⁵

Although California's opinion has a more complete set of guidelines than Arizona's, these guidelines are too uncertain and pertain to technology in general rather than the cloud specifically.¹⁷⁶ California's opinion also surrounds the use of laptops and public wireless connections mostly instead of the storage of electronic information or the cloud.¹⁷⁷ Attorneys are not informed clearly of the precautions that need to be evaluated before switching to the cloud.¹⁷⁸ Without clear and narrow instructions on precautions to take before using the cloud, this jumble of guidelines could cause a misapplication of the rule.¹⁷⁹

C. New York's Clearer Standard

Unlike the California and Arizona opinions, in 2010, New York's ethics committee set forth more detailed steps to follow in using online storage of information.¹⁸⁰ New York's Formal Ethics Opinion 842 states an attorney uses reasonable care when he or she meets the following requirements:

(1) [E]nsur[e] that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information; (2) investigat[e] the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances; (3) employ[] available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or (4) investigat[e] the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.¹⁸¹

This opinion sets out clear and detailed steps for attorneys to follow when storing electronic information without requiring the reader to sift through lengthy, unnecessary clutter.¹⁸² Also included are guidelines ensuring that ethi-

¹⁷⁵ *Id.*

¹⁷⁶ Lewallen, *supra* note 11, at 1148.

¹⁷⁷ See Cal. Bar Formal Op. 2010-179, *supra* note 174.

¹⁷⁸ *Cloud Ethics Opinions Around the U.S.*, *supra* note 18.

¹⁷⁹ See *id.*

¹⁸⁰ See N.Y. State Bar Ass'n Comm. On Prof'l Ethics, Formal Op. 842 (2010) [hereinafter N.Y. Bar Ass'n Formal Op. 842], <http://bit.ly/NYethop842>.

¹⁸¹ *Id.*

¹⁸² Lewallen, *supra* note 11, at 1151 (citing N.Y. Bar Ass'n Formal Op. 842, *supra* note 180).

cal obligations surrounding a law firm's choice of cloud provider are upheld.¹⁸³ The specific duties of a lawyer and risks in the daily use of technology after the integration of cloud computing are outlined as well.¹⁸⁴

D. Pennsylvania Hits the Nail on the Head

In 2011, the Pennsylvania Bar Association issued a formal opinion surrounding the ethical issues involving storing clients' confidential information in the cloud.¹⁸⁵ Pennsylvania's opinion is the most concrete standard among those mentioned because it provides "both internal and external due diligence considerations."¹⁸⁶

The Pennsylvania Committee concluded, "[a]n 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."¹⁸⁷

The Committee goes on to address the standard of reasonable care, recommending several requirements for an outside cloud provider to possess before being hired on by a law firm.¹⁸⁸ Pennsylvania's opinion also lists several potential inclusions for the standard of reasonable care specifically for cloud computing such as backing up data, installing a firewall, and implementing electronic audit trail procedures.¹⁸⁹ It also provides recommended guidelines for insuring the confidentiality agreement between client and attorney is upheld through cloud computing.¹⁹⁰

Pennsylvania's ethics opinion is the most thorough among those issued. It defines cloud computing in great detail and discusses the numerous benefits as well as the potential risks of using the cloud.¹⁹¹ Fifteen specific options for reasonable safeguards for protection of confidential client information from breach, data loss, and other risk are mentioned.¹⁹² This opinion also covers the

¹⁸³ *Id.*

¹⁸⁴ See N.Y. Bar Ass'n Formal Op. 842, *supra* note 180.

¹⁸⁵ See Pa. Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2011-200 (2011) [hereinafter Pa. Bar Ass'n Formal Op. 2011-200], <http://bit.ly/PA2011200>.

¹⁸⁶ Lewallen, *supra* note 11, at 1154.

¹⁸⁷ Pa. Bar Ass'n Formal Op. 2011-200, *supra* note 185, at 1.

¹⁸⁸ *Id.* at 3-4.

¹⁸⁹ *Id.* at 3-4, 8.

¹⁹⁰ Lewallen, *supra* note 11, at 1154 (citing Pa. Bar Ass'n Formal Op. 2011-200, *supra* note 185).

¹⁹¹ See Pa. Bar Ass'n Formal Op. 2011-200, *supra* note 185.

¹⁹² *Id.* at 8-10.

expectations and duties in which non-lawyer employees play when safeguarding of client information.¹⁹³ Its opinion provides step-by-step procedures for switching to the cloud and is the model ethics opinion for any jurisdiction seeking to implement this guidance.¹⁹⁴

VII. A MORE CONCRETE STANDARD IS WARRANTED AND NECESSARY IN EVERY JURISDICTION

With constantly evolving technology, the explosion of electronic information is endless, and the transmission and storage of this information via outdated methods is putting law firms, other businesses, and clients at great risk.¹⁹⁵ Technological advances cannot be ignored. Advances such as the Internet and e-mail have changed the way that attorneys conduct business and interact with clients in a major way.¹⁹⁶ Many lawyers already dump tons of information into the cloud daily by default without realizing that they are doing so.¹⁹⁷ Client e-mails are stored in the cloud even after they are deleted from laptops or smartphones.¹⁹⁸

The prolific use of cloud computing cannot be ignored by the remaining 30 jurisdictions that have not published opinions on the matter for much longer.¹⁹⁹ For instance, the current state of the District of Columbia's Rules of Professional Conduct lack a formal ethics opinion on cloud computing and should be amended to include guidelines for storing electronic information in the cloud.²⁰⁰ Many cases involving highly confidential information as well as national security cases are tried in the District of Columbia.²⁰¹

D.C. Model Rule 1.6 outlines "Confidentiality of Information" within the District of Columbia.²⁰² In its current state, a lawyer may not disclose sensitive client information unless a client has used or is using a lawyer's services to

¹⁹³ *Id.* at 7.

¹⁹⁴ *See id.*

¹⁹⁵ ARKFELD, *supra* note 1, at 3.

¹⁹⁶ *Id.*

¹⁹⁷ *See* Glover, *supra* note 14 (discussing the author's personal experience as a lawyer using the cloud as a default place to store information).

¹⁹⁸ *See* Peyton, *supra* note 115, at 21.

¹⁹⁹ *See generally* *Cloud Ethics Opinions Around the U.S.*, *supra* note 18.

²⁰⁰ *See id.* (listing the jurisdictions that have published ethics opinions on cloud computing, which does not include the District of Columbia).

²⁰¹ *See, e.g.*, *Elec. Privacy Info. Ctr. v. NSA*, 678 F.3d 926, 929 (D.C.Cir. 2012) (discussing a lawsuit under the Freedom of Information Act where plaintiff challenged NSA's Glomar response to an information request); *see also* *Schoenman v. FBI*, 763 F.Supp.2d 173, 177-78 (D.D.C. 2011) (discussing a case where plaintiff sought an array of records pursuant to FOIA and the Privacy Act of 1974).

²⁰² *See* D.C. RULES OF PROF'L CONDUCT r. 1.6(a) (2015).

further a crime or fraud, to prevent further potential crime or injury, to prevent the bribery or intimidation of witnesses, or if consent is given by the client.²⁰³ Section (f) of Rule 1.6 provides that “[a] lawyer shall exercise reasonable care to prevent the lawyer’s employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidences or secrets of a client, except that such persons may reveal information permitted to be disclosed by paragraphs (c), (d), or (e).”²⁰⁴ An easy amendment could be tagged on to the phrase “others whose services are utilized by the lawyer” to include third parties such as outside cloud computing providers.²⁰⁵

In addition to the District of Columbia Bar, every remaining jurisdiction that is lacking an ethics opinion on the matter should issue a formal opinion to amend their current Rules of Professional Conduct to include guidelines for cloud computing within a law firm. These ethics opinions only offer persuasive authority, but around 30 states are lacking any kind of guidance for lawyers using the cloud to store privileged client information.²⁰⁶ If each state implemented an ethics opinion, much like that of Pennsylvania’s, proper steps could be taken to safeguard client information. This would cause a significant decrease in not only data and security breaches but also in failures to uphold the duty of confidentiality and competency requirement.

Much like Pennsylvania Bar Association’s formal opinion, internal and external due diligence considerations should be included in each state’s formal ethics opinion.²⁰⁷ The standard of reasonable care needs to be addressed to accommodate law firms entrusting ESI to third party cloud providers as well as those law firms that store data on-site.²⁰⁸

These ethics opinions should also outline measures that should be taken by law firms choosing a cloud provider. Also instructions on which electronic information should remain on-site, as opposed to transmitted to third party providers, should be included. Law firms should be smart about using the cloud.²⁰⁹ There is no need to store certain documents, such as closed files, in the cloud for easy access.²¹⁰ “You can either have security or conven-

²⁰³ *Id.* r. 1.6(c)-(d).

²⁰⁴ *Id.* r. 1.6(f).

²⁰⁵ *Id.*

²⁰⁶ See *Cloud Ethics Opinions Around the U.S.*, *supra* note 18 (listing and describing the requirements of the twenty jurisdictions that have published a formal ethics opinion).

²⁰⁷ See Pa. Bar Ass’n Formal Op. 2011-200, *supra* note 185.

²⁰⁸ *Id.* at 20.

²⁰⁹ Glover, *supra* note 14.

²¹⁰ *Id.*

ience...Not both. At least not yet.”²¹¹ Unfortunately, cloud security is never 100% guaranteed.²¹² Technology just isn’t there yet.²¹³ Therefore, the cloud should only be used to store highly sensitive information when absolutely necessary.²¹⁴ Guidelines regulating what types of documents should be kept off the cloud and on-site are required.

This new ethics opinion should encourage lawyers to stay up to date with current technological advances because not doing so is a disservice to their clients and their ethical obligations to provide competent legal services.²¹⁵ The new comment to MRPC Rule 1.1 states, “[A] lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.”²¹⁶ Technological skills and knowledge will generally vary depending on practice areas and client needs.²¹⁷

These formal ethics opinions should define cloud computing and outline the benefits as well as the risks associated with using the cloud. Much like the other existing opinions, the standard should be reasonable care, and inclusions for the standard of reasonable care for cloud computing specifically should be addressed. Provisions for non-lawyer employees in the law firm are required as well as third party cloud provider requirements. A thorough analysis with more options will allow a law firm to tailor their ESI needs under proper guidance.

There are regulatory frameworks such as the ethical duty of confidentiality²¹⁸ the safekeeping of client property,²¹⁹ competency,²²⁰ and diligence²²¹ that guide attorneys but the majority of states still have no framework that ties all of these together with respect to regulating ESI and cloud computing.²²² A more concrete standard is required to fill this gap.

The danger of security breaches is very real, and the effects of these breaches are readily viewable from every news source.²²³ With benefits such as convenience, simplicity, and economic gain outweighing the pitfalls of privacy

²¹¹ *Id.*

²¹² *See* Babcock, *supra* note 58.

²¹³ *See id.*

²¹⁴ Glover, *supra* note 14.

²¹⁵ *Id.*

²¹⁶ MODEL RULES OF PROF’L CONDUCT r. 1.1 cmt. 8.

²¹⁷ Peyton, *supra* note 115, at 5.

²¹⁸ MODEL RULES OF PROF’L CONDUCT r. 1.6.

²¹⁹ *Id.* r. 1.15.

²²⁰ *Id.* r. 1.1.

²²¹ *Id.* r. 1.3.

²²² *See id.*; *see also* Lewallen, *supra* note 11, at 1135-36.

²²³ *See* Reed Abelson and Julie Creswell, *Data Breach at Anthem May Forecast a Trend*, N.Y. TIMES (Feb. 6, 2015), <http://nyti.ms/1SCct5I> (discussing the breach of a large health care insurer’s records and how the new trend of keeping electronic records puts the health care field at a higher risk of such data breaches).

risk, more law firms are continuing to make the switch to cloud computing.²²⁴ These attorneys need guidance on switching to the cloud and instructions on maintaining client confidentiality when utilizing the cloud to store sensitive client information.²²⁵

VIII. CONCLUSION

As technology continues to advance, information is becoming easier to access, quicker to download, and more abundant.²²⁶ Cloud computing is the most efficient storage option for electronic information, spatially and financially. The cloud does pose security risks, but proper guidance and precautions aid in preventing a security breach.²²⁷

There are many federal and state laws as well as regulations, ethics opinions, and court-imposed duties that could govern the use of the cloud.²²⁸ As for regulating law firms' use of the cloud, less than half of the country have issued formal ethics opinions to instruct law firms in making the switch to the cloud and maintain client confidentiality after doing so.²²⁹ The option of cloud storage may not be the best tool for every law firm, but the majority of jurisdictions in America cannot continue to ignore it. Standards are an absolute requirement throughout every jurisdiction to guide lawyers through ethical issues surrounding cloud storage.

Pennsylvania's formal ethics opinion hit the nail on the head with the appropriate amount of clarity and guidance.²³⁰ Unlike many other states' ethics opinions on cloud storage, this opinion is thorough, explanatory, and provides numerous options and tools for maintaining client confidentiality while using the cloud.²³¹ The 30 jurisdictions that are still lacking an ethics opinion should implement an opinion much like the one issued by Pennsylvania in 2011.

In 2014, the country watched as our most beloved celebrities bore it all to family, friends, and fans due to their dependence on default cloud settings.²³² Lawyers should take note of this horrific event and cease using the cloud as the

²²⁴ ARKFELD, *supra* note 1, at 4.

²²⁵ Lewallen, *supra* note 11, at 1163.

²²⁶ ARKFELD, *supra* note 1, at 4.

²²⁷ Glover, *supra* note 14.

²²⁸ Ryan, *supra* note 91, at 506.

²²⁹ See *Cloud Ethics Opinions Around the U.S.*, *supra* note 18.

²³⁰ Pa. Bar Ass'n Formal Op. 2011-200, *supra* note 185, at 1.

²³¹ *Id.* at 8-10.

²³² Bennion, *supra* note 136.

default option for storing sensitive information.²³³ There is a lesson to be learned from this unfortunate and gut-wrenching incident. That lesson is to take every precaution to safeguard sensitive client information like it is a personal photograph that you would not want published on the Internet.

²³³ See Glover, *supra* note 14.