CLOUDY WITH A CHANCE OF RAIN: ETHICAL LEGAL PRACTICE IN AN INCREASINGLY DIGITAL WORLD

THOMAS A. KULIK, *Dallas*
Scheef & Stone, LLP

State Bar of Texas
24TH ANNUAL
ADVANCED ESTATE PLANNING STRATEGIES
April 12-13, 2018
Santa Fe

CHAPTER 2

SCHEEF & STONE, L.L.P.
LEGAL COUNSEL BASED ON SOLID PRINCIPLES

ATTORNEY

Education
J.D., Pace University School of Law School, 1993
B.A., Franklin & Marshall College, 1987

Awards

- "Best Lawyers in Dallas", D Magazine, 2016 and 2017

- 1 of 3 IP Columnists Nationwide

Tom Kulik

Tom Kulik is a leading Intellectual Property and Technology Law Partner at Scheef & Stone headquartered in Dallas, Texas. In his 25th year of private legal practice, Tom is a much sought-after technology lawyer, using his skills as a former computer systems engineer to creatively counsel his clients in navigating the complexities of law and technology in their business. With a unique understanding of how intellectual property assets influence business, he strategically counsels clients on matters involving the evaluation, acquisition, development and protection of intellectual property rights, with an emphasis on creatively leveraging such assets both domestically and internationally.

Prior to matriculation in law school, he was an award-winning systems engineer for 3Com Corporation, where he was responsible for local and wide-area network architecture and design supporting both Fortune 500 and start-up companies in the computer services, financial and pharmaceutical industries. After law school, he was appointed to a one-year state judicial clerkship in New Jersey, after which he began private practice splitting his time as a litigation attorney and transactional counsel. Before being recruited to Texas in 1998, he was fortunate enough to act as the primary intellectual property counsel to a consortium of state entities in NJ, NY, PA and DE for the implementation of a $500M electronic toll collection system known as "E-ZPass®".

Leveraging this industry experience, Tom's cutting-edge practice is focused on the legal impact of technology on clients' businesses. He strategically counsels and represents clients as outside general counsel on matters involving the evaluation, acquisition, development and protection of technology and associated IP rights, and creatively leverages such assets both domestically and internationally. His practice spans IT transactions, computer software development/licensing, cloud computing, emerging Internet technologies (such as blockchain and cryptocurrencies), e-commerce, mobile application development, social media/branding, cybersecurity, data privacy and IP/technology litigation. His practice also includes an extensive trademark preparation and prosecution practice, including both domestic and foreign trademark protection, TTAB oppositions, cancellations and appeals, as well as UDRP Proceedings. C-Suite executives regularly seek his assistance and counsel in navigating the increasingly complex intersection of law, business and technology.

T: (214) 706-4223
tom.kulik@solidcounsel.com

Areas of Practice

E-Commerce
Internet & Social Media
Licensing & Technology Transfer
Media & Entertainment
Trademark Preparation & Prosecution
Copyright Litigation
Patent Litigation
Patent Preparation & Prosecution
Trade Secret Litigation
Trademark Litigation

Dallas Office
Ph (214) 706-4200
Fx (214) 706-4242
500 North Akard Street
Suite 2700
Dallas, Texas 75201

ATTORNEY

Education
J.D., Pace University School of Law School, 1993
B.A., Franklin & Marshall College, 1987

Awards

- "Best Lawyers in Dallas", D Magazine, 2016 and 2017

- 1 of 3 IP Columnist Nationwide

He serves as a frequent resource to the media on issues involving the intersection of cyberspace and intellectual property law. National and international news outlets reach out to Tom for his insight. He has appeared on NBC5 DFW and been quoted by such media organizations as CNBC, Reuters and The Dallas Morning News. He is also a weekly IP columnist for AboveTheLaw.com, one of the nation's leading online legal news and entertainment publications. Read more about his thoughts on the intersection of law, technology and business at www.abovethelaw.com/author/tomkulik.

You can also keep up with his musings on various intellectual property law topics via his blog at www.legalintangibles.com.

Media

ICANN and Upcoming Withdrawal of US Oversight - WHDT World News Television Interview. September 2016

The future of ICANN – WSVA Radio interview, September 2016

Internet Openness, Browsing and App History Restrictions, and President Trump's New Law on Privacy – WHBC Radio interview, April 2017

Net Neutrality – John Bohannon Show Radio interview, May 2017

What is Net Neutrality – KGNW Radio interview, May 2017

Publications & Presentations

"The Online Tug-of-War for Copyrighted Content", Dallas Bar Association HEADNOTES, January 2009

"Stormy Weather: Forecasting the Legal Issues in Cloud Computing", Dallas Bar Association HEADNOTES, November 2010

"Typosquatting" and Your Brand: Picking the Fruits of Another's Domain", Direct Selling Association Supplier Course Newsletter, July 30, 2010

"Don't Get Robbed: Patent & Trademark Protection in a Digital World", 2010 Direct Selling Association Legal Issues of the Day Seminar (Washington, D.C. – September 2010)

"Partly Sunny with a Chance of Rain: Forecasting the Legal Issues in Cloud Computing" Dallas Bar Association, Computer Law Section CLE, September 2010

"Harvesting the Fruits of Another's Domain: Protecting Your Brand in a Social Media World", Direct Selling Association Annual Meeting, Miami, FL – June 2011

"Partly Sunny with a Chance of Rain II: Forecasting the Legal Issues in Cloud Computing"' Dallas Bar Association, Computer Law Section CLE, October 2013

"Non-Trademark Issues Trademark Practitioners Should Know" International Trademark Association Roundtable, June 2014

ATTORNEY

Education
J.D., Pace University School of Law School, 1993
B.A., Franklin & Marshall College, 1987

Awards

- "Best Lawyers in Dallas", D Magazine, 2016 and 2017

- 1 of 3 IP Columnist Nationwide

"More Than Meets the iOS: Three Important Takeaways from the Apple/FBI Standoff", Texas Bar Journal, July 2016

"Cybersecurity & Credit Unions: Practical Tools for IT Professionals to Minimize Risk & Legal Liability", Credit Union National Association IT Security Summit, Las Vegas, NV, September 27-28, 2016

"Emerging Issues in the Cloud: Examining the Tension Between Safety and Privacy Rights in 2016 and Beyond", The Knowledge Group LIVE Webcast, October 19, 2016

"Safeguarding Customer Data in an Unsafe World", Panelist, 2016 DSA Business & Policy Conference, Washington, D.C., October 24-25, 2016

"Recent Developments in Videogame Law" , Panelist, Joint Meeting of the Dallas Bar Association Science & Technology Law and Sports & Entertainment Law Sections, Dallas Bar Association, October 26th, 2016

"All Thumbs? Mobile Biometrics, Your Data and the Law", Texas Bar Journal, November 2016

"Don't Let the Cloud Rain on Your Parade. Emerging issues with software-as-a-service providers and ethical obligations.", Texas Bar Journal, February 2017

Quoted in CNBC.com article, "Disney Hacking Shows Why Companies Shouldn't Succumb to Digital Blackmail, Experts Say", May 2017

See library of AboveTheLaw.com articles here (August 2017 – Present)

"Not If, But When…": Limiting the Impact and Liability of a Data Breach, 2017 Credit Union National Association Technology Security Summit, September 2017

"Intellectual Property 101 for Startups", Frisco Chamber of Commerce Entrepreneur Invest Local Kickoff (October 2017)

"Law Firms, Data Privacy and Working on the Cloud", Tennessee Intellectual Property Lawyers Association Fall Seminar, November 2017

"A Rising Sense of (In)Security", Frisco Chamber of Commerce Annual HR Summit, February 2018

"Beyond the Fingerprint: The Legal Risks Involving Mobile Biometrics and Your Data" Practising Law Institute One-Hour Briefing Webinar, March 2018

Bar Admissions

- Texas
- New Jersey

Court Admissions

- U.S. District Court for the Northern District of Texas
- New Jersey District Court

Professional Involvement

- Member, Board of Directors, Earning by Learning of Dallas (a nationally recognized, research driven program, based on the use of incentives to encourage children to learn) – January 2011-present
- Member, Board of Directors, Big Thought (a learning partnership committed to inspiring, empowering and uniting children and communities through arts and culture) 2004-2010
- Past Member, Texas Pro Bono College
- Texas Bar Association: Intellectual Property, Computer & Technology and Entertainment & Sports Law Sections

- Dallas Bar Association Science & Technology Law Section, Treasurer (2011), Vice-Chairman (2012) & Chairman (2013); Member, Intellectual Property Law, Science & Technology Law and Sports and Entertainment Law Sections
- Chairman, State Bar of Texas District 1, Panel 1, Grievance Committee (2016); Panel Chair (2013-2016)

Clerkships

Mr. Kulik served under legislative appointment as a judicial law clerk in Superior Courts of New Jersey for Hon. James P. Courtney, Hon. James N. Citta and Hon. James D. Clyne (1993-1994).

TABLE OF CONTENTS

CLOUDY WITH A CHANCE OF RAIN: ETHICAL LEGAL PRACTICE IN AN INCREASINGLY DIGITAL WORLD

I. INTRODUCTION

Make no mistake - computer technology has been a boon to the practice of law. From the advent of word-processing (sorry, typewriters) to sophisticated eDiscovery software, we now have the capability to process expansive amounts of information faster, more efficiently, and with greater accuracy. That said, it is not without its unique challenges. The advent of software-as-a-service (SaaS) models, mobile platforms and associated "apps" represent interesting challenges, and if you are not careful, such "cloud" services may end up raining on your practice and your client's valuable confidential information.

The focus of this material is to shed light on the uses of technology in your practice and how such technology impacts client confidential information ("CCI") and the ethical obligations all lawyers have to maintaining the confidentiality of such information. By understanding these impacts, lawyers can be better prepared to deal with existing technologies in their practice and inevitable future technological developments without compromising their ethical obligations. If not, lawyers risk "obsoleting" their own ethical obligations, jeopardizing CCI and their legal practice.

II. A CRASH COURSE IN TECHNOLOGY IN LAW PRACTICE

A. Technology in Practice…in Your Practice

Technology touches every facet of law practice today. From word processing programs such as Microsoft Word and Corel's WordPerfect to email communications over the Internet and mobile devices, technology has found its place in 21st century law practice. In fact, earlier technologies (such as fax machines) are rapidly being replaced with scanned files forwarded as attachments to email communications. Oddly, most lawyers do not understand that such technologies, by their very nature, often use data in ways far beyond the content encapsulated in an email or word processing document. Although lawyers need not become technical experts in every software program or platform used in their practice, a basic understanding of certain technologies is necessary and, as you will see, indeed expected so as to protect the attorney-client relationship and associated CCI.

1. Metadata and Your Ethical Obligations

You will be hard pressed to find an attorney nowadays that does not use some form of word processor for the creation, modification and archiving of documentation in their law practice. Further, many lawyers will use software designed to create and/or read scanned documents and/or images as part of their practice (such as Adobe Professional and Adobe Acrobat). Using such software, however, involves the creation of "meta data" - embedded information about the file that is tagged to it…and it covers more than you think.

The Texas Office of the Attorney General has rendered Opinion No. 665 ("Opinion 665") to address CCI contained in such "metadata". The question posed in Opinion 665 was twofold:

> (i) What are a Texas lawyer's obligations under the Texas Disciplinary Rules of Professional Conduct ("TDRPC") to prevent the inadvertent transmission of metadata containing a client's confidential information?
> (ii) What are a Texas lawyer's obligations under the Texas Disciplinary Rules of Professional Conduct when the lawyer receives from another lawyer a document that contains metadata that the receiving lawyer believes contains and inadvertently discloses confidential information of the other lawyer's client?

Opinion 665, p.1.

Opinion 665 is quite instructive and covers both privileged and unprivileged CCI under as defined in Rule 1.05(a) of the TDRPC. In the opinion, "metadata" is defined as "[e]mbedded information that describes the history, tracking, or management of an electronic document", such as the owner of the document, when it was saved or last modified, as well as tracked changes. Opinion 655, p.1. Rule 1.5 of the TDRPC sets for the lawyer's duty to maintain the confidentiality of CCI and obtained through the course of representation, and not "knowingly" revealing such CCI to opposing counsel (subject to some limited exceptions). Opinion 665 makes it clear that:

> a lawyer's duty of competence requires that lawyers who use electronic documents understand that metadata is created in the generation of electronic documents, that transmission of electronic documents will include transmission of metadata, that the transmitted metadata *may include [CCI]*, that recipients of the documents can access metadata, and that actions can be taken to prevent or minimize the transmission of metadata.

Opinion 665, p.2. (emphasis added).

As a result, lawyers "have *a duty to take reasonable measures* to avoid the transmission of confidential information embedded in electronic documents, including the employment of *reasonably available technical means to remove such metadata* before sending such documents to persons to whom such confidential information is not to be revealed pursuant to the provisions of Rule 1.05. See id. Without question, the use of a word processor or other document creation software will result in metadata, but there is an obligation upon each lawyer to ensure that any CCI contained in metadata is scrubbed, converted or otherwise circumvented (such as by printing) prior to forwarding.

2. Beyond the Desktop - Mobile Devices, 'Apps" and Your Legal Practice

Opinion 665 lays an important groundwork for CCI in the context of embedded data, but what most lawyers need to appreciate is that such data is not restricted to the desktop or laptop anymore. Mobile devices have become almost ubiquitous with the advent of the modern smartphone (i.e. iPhone and Samsung Galaxy) and tablet computes (such as the Apple iPad and Samsung Galaxy Tab). Lawyers are not only receiving emails on their smartphones, but also receiving attachments, revising documents and even remotely accessing their workplace computers through these devices. Such convenience has been transformative for attorney-client communications but is equally challenging when viewed through the lens of CCI.

Many attorneys fail to realize that mobile devices and corresponding "apps" make compliance with ethical obligations more difficult. Although most attorneys consider the use of mobile devices to be mere extensions of the use of a desktop, this view is far too narrow. While it is true that mobile devices can access email and documents that involve CCI, the very mobility of these platforms cause greater concern. First, has access to such device been restricted? Although mobile devices such as the iPhone now utilize TouchID (and even FaceID for the iPhone X), many users of these platforms simply do not activate the password feature as a matter of convenience. Of course, this is unacceptable for counsel, and such devices must have access restrictions activated and properly configured.

Further, mobile "apps" cannot be taken for granted. Many apps may be programmed via a metadata-driven design…meaning that their functionality is tied to the use of (and interaction with) metadata. Worse, the Android operating system that powers the mobile phones and tablets of Samsung, Goggle and others is an open-source operating system – a community-driven code platform that is "open" to developers (as opposed to Apple's "closed" system for the iPhone). As a result, many apps developed for earlier Android operating systems (earlier than Android 7.0) may not have settings designed to prevent leakage of metadata of private files. As a result, ensuring that your mobile devices are up-to-date becomes not just good technical practice, but is arguably required *ethical* practice as well.

An even bigger issue, however, stems from how prevalent the use of such apps is becoming with software "services" made available on the Internet. Whether through the browser on the mobile device, or otherwise through a dedicated "app", attorneys are using such "software-as-a-service" more and more to store and access documents that contain CCI. Such use has been driven by availability, reduced costs and convenience; however, it can also be an ethical trap for the unwary.

B. What is the "Cloud"…and Why Should I Care?

When talking about the "cloud", it is important to understand what exactly constitutes the "cloud", and why it matters to your legal practice. When referring to the "cloud", the reference is usually to some internet-based service that may be subscription-based, pay-per-use or even free that usually provides some additional level of capability to an existing computer platform. Unlike programs installed on your local computer (or network server), "cloud" services are *accessed* over the Internet via a web browser, usually after a simple registration process. That said, there are certain characteristics common to "cloud" platforms, as well as common types of platforms, that are worth noting so as to lay the foundation for ethical obligations involving CCI and the use of "cloud" services via any cloud service provider(s) ("CSP(s))".

1. Introduction to the "Cloud" and "Cloud Computing"

Whether you realize it or not, you are most likely using some version of "cloud" services in your daily interactions with your computer or mobile device. Certain characteristics are common, indeed essential, to "cloud" computing platforms:

- **On-demand self-service** – unilateral and automatic provisioning of a user's computing needs
- **Broad network access** – services available through the network to cellphones, PDAs, laptops, iPads, etc.
- **Resource pooling** – dynamic assignment of physical and virtual computing resources
- **Rapid elasticity** – quick scale-out/scale-in – seamless and seemingly unlimited to the user

- **Measured Service** – automatic control to optimize management of resources (storage, processing, bandwidth, accounts)

See *The NIST Definition for Cloud Computing,* National Institute for Standards & Technology, Special Publication 800-145 (September 2011).

These characteristics are generally found in each of the 3 types of "cloud" computing services available on the internet:

- **Software-as-a-Service ("SaaS")** - External software hosting in a cloud infrastructure, such as Google Gmail, Google Drive, Microsoft Office 365 & Apple iCloud
- **Platform-as-a-Service ("PaaS")** - computing platform and "solution stack" for building and running custom applications by the user, such as Windows Azure, Salesforce AppExchange & the Google App Engine
- **Infrastructure-as-a-Service ("IaaS")** - Data processing, storage, network and other fundamental computing resources in cloud infrastructure, such as Amazon EC2, Rackspace & Google Compute Engine

See id.

As you can see, "cloud" computing platforms can take a few different forms, but what needs to be understood is that such scalable, on-demand shared platforms are not controlled by the user – they are *accessed* by the user *over the internet* and usually available as *shared* resources.

2. Why the Cloud Model is A "Perfect Storm" for the Legal Profession

Based upon the information set forth above, it becomes quite clear why the "cloud" model creates a "perfect storm" for the legal profession. The almost ubiquitous availability of services available for email, document creation and storage (even backup and archiving) are due in no small part to the reduced costs for computer processing power, memory and high-speed communications. A perfect example of this is Google Apps – a suite of programs covering, *inter alia*, email (Gmail), calendaring (Google Calendar), word processing (Google Docs), and document storage (Google Drive). These applications are quite useful, available for both desktops, laptops and even mobile smartphones and tablet…and better yet, provided *free of charge*! Unfortunately, this is where potential pitfalls can occur for the unwary practitioner, and care must be taken to ensure that use of the "cloud" doesn't hail on your ethical obligations.

Unlike platforms installed within the law office, "cloud" services use computer "servers' that are not necessarily dedicated to the specific practice or office location. In many cases, the server assigned to provide the services is shared, or otherwise "virtual" (i.e. created by software so that many virtual servers can reside on one physical platform, allowing hardware to be maximized and resources to by dynamically allocated as necessary). Moreover, "cloud" services may actually "fragment" data – specific documents may not all reside on one server in a single location, but may be allocated among a number of servers in multiple locations (and in some cases, outside the U.S.). As a result, the ethical use of "cloud" services requires more than simply registering as a user with the service provider – it requires something *more*.

III. CLIENT CONFIDENTIAL INFORMATION ("CCI") AND THE CLOUD

A. Ethical Obligations regarding CCI

1. ABA Formal Opinion 477R

The ABA Commission on Ethics and Professional Responsibility (the "ABA Ethics Commission") issued ABA Formal Opinion 477R ("Opinion 477r") on May 11, 2017 (revised May 22, 2017) regarding "a lawyer's ethical obligations to protect confidential client information *when transmitting information relating to the representation over the internet*." An update to Formal Opinion 99-413 (1999) that found the use of email to communicate with clients comported with a reasonable expectation of privacy and was ethically permissible under then-current technologies, Opinion 477r sought to address the leaps in technology that occurred since the original 1999 opinion, acknowledging that "legal services now regularly use a variety of devices to create, transmit and store confidential communications, including desktop, laptop and notebook computers, tablet devices, smartphones, and cloud resource and storage locations. Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer's ethical duties." See Opinion 477r, pp. 1-2, *citing* Jill D. Rhodes & Vincent I. Polley, *The ABA Cybersecurity Handbook: A Resource For Attorneys, Law Firms And Business Professionals*, p. 7 (2013). In doing so, the ABA Ethics Commission summarized its finding as follows:

> A lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken

> *reasonable efforts* to p*revent inadvertent or unauthorized access*. However, a lawyer may be required to take *special security precautions* to protect against the inadvertent or unauthorized disclosure of client information *when required by an agreement with the client or by law,* or when the *nature of the information requires a higher degree of security*.

Opinion 477r, p.1. (emphasis added).

In determining "reasonable efforts", the ABA Ethics Commission stressed that a lawyer's duty of competence under Model Rule 1.1 requires an attorney to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology" in order to maintain the requisite knowledge and skill for the practice of law. ABA Model Rules of Professional Conduct, Model Rule 1.1, Comment [8]. Further, the ABA Ethics Commission asserted that the duty of confidentiality under Model Rule 1.6(a) (s modified in 2012) requires that every attorney "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." ABA Model Rules of Professional Conduct, Model Rule 1.6(a) (2016). When addressing the duty of competence and duty of confidentiality together, the ABA Ethics Commission held that "lawyers *must* exercise reasonable efforts when using technology in communicating about client matters." Opinion 477r, p.4. (emphasis added). That said, such "reasonable efforts are not subject to any bright-line test or "hard and fast rule", but "contingent upon a set of factors" that "depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method." See id.

Using this fact-based approach, Model Rule 1.6(c) specifically addresses nonexclusive factors to be weighed when determining "reasonable efforts", such as

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

Model Rule 1.6(c), Comment [18] (2016).

This approach means that circumstances may warrant measures beyond simply sending unencrypted emails, such as encryption of emails or similar "enhanced security measures" for highly sensitive CCI, and may even require the informed consent of the client regarding such use and a discussion of the costs involved. Opinion 477r, p.5. This means that lawyers must "constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable." See id.

Another important point is that lawyers are not ethically bound to be guarantors of the security of client data on their systems, so there is no ethical breach for the unauthorized access to or inadvertent disclosure of CCI since such breaches can occur even where reasonable measures are taken. See Opinion 477r, p.4, Comment [11]. That said, the changes in the technological landscape arguably require lawyers to be *proactive* in the handling of CCI when using "cloud" platforms – lawyers cannot be naïve in the use of technological measures in their practices, and will be required to make "reasonable efforts" in the handling and securing of CCI.

2. Attorney Assistants & Paralegals Must Adhere to Such Standards

Attorney assistants & paralegals are no exception and must adhere to these standards, as they remain under the lawyer's supervision. Comment [18] to Opinion 477r states this requirement quite succinctly:

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Opinion 477r, p. 4, *citing* Model Rule 16.(a),Comment [18].

3. Texas Professional Ethics Committee Opinion 648 (April 2015)("Opinion 648")

Opinion 648 was rendered to address the fundamental question of whether Texas lawyers could use email to communicate CCI. Although the Professional Ethics Committee for the State Bar of Texas ("Ethics Committee") acknowledges that the Texas Disciplinary Rules of Professional Conduct "do not specifically address the use of email in the practice of law", Rule 1.05(b) specifically addresses the confidentiality of both privileged and non-privileged CCI. Opinion 648, pp. 1-2.

The Ethics Committee ultimately permitted "the use of email, including unencrypted email, is a proper method of communicating [CCI]" because Rule 1.05(b) required *knowingly* revealing CCI in violation of the Rule. Opinion 648, p.2. Although such violations are to be viewed on a case-by-case basis, the Ethic Committee expressly stated that "a "person's knowledge may be inferred from circumstances." See id. This is very important to understand – Rule 1.05 can be violated not only if the lawyer *knowingly* discloses CCI to a third-party not authorized to receive it, but arguably *should have known* that such disclosure could occur under the circumstances.

Opinion 648 gives a number of specific examples of whether normal email communication of CCI would be acceptable, or whether more strident security measures (such as encryption) are merited under the circumstances:

- communicating highly sensitive or confidential information via email or unencrypted email connections;
- sending an email to or from an account that the email sender or recipient shares with others;
- sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer (see ABA Commission on Ethics and Professional Responsibility, Formal Op. 11-459 (2011));
- sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an *unsecure network*;
- sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
- sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, with or without a warrant.

Opinion 648, p.3. (emphasis added).

4. Recommended Guidance

Opinion 477r hesitates to outline specific steps that should be taken to ensure "reasonable efforts" to protect CCI have been taken, but the opinion provides very helpful guidance:

- Understand the Nature of the Threat – i.e. Is there a higher risk for "hacking" the CCI?
- Understand How Client Confidential Information is Transmitted and Where It Is Stored – i.e. Do you understand how CCI is accessed, stored and foreseeably transmitted over your system(s)?
- Understand and Use Reasonable Electronic Security Measures – i.e. Have you implemented security measures addressing both *access* and *disclosure* to the firm's computer systems and connectivity solutions?
- Determine How Electronic Communications About Clients' Matters Should Be Protected – i.e. Are alternative non-electronic forms of communication merited given the nature of the CCI?
- Label Client Confidential Information – i.e. Are you marking privileged and confidential client communications, and if so, are you doing so *properly?*
- Train Lawyers and Non-lawyer Assistants in Technology and Information Security – i.e. Are you ensuring that your legal assistants and paralegals are adhering to these requirements?
- Conduct Due Diligence on Vendors Providing Communication Technology – i.e. Are you taking steps to understand how third-party vendor systems store and handle CCI?

Opinion 477r, pp. 6-10.

The above guidelines require more than just simple answers to these questions – steps must be taken in greater detail to address each of these guidelines to ensure that "reasonable efforts" are being taken to protect CCI in your own law firm environment.

B. Security & Privacy of CCI in the Cloud

As you can see, Opinion 477r provides important guidance for making "reasonable efforts" to protect CCI in your law firm systems…but what about your use of "cloud" services? Before diving into this issue, it is important to

understand a simply cybersecurity truth – third-parties are *absolutely targeting law firms for CCI*. Unfortunately, the nature of CCI makes it high-value data that draws the attention of hackers who are using different forms of intrusion to gain access to such CCI. These mechanisms include, but are not limited to malware insertions via phishing/spear-phishing emails and ransomware attacks. As a result, it is essential to understand the risks presented by "cloud" computing to CCI.

1. "Cloud" Services and Your Legal Practice

As discussed above, the use of "cloud" services has become more prevalent in law forms; however, not all "cloud" services are created equal. More importantly, are they "safe" to use in your practice? The answer is…*it depends*. Consistent with Opinion 477r, "reasonable efforts to prevent inadvertent or unauthorized access" must be taken. There are a number of great existing SaaS platforms that can be helpful to legal practice, but each platform must be evaluated on a case-by-case basis. More importantly, understanding how CCI may be stored and shared using a "cloud service" is pivotal. In fact, one can argue that the fact that a "cloud" service has been hacked in the past should be *known* to the potential lawyer or law firm so as to avoid unnecessary risk. For example, Google Docs is a cloud-based document repository that allows for the easy sharing of documents between parties who are registered users of a Google platform (such as Gmail). Unfortunately, Google was hacked in 2014 resulting in the capture of 5 *million* passwords. Other document sharing platforms like DropBox and EverNote were likewise hacked in 2013 and 2014, respectively, with the EverNote hack resulting in over *50 million* passwords being taken and compromised. It is arguably no longer acceptable for lawyers to simply use such platforms from CSPs without some level of due diligence as to (i) security measures implemented by the provider, (ii) storage and handling of CCI by the provider and (iii) whether such mechanisms are consistent with the level of protection that must be afforded such CCI in any particular case.

2. Beware of the Apps You Use and How You Use Them

For the mobile environment, these considerations are even more profound. Unlike desktop systems, smartphones and tablets are inherently mobile, and require a sensitivity to the increased security risks presented by them. Outside of enabling the built-in security features for accessing such devices (such as passwords or other biometric access mechanisms), care must be taken when implementing third-party apps on such devices. For example, Google Docs and DropBox offer free versions of their services; however, these versions do *not* encrypt the data placed in them. To the extent a lawyer seeks to transmit and store documents containing CCI on such platforms, extreme care should be taken to determine if the use of such platforms does not arguably violate the lawyer's duty of competence and confidentiality. See Opinion 477r; Opinion 648, p.2. In certain cases, the platform may provide for a subscription-based service that provides encryption (such as DropBox Business and G Suite). Based upon the potential for data breach and the duties of competence and confidentiality imparted upon every practicing lawyer, careful consideration *must* be given to every platform *before* implementation and use. At a minimum, every attorney:

- *Must* understand the cloud provider's operational model to facilitate compliance with reasonableness standard and whether it fits the need for heightened security (as applicable)
- *Review* cloud provider's terms of use/service and related policies for continuity with these requirements
- *Identify* data security controls at the software level (i.e. encryption, firewalls), as well as physical security, where heightened security is required

C. Contractual Considerations Impacting CCI When Using Cloud Services

Consistent with any due diligence of a "cloud" service platform, it is essential that the terms controlling the use of the "cloud" service by lawyers and their staff be understood in the context of the service itself. As aforementioned, location of service/data is *not* fixed, but distributed…and may in fact be dynamically changed under the terms of use. Moreover, "cloud" service contracts are normally *not* negotiable, which makes risk allocation far more difficult to address. For example, most "cloud" service providers offer little to no indemnity/infringement protection.

Other provisions may be equally troubling. Governing law and venue virtually always favor the CSP, and as for limitations of liability under the terms of use there is usually no liability for damages whatsoever (which means no liability for data deletion, corruption, failure to access, etc.). Limited to no warranties are provided (usually "AS-IS" or "as available"), and any reference to the service being uninterrupted or error-free is usually disclaimed. If there are any service level representations, they are usually limited to certain uptime guarantees that may be inadequate if the documents and CCI cannot be accessed.

As you can see, there are a number of significant considerations that should be addressed by any legal practitioner when considering the use of services provided by CSPs. At a minimum, legal practitioners:

- *Must* take CSP's operational model into consideration to address specific points of impact and allocate risk
- *Review* service levels/credits with a wary eye – they may *not* be enough to cover for impact of downtime of the practice
- *Must* address data export capabilities and ensure compatibility with business continuity and disaster recovery plan

IV. ETHICAL CONSIDERATIONS FOR LAWYERS USING TECHNOLOGY

As outlined above, there are some advisory opinions and related guidance available to help the legal practitioner determine "reasonable efforts' in protecting CCI with technology. Although quite instructive to the use of "cloud" services, such opinions and guidance do not *specifically* address "cloud" services and the use of CSPs. Thankfully, additional steps are being taken by the ABA and states to specifically do so.

The ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies ("ABA Commission") issued a Report on Electronic Confidentiality ("Report") that provides additional guidance. Specifically, the ABA Commission considers "cloud" computing to be a form of outsourcing. See Report, p. 4 (September 2010) *citing* ABA Formal Ethics Opinion 08-451 (lawyer's obligations when outsourcing work to non-lawyers). As a result, the ABA Commission invited comments regarding standard terms and conditions, recommended precautions in use of CSPs and "cloud" services, and even cyberinsurance. See Report, pp. 3-7.

A. State Bar Ethical Opinions Are Few…and Only Go So Far

Currently, twenty-four (24) states address CCI and CSPs by formal opinion. As a general proposition, each of these available opinions state that use of CSPs for the storage of CCI is ethically permissible *so long as a reasonable standard of care is exercised,* there are differences. The 24 states that currently have formal opinions are: Alabama, Alaska, Arizona, California, Connecticut, Florida, Illinois, Iowa, Kentucky, Maine, Massachusetts, New Hampshire, New Jersey, Nevada, New York, North Carolina, Ohio, Oregon, Pennsylvania, Tennessee, Vermont, Virginia, Washington and Wisconsin. Other states are providing more informal guidance, such as Colorado (via tips from its Office of Regulatory Counsel) and West Virginia (via adopting the 2012 revisions to Model Rule 1.1 that lawyer must "stay abreast" of the risks and benefits associated with "relevant technology").

1. A "Reasonable Standard of Care" in Using "Cloud" Services

What would be considered a "reasonable standard of care" regarding CCI stored by CSPs? At a minimum, the legal practitioner must arguably be knowledgeable about CSP's handling of CCI, and must ensure that reasonable safeguards are in place to handle and protect such CCI. Where necessary, the legal practitioner should also contract with the CSP to preserve confidentiality/security of data

Transposing the "reasonableness" standard from "brick & mortar" to the "cloud" is not as easy as you may think. For one, client confidentiality requires strong contractual protections to meet the duty of confidentiality.

Backups – MUST think about IaaS infrastructure
Data access – SLA service credit should NOT be sole remedy
Portability – Transfer of data in event of termination crucial
Bankruptcy of CSP – how to account for possibility?
Use DILIGENCE and COMPETENCE exercising reasonable care
MUST have a BASIC understanding of the technologies used
Have an OBLIGATION to remain current on the technologies

2. Texas Has No Formal Ethics Opinion on Cloud Use, But Other Opinions Instructive

Although Texas currently as no formal opinion regarding storage of CCI in CSPs, other state formal opinions provide helpful guidance. For example, the State Bar of Tennessee has issued Formal Ethics Opinion 2015-F-159, which states in relevant part:

> "A lawyer may ethically allow confidential client information to be stored in "the cloud" if the lawyer takes *reasonable care* to assure that: (1) all such information or materials *remain confidential*; and (2) *reasonable safeguards are employed* to ensure that the information is *protected from breaches, loss, and other risks*. Due to rapidly changing technology, the Board doesn't attempt to establish a standard of care, but instead offers guidance from other jurisdictions."

Formal Ethics Opinion 2015-F-159, p.1 (September 2015) (emphasis added).

This opinion is noteworthy in that it addresses the use of a reasonable standard of care regarding not only confidentiality, but in the reasonable safeguards that should be employed to protect CCI against breaches and other risks – requirements consistent not only with ABA Opinion 477r, but Texas Opinions 648 and 655, *supra*.

By its own admission, other jurisdictions have been instructive in shaping Formal Ethics Opinion 201-F-159 a number of levels. The opinion acknowledges that "the placement of a service provider between the lawyer and confidential client information for which the lawyer is responsible adds a layer of risk and loss of direct control by the lawyer over the stored or transmitted information." Formal Ethics Opinion 201-F-159, p.1 *citing* N.H. Adv. Ethics Op. 2012-13/4 (2013). It also acknowledges that there should be no disparate treatment for CCI in the "cloud" – "[a] lawyer owes the same ethical duties, obligations and protections to clients with respect to information for which they employ cloud computing as they otherwise owe clients pursuant to the Rules of Professional Conduct with respect to information in whatever form." Formal Ethics Opinion 201-F-159, p.1 *citing* Me. Ethics Op. 207 (2013), Ohio Informal Ethics Op. 2013-13 (2013) and Penn. Formal Ethics Op. 2011-200 (undated).; see also Fla. Ethics Op. 12-3 (2012) (urging lawyers to "consider whether the lawyer should use the outside service provider or use additional security in specific matters in which the lawyer has proprietary client information or has other particularly sensitive information.").

The State Bar of Alabama has actually gone so far as to address "reasonable care" with a certain degree of specificity. The Alabama Disciplinary Commission sets forth the conclusion "that a lawyer may use 'cloud computing' or third-party providers to store client data provided that the attorney exercises reasonable care in doing so." Alabama State Bar Disciplinary Commission Ethics Opinion 2010-02, 2010). The Commission defined "reasonable care" as requiring the lawyer to:

- Learn how the provider would handle the storage and security of the data;
- reasonably ensure that the provider abides by a confidentiality agreement in handling the data; and h not binding
- stay abreast of appropriate safeguards that should be employed by both the lawyer and the third party.

Of course, the above is merely a survey of some relevant formal opinions involving the ethical use of "cloud" services for storing CCI. That said, the overwhelming majority of these opinions focus on "reasonable care" to maintain confidentiality of CCI in the "cloud" and implement "reasonable safeguards" to assure that confidentiality of CCI is maintained. Although not binding in Texas, lawyers would be well served in adhering to the guidelines set forth in the formal opinions of these 24 states so as to ensure "reasonable care" in the handling of CCI in the "cloud".

V. CONCLUSION

As a practical matter, lawyers can ethically use cloud computing products in their law practices…but before doing so, lawyers *must* fully assess their ethical obligations and exercise due diligence in vetting the CSP of choice. For Texas practitioners, the absence of a formal opinion does not mean there is no guidance – from ABA Opinion 477r to Texas Opinions 648 and 655 to the various formal opinions of 24 states, ample guidance exists to help shape "reasonable care" in the handling of CCI as well as in the evaluation of CSP services that store such information. At its core, Texas lawyers would be well-served to use their common sense in having a basic understanding of the technologies they are using to store and communicate CCI. In so doing, they will be better positioned to perform due diligence on applicable CSPs, ask the right questions in doing so, and prevent any storm clouds from brewing over client CCI in the process.