ARTIFICIAL INTELLIGENCE & LEGAL ETHICS: "TELELAW" –THE [NEXT] FRONTIER[1,2 3]

GARRETT COUTS, *Lubbock*
Brady & Hamilton LLP

The National Agricultural Law Center & NASDA Foundation
13TH ANNUAL MID-SOUTH AGRICULTURAL AND ENVIRONMENTAL LAW CONFERENCE
June 5, 2026
Memphis, Tennessee

---

[1] Portions of this paper were quoted or adapted from the following paper: *Tech Basics – Tools for Solo and General-Practice Practitioners*, GARRETT COUTS & AL HARRISON, State Bar of Texas 22nd Annual Summer School Course (July 16 - 18, 2020).
[2] Portions of this paper were quoted or adapted from the following paper: *"Telelaw" – The [Next] Frontier*, GARRETT COUTS, American Agricultural Law Association 44th Annual Agricultural Law Educational Symposium (November 9-11, 2023).
[3] Portions of the ELECTRONIC DOCUMENTS & SIGNATURES section of this paper are quoted from or adapted from the following paper: *"Telelaw" – The [Next] Frontier*, GARRETT COUTS & CHRISTINA JENKINS, State Bar of Texas 24th Annual Summer School Course (July 21-23, 2022).

TABLE OF CONTENTS

ARTIFICIAL INTELLIGENCE & LEGAL ETHICS: "TELELAW" –THE [NEXT] FRONTIER

I. INTRODUCTION

Firms big and small are now in a world awash with technology. For better or worse, this is the ***"telelaw"*** age. There is no shortage of reactions to these technological advancements. Practitioners and clients react anywhere within a range from early adopters who would digitize the world if possible, to defiant holdouts that would ban technology if they could. The reality is our individual interests and preferences only matter to a limited point. After that, what clients want – quick, easy, accessible technology – is what clients get.

In addition, our ethical obligations and overall governance of our profession now include obligations related to technology, client privacy and safety, and other tech-related aspects. So, ready or not, it's time to tech-up. Hopefully by the end of this paper, you will feel more prepared to transition some tech-savvy tactics into your practice.

II. ETHICS

A. Ethics & Disciplinary Rules

Numerous states, courts, bar associations, legal-administrative bodies, and other regulatory agencies or authorities with oversight of the legal profession have adopted ethics or disciplinary rules regarding the use of technology.

As you might expect, the approach of regulating technology use in the legal profession varies widely given that each state has its own system for licensing and regulation. Some states have mandatory bar associations, others are directly regulated by the state supreme court, and yet others are subject to oversight by a board elected or appointed as part of the state government.

In addition to individual states, the American Bar Association has also adopted standards regarding the use of technology in legal practice. Primarily, the ABA adopted Comment 8 to Model Rules of Professional Conduct 1.1, which reads as follows:

> [8] 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 relevant technology***, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.[1]

This amendment has been substantively adopted – in some, relatively similar form – in many states. So, for the *"early adopters"* out there – rejoice. For the *"late-comers"* of technology, don't despair, but you might consider a technology-based CLE or technology class.

The expanse of this requirement will differ from firm to firm and lawyer to lawyer, but it is a requirement all the same. Ms. Elizabeth A. Rogers provided an excellent review of the Texas version of this amendment in the May 2019 edition of the Texas Bar Journal.[2] Ms. Rogers summarized the amendment as follows:

> [T]he ethical duty of technology competence may be discharged differently for lawyers in medium to large firms versus lawyers in small firms or solo practitioners.
> . . .
> For small firm lawyers and solo practitioners, the ethical duty of technology competence can present a challenge because most lawyers are not technologists

[1] MODEL RULES OF PROF'L CONDUCT r. 1.1 cmt. 8 (emphasis added).
[2] Elizabeth A. Rogers, *Technology Matters*, Vol. 82, No. 5 Tex. B.J., 325 (May 2019).

> and often lack training and experience in security. Nevertheless, like the duty of legal competence, lawyers in small firms and solo practitioners will be expected to comply with the ethical duty of technology competence by taking continuing legal education courses focused on technology for law practice management and/or by outsourcing information security services to other professionals who are competent in the area or both. These steps will likely be regarded as minimum standards, and failure to comply with them may constitute unethical conduct.[3]

Numerous other states have enacted similar rules regarding technology in the legal profession. The District of Columbia and Puerto Rico have also enacted technology-competency rules.[4] The nine states without a specific technology- competency rule are the following:

1. Alabama
2. Georgia
3. Maine
4. Maryland
5. Mississippi
6. Nevada* (*see footnote 5)
7. New Jersey
8. Oregon
9. Rhode Island[5]

> However, many such rules simply obligate attorneys to "keep abreast of changes in the law and its practice, engage in continuing study and education and comply with all continuing legal education requirements to which the attorney is subject."[6] Therefore CLE obligations could impose technology competency even if the ethics rules do not explicitly include technology competency.

B. Member Benefits and Services - Technology

Luckily, many bar associations and other organizations offer numerous resources regarding technology readiness and education, including ***The State Bar of Texas Computer and Technology Section*** and its widely-viewed ***Tech Bytes*** short videos. Tech Bytes are "byte size" (pun intended) videos providing you an understanding of various technology issues and ways to implement strategies and related tools and techniques to effectively address them. The videos can be found at the following URL on the State Bar of Texas website: https://www.texasbar.com/AM/Template.cfm?Section=articles&ContentID=37530&Template=/CM/HTMLDisplay.cfm.

Additionally, many bar associations have negotiated with numerous *"**Preferred Provider**"* vendors for discounts and benefits for association members. In Texas, the services provided by these vendors

---

[3] *Id.*

[4] Robert Ambrogi, *Tech Competence: 40 States, D.C. and P.R. Have Adopted the Duty of Technology Competence*, LAWSITES, https://www.lawnext.com/tech-competence (last visited April 18, 2026).

[5] *Id.*; SD ST RPC APP CH 16-18 Rule 1.1, Cmt. 6 (South Dakota – Competence). *See also,* AL R RPC Rule 1.1 (Alabama – Competence), GA R BAR Rule 4-102, RPC Rule 1.1 (Georgia – Competence), ME R RPC Rule 1.1 (Maine – Competence), MD R ATTORNEYS Rule 19-301.1 (Maryland – Competence), MS R RPC Rule 1.1 (Mississippi – Competence), NV ST RPC Rule 1.1 (Nevada – Competence), N.J. Rules Prof'l Conduct R. 1.1 (New Jersey – Competence), OR R PROF COND Rule 1.1 (Oregon – Competence), RI R S CT ART V RPC Rule 1.1 (Rhode Island – Competence). *But see* Paul Matteoni, Esq., *2020 - Our Duty of Technology Competence*, NEV. LAW. 4 (2020) (article by then President of the State Bar of Nevada arguing that Technology Competence applies in Nevada); ME R RPC Rule 4.4 (Maine - Respect for Rights of Third Persons; Inadvertent Disclosures) ("The Task Force also recognized the advent of new technologies may alter the nature of some inadvertent disclosures.[…]").

[6] *E.g.*, MD R ATTORNEYS Rule 19-301.1, cmt. 6.

include the following seven categories: (1) *Lifestyle*, (2) *Office*, (3) *Travel*, (4) *Insurance and Finance*, (5) *Professional Liability*, (6) *Regional Offers*, and (7) ***Technology***. These vendors provide a litany of services from billing and online client portals to encrypted email and other cybersecurity services. They also can provide inputs such as computers and other devices for your practice.

C. Malpractice Insurance Coverage

Many malpractice-insurance carriers include ***cybersecurity*** breaches and threats in their coverage. However, you should check with your carrier to ensure you have the coverage needed for your particular practice needs. In addition, many providers will require that you have certain policies, practices, tools, or technological defenses in place in order to obtain a policy or assert a valid claim – such as a ***Document Retention and Destruction Policy***. You should contact your carrier to confirm your coverage and review your policy to ensure you have all of the practices and procedures in place to qualify for coverage should you need to file a claim.

According to the American Bar Association, as of 2022, 46% of respondents reported their firms have cyber liability insurance. "Respondents from firms of 10-49 attorneys are the most likely to have cyber liability insurance (56%), followed by 43% of firms more than 100 attorneys, 42% firms of 2-9 attorneys, 40% firms of 50-99, and 38% for solo attorneys."[7]

III. ENCRYPTED EMAIL & DOCUMENTS

A. Introduction

A primary example of a technology required under the ethical duty of "relevant technology" is ***encryption*** of documents, emails, and other information transmitted electronically or in digital form/medium. As the practice of law has become increasingly reliant upon electronic-based technology for communication with clients, and receipt, transfer, and storage of client information, confidentiality and security associated therewith has unavoidably become critically important.

Have you ever received an email response from opposing counsel or a third-party with that ugly little box stating something like **"CAUTION: External email"**? Or, have you ever been prompted to login to a profile or program in order to see an email or download a document? Each of these is an example of an encrypted email or document system.

It is likely you have seen an increasing number of these emails or encrypted documents from other attorneys – that's no accident. Under many states' ethics rules and opinions, encrypted email and document transmission are now a **requirement** for many practitioners. As always, there are exceptions.

The American Bar Association reports that 49% of respondents utilize file encryption and 40.1% of respondents indicated that email encryption was available.[8]

"Law firms with 2-9 lawyers were at the low end with 30.4%. The percentage increased as the law firm size increased with 500 or more lawyers being at 53.3%. Larger law firms tend to have encrypted email as part of their email service, while the solo and small firm lawyers tend to take advantage of the secure communications capabilities within their practice management system."[9]

For a brief overview of sample encryption duties and types of encryption, review the *Encryption Made Easy (For Lawyers And Clients)* Tech Bytes video at the following URL: https://www.texasbar.com/AM/Template.cfm?Section=articles&ContentID=37530&Template=/CM/HTMLDisplay.cfm.

---

[7] AMERICAN BAR ASSOCIATION, 2022 CYBERSECURITY, https://www.americanbar.org/groups/law_practice/publications/techreport/2022/cybersecurity/ (last visited April 18, 2026).

[8] *Id.*

[9] *Id.*

1. **Why it matters**

As of 2022, approximately 64% of Americans had experienced a cybersecurity breach regarding their personal data.[10] Additionally, Americans have grown less confident in the security of their data as technology has progressed. As of 2019, approximately 70% of Americans believed their personal information is less secure than it was just five years earlier.[11] Approximately 52% of Americans will refuse to use a product or service if they are concerned about the exposure of their personal information.[12] Specifically for law firms, 25% of ABA Survey respondents reported an experience with a firm data breach.[13]

2. Breach Notification & Data Privacy Laws

Many states have enacted ***Breach Notification Laws*** regarding breaches in cybersecurity, ***Data Privacy Laws*** regarding minimum security measures for customer data, or both.

a. **Brach Notification Laws**

Currently, all 50 states, as well as the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have ***Breach Notification Laws***.[14] For example, Texas has enacted the ***Identity Theft Enforcement and Protection Act***.[15] A Texas business, including a law firm, which ***collects*** or ***maintains*** "*sensitive personal information"* in the regular course of business "*shall implement and maintain reasonable procedures, including taking any appropriate corrective action*" to protect the information from unlawful use or disclosure.[16]

Depending upon the extent of the breach, there are varying notification requirements. Many states put thresholds – number of customers affected or amount of data breached – while others apply notification requirements on an individual basis. The requirements of notification can be extensive and the scope of their application broad.

For example, under Texas law, there is no exception, protection, or safe harbor regarding hackers or third-party attacks against your firm's cybersecurity.[17] Meaning, if your clients' personal information or data is stolen by a third-party, you are still subject to the Breach Notification requirements.[18] However, there is an exception for the theft or loss of ***encrypted*** data, which is ***not*** considered "***sensitive personal information".***[19]

b. **Data Privacy Laws**

Additionally, many states have enacted legislation regarding the collection, storage, and use of customer data. As of April 2026, the following 21 states have enacted a data-privacy law in some form:

---

[10] Aaron Smith, *Americans & Cybersecurity*, PEW RESEARCH CENTER (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/.

[11] Brooke Auxier, *How Americans see digital privacy issues amid the COVID-19 outbreak*, PEW RESEARCH CENTER (May 4, 2020), https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/.

[12] *Id*.

[13] AMERICAN BAR ASSOCIATION, 2022 CYBERSECURITY, https://www.americanbar.org/groups/law_practice/publications/techreport/2022/cybersecurity/ (last visited April 18, 2026).

[14] *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (last updated Jan. 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws#:~:text=All%2050%20states%2C%20the%20District,information%20involving%20personally%20identifiable%20information (last visited April 18, 2026,).

[15] TEX. BUS. & COM. CODE § 521.001.

[16] TEX. BUS. & COM. CODE § 521.052.

[17] *See id*.

[18] TEX. BUS. & COM. CODE § 521.053.

[19] TEX. BUS. & COM. CODE § 521.002(a)(2).

1. Alabama
2. California
3. Colorado
4. Connecticut
5. Delaware
6. Indiana
7. Iowa
8. Kentucky
9. Maryland
10. Minnesota
11. Montana
12. Nebraska
13. New Hampshire
14. New Jersey
15. Oklahoma
16. Oregon
17. Rhode Island
18. Tennessee
19. Texas
20. Utah
21. Virginia[20]

Scope. These statutes can vary widely by state – primarily in their scope and their specific security requirements. Some states have narrowly tailored laws only applicable to large-scale businesses (with large data collection practices), while other states have enacted legislation with a broad scope, essentially encompassing most businesses generally. Many states place revenue and data thresholds, while others have sweeping application with limited exceptions for small businesses.

Additionally, these laws may not apply in all contexts. Many such laws only apply to consumers or consumer transactions and do not apply in a commercial or employment context.[21]

Definitions. It is crucial to determine what definitions are applicable in your state. For example, while many states do not include anonymous data or data that is not directly linked to a particular person's identity in their definition of "***Personal Data***" or "***Private Data***", other states do include such data. Texas does include such randomized data if that data can be associated with other information that "can be reasonably linked" to an identified or identifiable individual or that individual's electronic device. "Identified or identifiable individual" means "a consumer who can be readily identified, directly ***or indirectly***."[22]

At first glance, you may believe your firm is beyond the scope of these laws, but a careful review of the definitions may be enlightening. For example, in Texas, subject to exemptions, the following are within the scope of the law:

> a person that:
> (1) conducts business in this state or produces a product or service consumed by residents of [Texas];
> (2) processes or engages in the sale of personal data; and

---

[20] *See* C. Kibby, *US Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (Updated April 20, 2026), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/5QRD-JK3V] (Last visited May 1, 2026).

[21] *E.g.*, TEX. BUS. & COM. CODE ANN. § 541.001(7)("Consumer" means "an individual who is a resident of this state acting only in an individual or household context. The term does not include an individual acting in a commercial or employment context.").

[22] *E.g.*, TEX. BUS. & COM. CODE ANN. § 541.001(19).

(3) is not a small business as defined by the United States Small Business Administration, [with exceptions].[23]

You might think that because your firm does not sell your client's personal data that you are not subject to this law. But, surprise, the definition of "process" or "processing" means "*an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the* ***collection, use, storage, disclosure, analysis, deletion, or modification of personal data****[,]*" which practically encompasses any amount of information that you might collect in your representation of a client. For example, in an estate-planning matter you may collect any or all of the following: Social-security numbers, birthdates, legal names, mailing addresses, children's names, etc., etc., etc. Depending upon your state's definition of "***Personal Data***" any number of these items could qualify as information that is subject to protection from disclosure – and most certainly subject to limitations in its sale.

It is important to determine how your firm's role would be defined under the statute. Different roles have different obligations regarding the consumer data. For example, in Texas, a "***Controller***" means "an individual or other person that, alone or jointly with others, determines the purpose and means of processing personal data[,]" while a "***Processor***" means "a person that processes personal data on behalf of a controller."[24]

Exemptions. Generally, many groups are exempt from these laws, such as the following: healthcare providers which are subject to HIPAA and other federal laws; nonprofits; higher education institutions; governmental agencies and political subdivisions; financial institutions subject to federal regulation or law; some utility providers; and small businesses (as defined by the United States Small Business Administration) but subject to limitations.[25]

Consumer Rights. These laws generally provide consumers with delineated rights regarding their data which usually include rights similar to the following:

(1) confirm whether a controller is processing their personal data and access that data;
(2) correct inaccuracies in their personal data;
(3) request deletion of their data (whether the personal data was provided by the consumer or obtained about the consumer);
(4) obtain a portable copy of their personal data;
(5) opt out of processing for the purposes of targeted advertising, sale of personal data or profiling; and
(6) appeal a controller's refusal to take action on a consumer request to exercise their rights.[26]

3. **Types of Encryption**

Attempting to boil down the exact meaning of "***encryption***" is similar to attempting to objectively determine which ice cream is better, chocolate or vanilla. You will find an answer on either side and several answers in-between.

Merriam-Webster Dictionary defines "*encryption*" as follows:

---

[23] TEX. BUS. & COM. CODE ANN. § 541.002.
[24] TEX. BUS. & COM. CODE ANN. § 541.001(8),(23).
[25] *E.g.*, TEX. BUS. & COM. CODE ANN. § 541.002.
[26] *E.g.*, TEX. BUS. & COM. CODE ANN. § 541.051(b); Natasha G. Kohne, Michelle A. Reed, Molly E. Whitman, Rachel Claire Kurzweil, Joseph Hold*, Texas Data Privacy Act: What Businesses Need to Know*, AKIN GUMP STRAUSS HAUER & FELD LLP (July 28, 2023) (https://www.akingump.com/en/insights/alerts/texas-data-privacy-act-what-businesses-need-to-know).

> *[T]he act or process of encrypting something; a conversion of something (such as data) into a code or cipher.*[27]

There are two primary types of encryption, ***Single-Key*** and ***Paired Public/Private Key***. *The Tech Bytes – Encryption for Lawyers* video provided by *The State Bar of Texas Computer and Technology Section* provides a practical introduction to these encryption types. The video can be found at the following URL: https://www.texasbar.com/AM/Template.cfm?Section=articles&ContentID=37530&Template=/CM/HTMLDisplay.cfm. Below is a brief synopsis of information provided by the *Tech Bytes – Encryption for Lawyers* video.

a. Single-Key Encryption

Single-Key Encryption is simpler and typically accessible on most mainstream programs, etc. You or your client are less likely to need special software or programs to use this type of system.

Single-Key is what most people think of when you say "encryption." It is a single password which both deciphers and provides access to the document or data you have encrypted. However, the simplicity which makes this type of encryption appealing is also its greatest vulnerability. If an unauthorized person gains access to the password, they could gain full access to the information. In other words, the single password is a "single-line-of-defense" system. If the first line of defense is breached, there is no secondary defense in place.

b. Paired Public/Private Key Encryption

A Paired Public/Private Key Encryption is more secure than a Single-Key Encryption, but also far more complex. Think of it like the cliché two-keys needed to push the proverbial "big red button" in an action movie. To launch the rocket, you need both keys and two people in the command room turning the keys in unison.

You would have two "keys," a "private" key and a "public" key. Your client – or the recipient of the document or data you are sending – would have their own private and public key. Four keys in total. When you transmit the information, the public keys are exchanged. The receiving party will need the sender's public key, which was transmitted to them with the document or data, and their own private key. A computer program, whichever program the recipient is using to view the document or data, will match their private key with the public key received from the sender.

If you're thinking "that sounds complicated," you are correct. Nevertheless, it is a secure form of data transmission. The downside is its complexity and the need for software or programs compatible with this form of encryption. You, your client, or both may need to obtain suitable software and walk through prerequisite administrative steps to properly establish your "keys" before this encryption protocol may be used.

c. Practice Tip

Have adequate password-management in place. One option is to maintain a consistent method for generating the passwords specific to a client, or you can save the password in a secure location and reference it later in order to access the encrypted files. There are also a number of password-management applications and software programs which can maintain your passwords for you.

B. Ethics Opinion

If you are scratching your head or contemplating how your clients' data may be at risk, you are not alone. There have been several ethics opinions published throughout the country on various questions of

---

[27] *Encryption*, MERRIAM-WEBSTER DICTIONARY (online), https://www.merriam-webster.com/dictionary/encryption?src=search-dict-hed (last visited April 18, 2026).

data security. For example, *The Professional Ethics Committee* for the *State Bar of Texas* (the "*Committee*") has issued multiple opinions specifically addressing lawyer concerns over the interplay of technology and their clients' data and information.

1. Use of Email for Communicating Confidential Information

a. **Yes, but proceed with caution**

In Ethics Opinion No 648, the Committee of the State Bar of Texas addressed the following question:

> Under the Texas Disciplinary Rules of Professional Conduct, may a lawyer communicate confidential information by email?

The opinion even considered ***unencrypted*** email. The short answer is yes, but it's not quite that simple. In general, considering the present state of technology and email usage, a lawyer may communicate confidential information by email.[28]

The committee begins by clarifying that The Texas Disciplinary Rules of Professional Conduct do not specifically address the use of email in the practice of law[.]"[29] However, Rule 1.05(a) already imposes a substantial obligation on attorneys to protect the confidential information of their clients, including both ***privileged*** and ***unprivileged*** information.[30] This obligation applies to the transmission of information via email.[31]

The standard under the rule is whether a lawyer "***knowingly***" reveals the information to an unpermitted person.[32]

The Terminology section of the Rules states that "'[k]nowingly' . . . denotes actual knowledge of the fact in question" and that a "person's knowledge may be inferred from circumstances." A determination of whether a lawyer violates the Disciplinary Rules, as opposed to fiduciary obligations, the law, or best practices, by sending an email containing confidential information, requires a case-by-case evaluation of whether that lawyer knowingly revealed confidential information to a person who was not permitted to receive that information under Rule 1.05.[33]

The Committee noted that several other state-bar committees have found the use of email, ***both encrypted and unencrypted***, as a proper communication medium for confidential information, including the following committees or bar associations:

1. American Bar Association
2. California
3. Maine
4. New York
5. Alaska
6. Illinois
7. North Dakota
8. South Carolina
9. Vermont[34]

There are two primary points supporting this determination: (1) all communication mediums have an inherent risk of unauthorized access, and (2) persons have a reasonable expectation of privacy in the receipt of email.

---

[28] TEX. COMM. ON PROFESSIONAL ETHICS, Ethics Opinion No 648 (2015).
[29] *Id*.
[30] *Id*.; TEX. DISCIPLINARY R. PROF. CONDUCT Rule 1.05(a).
[31] TEX. COMM. ON PROFESSIONAL ETHICS, Ethics Opinion No 648 (2015).
[32] *Id.*; TEX. DISCIPLINARY R. PROF. CONDUCT Rule 1.05(a).
[33] TEX. COMM. ON PROFESSIONAL ETHICS, Ethics Opinion No 648 (2015).
[34] *Id.*

However, there are certain circumstances that would require an attorney to assess the prudence of ***encrypting*** the email communication, such as the following:

1. communicating highly sensitive or confidential information via email or unencrypted email connections;
2. sending an email to or from an account that the email sender or recipient shares with others;
3. 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 Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011));
4. 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;
5. 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
6. 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.[35]

The committee also noted that this standard may change with the advent of new technologies and technology risks, and that attorneys should consider obtaining a client's informed consent for the use of email.[36] Finally, there may be other authorities, such as *HIPAA*, that prevent the use of email for transmission of client information.

b. **Practice Tips**

Encryption services are readily available. You most likely have received an encrypted email. Financial institutions are required to encrypt almost all of their communications, as are many governmental institutions. You can even have a "***blanket" encryption system*** which encrypts each and every email that you send. Alternatively, you can have individual emails encrypted as necessary.

Also, if you intend to use digital mediums, it is best – although not always required – to get the informed consent of your client. This is beneficial not only from an ethical standpoint, but also from an enforceability perspective. There are numerous other requirements and considerations regarding the use of e-signatures with clients, which we will discuss later in this paper.

2. Use of Cloud-Based Services

a. **Yes, But Proceed with Caution**

You have almost certainly heard about, or use, a cloud-based service of one kind or another either personally or professionally. Cloud computing has essentially revolutionized how we transport, share, store, and maintain files. Because of its essentially limitless capacity, cloud computing has become a staple for managing mass quantities of data and information. Law firm and client data, of course, are no exception to this prevalent phenomenon.

In Ethics Opinion No 680, the Committee addressed the following question:

> Under the Texas Disciplinary Rules of Professional Conduct may a lawyer use cloud-based client data storage systems or use cloud-based software systems for the creation of client-specific documents where confidential client information is stored or submitted to a cloud-based system?[37]

---

[35] *Id.*
[36] *Id.*
[37] TEX. COMM. ON PROFESSIONAL ETHICS, Ethics Opinion No 680 (2018).

Similar to the Committee's consideration of email, Rule 1.05(a) provides the crux of the determination. The short answer is yes, but, again, we have to have those stereotypical-lawyer caveats.

Considering the present state of technology, its common usage to store confidential information, and the potential cost and time savings for clients, a lawyer may use cloud-based electronic data systems and document preparation software for client confidential information[.][38]

Enter stage right, the caveats. The Committee imposed a sort of "inquiry" and "assessment" duty on a lawyer when using cloud-based services.[39]

> [L]awyers should remain continually alert to the vulnerability of cloud-based vendors and systems to data breaches and whether a particular vendor or system appears to be unusually vulnerable, based on systemic failures by that vendor or system of which the lawyer should be aware. In certain circumstances, a lawyer may decide that some client confidential information is too vulnerable to unauthorized access or disclosure to risk its storage or use in a cloud-based electronic system or too vulnerable to such risk without that data being adequately encrypted or without additional technological safeguards in place.[40]

The Committee again emphasized that technology and circumstances change, and attorneys should consider obtaining the informed consent of clients when using cloud-based services, remain aware of such changes, and alter their practices when necessary.[41]

Finally, the Committee delineated six "precautions" which attorneys should implement when using cloud-services for the ***storage*** or ***creation*** of ***client-specific documents which include client confidential information***. *Id*. Those precautions are as follows:

(1) acquiring a general understanding of how the cloud technology works;
(2) reviewing the "terms of service" to which the lawyer submits when using a specific cloud-based provider just as the lawyer should do when choosing and supervising other types of service providers;
(3) learning what protections already exist within the technology for data security;
(4) determining whether additional steps, including but not limited to the encryption of client confidential information, should be taken before submitting that client information to a cloud-based system;
(5) remaining alert as to whether a particular cloud-based provider is known to be deficient in its data security measures or is or has been unusually vulnerable to "hacking" of stored information; and
(6) training for lawyers and staff regarding appropriate protections and considerations.[42]

The Committee's summary of the precautions provides a great rule-of-thumb regarding many of the technology topics we have discussed:

> These precautions do not require lawyers to become experts in technology; ***however, they do require lawyers to become and remain vigilant about data security issues from the outset of using a particular technology in connection with client confidential information.***[43]

b. **Practice Tips**

---

[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id*. (emphasis added).

Many service providers will have a ***Privacy Policy*** readily available for your review. Better yet, especially if you are paying for the service, contact them and request evidence of your state or bar association's required security measures.

It may also be wise to include specific language in your *Engagement Letters/Agreements* if there are particular services, or types of services, that you frequently use which are based upon a cloud platform. An example might be the use of an electronic or digital signatures platform. Many times, the document you are transmitting for signature is not simply attached to a message and sent, but upload to the service-providers server and a link to the document is then provided to your client. Therefore, obtaining your client's consent could prove prudent.

Finally, if you heavily use third-party vendors for information storage and/or transmission, you may consider maintaining an inventory or spreadsheet of all these vendors, their contact information, their privacy policies, etc.

IV. ELECTRONIC DOCUMENTS & SIGNATURES[44]

A. Introduction

Portions of the ELECTRONIC DOCUMENTS & SIGNATURES article of this paper are quoted from or adapted from the following paper: *"Telelaw" – The [Next] Frontier*, GARRETT COUTS & CHRISTINA JENKINS, State Bar of Texas 24th Annual Summer School Course (July 21-23, 2022). I want to give a special thanks to ***Christina Jenkins*** for all of her hard work on this topic.

Electronic signatures are woven into the fabric of the U.S. Economy. Although most practitioners use electronic signatures on a daily basis, fewer of us see them under a microscope. And then, every once in a while, something occurs that requires us to re-visit the concept of electronic signatures. In 2020, that event was COVID when governors, legislators, and practitioners across the country moved business operations, real estate closings, and notarizations online to avoid in person contact.

B. Scope

This paper addresses the law of electronic signatures generally. The law of individual states and circumstances of e-signature use may vary the applicable standards or rules. This paper will primarily discuss the *Uniform Electronic Transactions Act* and the federal *Electronic Signatures in Global and National Commerce Act*, and provide example cases, primarily from Texas, demonstrating the various challenges, issues, and errors regarding those laws.

C. Legal Framework

1. UETA and ESIGN

The legal framework for electronic signatures began in 1999 with the creation of the *Uniform Electronic Transactions Act* by the National Conference of Commissioners on Uniform State Laws (NCCUSL) ("***UETA***"), and in 2000 when Congress enacted the *Electronic Signatures in Global and National Commerce Act* ("***ESIGN***").[45]

a. UETA and ESIGN Similarities.

While not identical in nature, the common purpose of UETA and ESIGN is to supply the same legal validity to electronic closings and signatures as exists for in person closings and wet signatures. Neither UETA nor ESIGN operate to limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under such statute, regulation, or

[44] Portions of the ELECTRONIC DOCUMENTS & SIGNATURES section of this paper are quoted from or adapted from the following paper: "Telelaw" – The [Next] Frontier, GARRETT COUTS & CHRISTINA JENKINS, State Bar of Texas 24th Annual Summer School Course (July 21-23, 2022). I want to give a special thanks to ***Christina Jenkins*** for all of her hard work on this topic.

[45] 15 U.S.C.A. §7001, *et. seq.*

rule.[46] Both UETA and ESIGN are technology neutral, meaning they do not adopt a particular form of technology but rather operate to "provide[e] a solid legal framework that allows for the continued development of innovative technology to facilitate electronic transactions".[47] Notarization and acknowledgment requirements under both laws are substantially the same.

b. **UETA and ESIGN Differences.**

UETA applies to transactions where the parties have already agreed to engage in an electronic transaction.[48] ESIGN, however, sets forth requirements for effective consent and agreement to enter into electronic transactions. UETA takes a procedural approach and provides practical steps to guide unsophisticated parties dealing in electronic transactions. ESIGN focuses on the disclosures required and methods of obtaining a consumer's affirmative consent to engage in electronic transactions.[49]

c. **Federal Preemption.**

ESIGN encourages uniform adoption of UETA by allowing the states to "modify, limit, or supersede" the consumer disclosure provisions of ESIGN by either: i) adopting UETA without changes ("first option"), or ii) enacting their own procedures that comply with ESIGN (and specifically state the intent to supersede ESIGN if the state law was enacted after 6-30-00). When enacting ESIGN, Congress commented that "any variation or deviation from the exact UETA document reported and recommended for enactment… will not qualify for superseding ESIGN under the first option."

UETA – or some version of it - has been adopted in some form by 49 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands.[50] The state of New York, the lone holdout, has enacted its own Electronic Signatures and Records Act (ESRA).[51]

No state has adopted UETA without changes; most states have adopted UETA ***with*** changes; and only one state, North Carolina, has enacted its own procedures that are substantially similar to those in ESIGN. The question of whether a state has effectively opted out of the consumer disclosure requirements of ESIGN is eclipsed by general business practices, which have essentially standardized the use of ESIGN's consent disclosure requirements. Residential mortgage transactions salable to Fannie Mae must also comply with ESIGN.

2. UETA Definitions

Defined Terms. Understanding the terminology related to electronic signatures is critical to understanding the overall concept of electronic signatures for legal documents. For the purposes of this paper, the following UETA definitions are important to know:

> "***Agreement***" means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures given the effect of agreements under laws otherwise applicable to a particular transaction. (In some states, an agreement may be in writing or otherwise. Practice Tip - practitioners should obtain an agreement to engage in electronic transactions for avoidance of doubt as to the intentions of the parties.)
>
> "***Automated transaction***" means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not

---

[46] 15 U.S.C.A. §7001(b)(1).
[47] *See* Prefatory Note to the Uniform Electronic Transactions Act of 1999.
[48] *See* UETA § 5(b).
[49] 15 U.S.C.A. §7001(c).
[50] Uniform Law Commission, *Electronic Transactions Act* (https://www.uniformlaws.org/committees/community-home?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034) (last visited May 2, 2026).
[51] N.Y. State Tech. Law §§ 301-309.

reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.

"***Computer program***" means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.

"***Contract***" means the total legal obligation resulting from the parties' agreement as affected by this [Act] and other applicable law. (Generally, the substantive Law of Contracts applies to contracts entered into electronically.)

"***Electronic***" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

"***Electronic agent***" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.

"***Electronic record***" means a record created, generated, sent, communicated, received, or stored by electronic means.

"***Electronic signature***" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

"***Information***" means data, text, images, sounds, codes, computer programs, software, databases, or the like.

"***Information processing system***" means an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information.

"***Record***" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

"***Security procedure***" means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

"***Transaction***" means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.[52]

3. <u>Scope of Electronic Transactions Subject to the UETA</u>.

Just as the UETA is altered in each state, the scope of its application also varies widely. So, the rule of thumb is this – check what transactions can be executed electronically in the jurisdiction with legal authority over the transaction **<u>and</u>** the parties. If your transaction is crossing state lines – check both states.

As an example, Texas is one of a handful of states that substantially adopted UETA's provisions but also included other state specific provisions. The Texas UETA provides that it modifies, limits, or

[52] UETA § 2.

supersedes the provisions of ESIGN, and so is the controlling law in Texas to the extent that it is consistent with ESIGN.[53]

Unlike many states which have enacted statutes authorizing electronic wills, excluded from the Texas UETA are transactions governed by laws that control the creation and execution of wills, codicils, or testamentary trusts and many of the provisions of the Uniform Commercial Code.[54] Sales and Leases under the Uniform Commercial Code, Chapters 2 and 2A respectively, are subject to the Texas UETA.[55] Certain court reporter or shorthand reporting firm documents used in the state or federal judicial system; or governed by rules adopted by the Texas supreme court, including the electronic filing system established by the court, are excluded from coverage under the Act as it relates to the transmission, preparation, completion, enforceability, or admissibility of those documents.[56] The Texas UETA does not apply to any notice of: i) the cancellation or termination of utility services (including water, heat, and power); ii) default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual; iii) the cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or iv) recall of a product, or material failure of a product, that risks endangering health or safety; or v) any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.[57] Further, it does not authorize any activity that is prohibited by the Texas Penal Code.[58]

Covered Transactions and Method of Agreement.
The UETA does not require the use of electronic transactions and only applies to transactions where the parties have already agreed to conduct transactions by electronic means.[59] Agreement is determined from the context and surrounding circumstances, including the parties' conduct. The critical element is the intent of a party to conduct a transaction electronically. This is different from ESIGN which explains in detail the process needed for obtaining consent to engage in electronic transactions. A party that agrees to conduct a transaction by electronic means has a right, which cannot be waived by agreement, to refuse to conduct other transactions by electronic means.[60] Unless specifically prohibited within the UETA, the effect of any of its provisions may be varied by agreement.[61] Whether an electronic record or electronic signature has legal consequences is decided by the UETA and other applicable law.[62]

Construction and Application. The UETA must be construed and applied to i) facilitate electronic transactions consistent with other applicable law; ii) be consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices; and iii) to effectuate its general purpose to make uniform the law with respect to the subject of this [Act] among States enacting it.[63]

Legal Recognition of Electronic Records, Electronic Signatures, and Electronic Contracts – The Millennials' Dream Come True. Millennials, brace yourselves. One of your dreams is coming true:

1. **Legal Effect**. A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.[64]

---

[53] TEX. BUS. & COM. CODE § 322.019.
[54] *See* TEX. BUS. & COM. CODE § 322.003(b).
[55] *See id*.
[56] *See id*.
[57] 15 U.S.C.A. § 7003(b),
[58] TEX. BUS. & COM. CODE § 322.020.
[59] UETA § 5(b).
[60] UETA § 5(c).
[61] UETA § 5(d).
[62] UETA § 5(e).
[63] UETA § 6.
[64] UETA § 7(a).

2. **Contracts**. A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.[65]
3. **Writing**. If a law requires a record to be in writing, an electronic record satisfies the law.[66]
4. **E-Signature**. If a law requires a signature, an electronic signature satisfies the law.[67]
5. **Evidence**. In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.[68]
6. **Notarization**. If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.[69] Electronic notarizations will be discussed in greater detail below.
7. **Record Retention**. If a law requires: (i) that a record be retained; (ii) a record to be presented or retained in its original form, or provides consequences if the record is not presented or retained in its original form; (iii) retention of a check (practice tip – front and back); or (iv) a person to retain a record for evidentiary, audit, or like purposes (unless the law specifically prohibits electronic records and was enacted after UETA), such law/requirement is satisfied by retaining an electronic record of the information in the record which:
   a. accurately reflects the information in the record after it was first generated in its final form as an electronic record or otherwise; and
   b. remains accessible for later reference.[70]

   This does not apply to any information the sole purpose of which is to enable the record to be sent, communicated, or received.[71] A person may satisfy the above requirements by using the services of another person so long as the service is compliant.[72]

Presentation of Records. All electronic records must be capable of retention by the recipient at the time of receipt.[73] An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record.[74] Furthermore, if a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient.[75]

If another law requires a record (i) to be posted or displayed in a certain manner, (ii) to be sent, communicated, or transmitted by a specified method, or (iii) to contain information that is formatted in a certain manner, the following rules apply:

1. The record must be posted or displayed in the manner specified in the other law.
2. The record must be sent, communicated, or transmitted by the method specified in the other law.
3. Subject to limited exceptions, the record must contain the information formatted in the manner specified in the other law.[76]

---

[65] UETA § 7(b).
[66] UETA § 7(c).
[67] UETA § 7(d).
[68] UETA § 13.
[69] UETA § 11.
[70] UETA § 12.
[71] UETA § 12(b).
[72] UETA § 12(c).
[73] UETA § 8(a).
[74] *Id.*
[75] UETA § 8(c).
[76] UETA § 8(b).

For example, a disclosure required to be in 12-point bold font and delivered before any other document is signed must have the font and priority required by applicable law.

The above requirements cannot be varied by agreement except in the following instances:

1. to the extent a law other than UETA requires information to be provided, sent, or delivered in writing but permits that requirement to be varied by agreement, the above requirement that the information be in the form of an electronic record capable of retention may also be varied by agreement; and
2. a requirement under a law other than UETA to send, communicate, or transmit a record by first-class mail, postage prepaid or regular United States mail, may be varied by agreement to the extent permitted by the other law.[77]

Attributing Electronic Records and Signatures to a Person. An electronic record or electronic signature is attributable to a person if it was the act of the person.[78] The act of the person may be shown in any manner, including a showing of the efficiency of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable, e.g., a "click-through" method.[79] The effect of an electronic record or electronic signature attributed to a person is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law.[80]

Changes or Errors in Electronic Records. If a change or error in an electronic record occurs in a transmission between parties to a transaction, the following rules apply. Assume that the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure, but the other party has not. If the nonconforming party would have detected the change or error, had it also conformed to the procedure, then the conforming party may avoid the effect of the changed or erroneous electronic record.[81]

In an automated transaction involving an individual, the individual may avoid the effect of an electronic record that resulted from an error made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual:

1. promptly notifies the other person of the error and that the individual did not intend to be bound by the electronic record received by the other person;
2. takes reasonable steps, including steps that conform to the other person's reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and
3. has not used or received any benefit or value from the consideration, if any, received from the other person.[82]

If neither of the above scenarios apply to the change or error, then such change or error has the effect provided by other law, including the law of mistake, and any contract between the parties.[83] The provisions relating to automated transactions involving an individual and the application of other law to a change or error cannot be varied by agreement.[84]

---

[77] UETA § 8(d).
[78] UETA § 9(a).
[79] *Id.*
[80] UETA § 9(b).
[81] UETA § 10(1).
[82] UETA § 10(2).
[83] UETA § 3.
[84] UETA § 4.

A party acting through an electronic agent should build in safeguards which enable the customer to prevent sending records with errors. One suggestion in UETA is that the electronic agent be programmed to provide a confirmation screen to be approved by a customer before finalizing the transaction. Electronic signature platforms should establish a procedure for errors or changes and have the customer agree to such procedures.

Automated Transactions. A contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements.[85] A contract may be formed by the interaction of an electronic agent and an individual, acting on the individual's own behalf or for another person, including by an interaction in which the individual performs actions that the individual is free to refuse to perform and which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance.[86] The terms of the contract are determined by the substantive law applicable to it.[87]

An "***electronic agent***" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.[88]

Time and Place of Receipt of Electronic Records. Unless otherwise agreed between the sender and the recipient, an electronic record is ***sent*** when it:

1. is addressed properly or otherwise directed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record;
2. is in a form capable of being processed by that system; and
3. enters an information processing system outside the control of the sender or of a person that sent the electronic record on behalf of the sender or enters a region of the information processing system designated or used by the recipient which is under the control of the recipient. [89]

Unless otherwise agreed between a sender and the recipient, an electronic record is ***received*** when:

1. it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record; and
2. it is in a form capable of being processed by that system.[90]

This applies even if the place the information processing system is located is different from the place the electronic record is deemed to be received under the UETA; and even if no individual is aware of its receipt.[91] Receipt of an electronic acknowledgment from an information processing system establishes that a record was received but, by itself, does not establish that the content sent corresponds to the content received.[92]

---

[85] UETA § 14(1).
[86] UETA § 14(2).
[87] UETA § 14(3).
[88] UETA § 2(6).
[89] UETA § 14(a).
[90] UETA § 14(b).
[91] UETA § 14(c),(e).
[92] UETA § (f).

Unless otherwise expressly provided in the electronic record or agreed between the sender and the recipient, an electronic record is deemed to be sent from the sender's place of business and to be received at the recipient's place of business pursuant to the following rules:

1. if the sender or recipient has more than one place of business, the place of business of that person is the place having the closest relationship to the underlying transaction;
2. if the sender or the recipient does not have a place of business, the place of business is the sender's or recipient's residence, as the case may be.[93]

If a person is aware that a record was not sent or received, then the legal effect of whether it was sent or received is determined by other applicable law.[94]

Unless permitted by other applicable law, these requirements regarding time and place of electronic records may not be varied by agreement.[95]

Transferable Records. A "***transferable record***" means an electronic record that:

1. would be a promissory note under the UCC, or
2. a document under the UCC if the electronic record were in writing; and
3. the issuer of the electronic record expressly has agreed is a transferable record.[96]

A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.[97]

A system satisfies this requirement, and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that:

1. a single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided below, unalterable;
2. the authoritative copy identifies the person asserting control as the person to which the transferable record was issued; or if the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred;
3. the authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;
4. copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;
5. each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and
6. any revision of the authoritative copy is readily identifiable as authorized or unauthorized.[98]

If requested by a person against whom enforcement is sought, the person seeking to enforce the transferable record shall provide reasonable proof that the person is in control of the transferable record.[99] Proof may include access to the authoritative copy of the transferable record and related business records

---

[93] UETA § 14(d).
[94] UETA § 14(g).
[95] *Id*.
[96] UETA § 16(a).
[97] UETA § 16(b).
[98] UETA § 16(c).
[99] UETA § 16(f).

sufficient to review the terms of the transferable record and to establish the identity of the person having control of the transferable record.[100]

Electronic Documents – Government Agencies. Under the UETA, state agencies have discretion on whether to create and retain electronic records and/or convert written records to electronic records.[101]

However, you may find that your state has specifically instructed agencies to conduct electronic transactions or to utilize electronic records or they have prohibited such practices in certain contexts (*i.e*, audits). One federal example would be the *National Archives and Records Administration's Federal Electronic Records Modernization Initiative (FERMI)*.

Common Issues of, Errors of, and Challenges to Electronic Signatures

Practitioners should be aware of how electronic transactions impact everyday practice, from drafting emails to client engagement to negotiating real estate deals. The law of electronic signatures has developed among state trial and appellate courts that have consistently upheld the validity of electronic signatures in accordance with the Construction and Application provisions of the UETA.

For demonstration purpose, the following examples are sourced from Texas case law.

When does an email communication qualify as an electronic signature? This question has generated significant discussion and diverging viewpoints among the courts, and many courts of last resort have yet to directly address the issue.[102]

In cases where there is no dispute that a document was signed electronically, common law generally accepts the legally binding nature of an electronic signature.[103]

Statute of Frauds Defenses. A common challenge to electronic signatures is that they are not a "writing" under the statute of frauds. These cases are fact and state specific. However, as an example, the "from" field in an email is a signature under the Texas UETA that is attributed to the sender, thereby satisfying the Statute of Frauds requirement that an agreement be (1) in writing; and (2) signed by the person to be charged with the promise or agreement.[104] Not all emails, however, will satisfy the statute of frauds. In *Bujnoch v. Copano Energy, LLC*, an email that did not identify the parties to an agreement did not contain all the essential terms of the agreement and did not satisfy the statute of frauds.[105]

Signature Placement or Appearance. Challenges to electronic signatures-based placement or appearance are decided based on the facts of each case and, as described below, the court that hears it. An email containing a signature block without a signature within it is not an electronic signature when no evidence suggests that the information was typed purposefully rather than generated automatically, that the sender intended the typing of her name to be her signature, or that the parties had previously agreed that this action would constitute a signature. Thus, the signature would not satisfy the writing requirement for a Rule 11 Agreement under the TEXAS RULES OF CIVIL PROCEDURES.[106] It's worth mentioning that the court in

---

[100] *Id.*

[101] UETA § 17.

[102] *See e.g.*, *Williamson v. Bank of New York Mellon*, 947 F. Supp. 2d 704, 709 (N.D. Tex. 2013) (venturing an "Erie guess" that the Texas Supreme Court would consider typed names and signature blocks in emails as signatures). *Bujnoch v. Copano Energy, LLC*, 581 S.W.3d 262 at 271, 2017 Tex. App. LEXIS 12048 (Tex. App. Corpus Christi—Dec. 28, 2017), rev'd in part, 593 S.W.3d 721, 2020 Tex. LEXIS 49 (Tex. 2020).

[103] *E.g.*, *Navari, LLC v. Sysco Cent. Tex., Inc.*, No. 03-18-00006-CV, 2019 Tex. App. LEXIS 1002 (Tex. App. Austin Feb. 13, 2019) (Restaurant owner's digital signature on the personal guaranty was sufficient to support a finding of liability because such a signature was legally binding).

[104] *Khoury v. Tomlinson*, 518 S.W.3d 568 (Tex. App. Houston 1st Dist.—Mar. 30, 2017, no pet.); TEX. BUS. & COM. CODE ANN. § 26.01(a)(1)- (2), (b)(2).

[105] *Bujnoch v. Copano Energy, LLC*, 581 S.W.3d 262, 2017 Tex. App. LEXIS 12048 (Tex. App. Corpus Christi Dec. 28, 2017), rev'd in part, 593 S.W.3d 721, 2020 Tex. LEXIS 49 (Tex. 2020).

[106] *Cunningham v. Zurich* American Ins. Co. 352 S.W.3d 519, 530 (Tex. App.—Fort Worth 2011, pet. denied).

Khoury v. Tomlinson disagreed with the holding in *Cunningham*, stating that the holding "*offered no explanation for why physically typing in a signature line at the time of drafting the e-mail should be required for a 'signature block' to constitute a signature.*"[107]

A real estate option contract formed by emails that were signed "*David*" or "*Debbie*" and that set forth the terms, offers, and counteroffers of the parties satisfied the statute of frauds the parties' conduct indicated an intent to conduct the transaction electronically.[108]

"*Thank you, Clyde*" at the end of a Company VP's emails was an electronic signature that, along with the content of the emails themselves, established his acknowledgment of the debt and his intention and willingness to pay it. Further, the court found that the emails were an acknowledgement of the debt extending the statute of limitations under Texas statute.[109]

Contract Offer and Acceptance. Once a signature is determined to be electronic, the courts will look to the context and surrounding circumstances, including the parties' conduct for evidence of an intent to conduct a transaction electronically.[110]

An independent contractor agreement that was emailed to and signed by just one of the parties is a binding contract when, combined with surrounding circumstances (most conversations of the parties were by email), there is evidence of an intent to transact business electronically.[111]

Computer Programs and Other Electronic Agents. Texas courts generally uphold the legal validity of computer programs or electronic agents that include Security procedures to authenticate and record the acts of individual users. This is especially true when backed by pattern, practice, policy and procedure. An employee that electronically signs an arbitration agreement embedded in another document establishes a valid agreement to arbitrate, even if the employee did not see or read the form.[112] The act of an employee using his confidential associate identification number and password, accessing the company's training computer program, clicking through the training, and clicked to acknowledge his completion of the module was sufficient evidence of the employee's agreement to conduct the transaction by electronic means.[113] Evidence of an employer's online application with an arbitration agreement was conclusive proof that an employee consented to the online arbitration agreement by electronically signing it.[114] Employer's evidence of its proprietary hiring computer program, including that the hiring process cannot be complete unless all documents are electronically signed was sufficient to overcome an employee's testimony that he did not execute an arbitration agreement.[115]

Perhaps one of the clearest explanations of the evidentiary hurdle an employee faces against a computer program or electronic agent backed by company policy of mandatory use was in the Burger King Case, where the court stated:

> For Silva to have raised a fact issue, a person would have to conclude the following: Silva completed a paper application although all other Burger King employees completed online

---

[107] *Khoury v. Tomlinson*, 518 S.W.3d 568, 575 (Tex. App.—Houston [1st Dist.] 2017, no pet.).
[108] *See Dittman v. Cerone*, No. 13-11-00196-CV, 2013 Tex. App. LEXIS 13404 (Tex. App. Corpus Christi—Oct. 31, 2013).
[109] *Parks v. Seybold*, No. 05-13-00694-CV, 2015 Tex. App. LEXIS 7685 (Tex. App. Dallas—July 23, 2015).
[110] UETA § 5(b).
[111] *Unique Staff Leasing, LLC v. Onder*, No. 13-09-00213-CV, 2010 Tex. App. LEXIS 9751 (Tex. App. Corpus Christi—Dec. 9, 2010).
[112] *H-E-B, LP v. Saenz*, No. 01-20-00850-CV, 2021 Tex. App. LEXIS 8283 (Tex. App. Houston 1st Dist.—Oct. 12, 2021).
[113] *Wal-Mart Stores, Inc. v. Constantine*, No. 05-17-00694-CV, 2018 Tex. App. LEXIS 3023 (Tex. App. Dallas Apr. 30, 2018).
[114] *Fries Rest. Mgmt., LLC v. Silva*, No. 13-18-00596-CV, 2020 Tex. App. LEXIS 5970 (Tex. App. Corpus Christi—July 30, 2020) ("*Burger King Case*").
[115] *Aerotek, Inc. v. Boyd*, 624 S.W.3d 199 (Tex. 2021).

> applications and Burger King utilizes a paperless application system; (2) Silva's paper application disappeared from her personnel file; (3) Burger King somehow anticipated Silva would sue Fries such that someone other than Silva forged an online job application using her name, personal contact information, social security number, education, job history, e-mail address, and personal references; (4) someone other than Silva signed the online application on Silva's behalf and retroactively applied a date and time stamp to coincide with the date she claims she filled out a paper application; (5) and Arteaga managed to include Silva on payroll even though she did not fill out the required online forms. Fries' evidence proves that such a set of events is highly unlikely such that it was sufficient to raise a genuine issue of material fact.[116] In other words, the evidence presented by Fries conclusively establishes the opposite of Silva's testimony.[117]

In *Holmes v. Air Liquide USA LLC*, the court states that "[w]hile it is conceivable that someone else could have used Holmes' unique log in information to access her computer, her email, and her HR site, and then signed the ADR agreement on her behalf, Defendants' evidence proves that such a set of events would be highly unlikely."[118]

Not all courts agree with the above analysis. In denying Kmart's motion to compel arbitration, The Eighth District Court of Appeals in El Paso ("El Paso court") held that hearing testimony from an employee denying that she ever received or knew about the agreement created a genuine fact issue on notice that the trial court could have resolved in her favor, even though Kmart's electronic records purportedly show her unique login credentials were used to access and acknowledge the agreement on the online portal. Refusing to overturn the decision of the trial court, The El Paso court continued: "[w]e trust in the ability of the lower courts to resolve factual discrepancies, to discern the truth, and to ferret out dishonest or perjurious attempts by employees to avoid the ramifications of failing to read employer notices."[119]

Multiple Electronic Documents. Electronic signatures on emails may bind parties in a transaction. Whether or not a contract exists could depend on the combined content of one or more emails. In the Dittman case, electronic signatures on emails exchanged between the parties created a real estate option contract that satisfies the statute of frauds because the conduct of the parties in three emails, read together, indicated an intent to conduct the transaction electronically.[120] In so holding, the Dittman court stated that "[i]t is well-established law that instruments pertaining to the same transaction may be read together to ascertain the parties' intent."[121] "This rule is echoed in statute of frauds jurisprudence: in order to satisfy a statute of frauds, multiple documents can be read together."[122] "The multiple documents need not contain all of the terms; instead, only the essential terms are required."[123]

A Sample Challenge – Texas - *Aerotek V. Boyd*

Providing a comprehensive review of the various cases brought throughout the country regarding e-signatures would be a daunting task to say the least and most certainly would cause time-constraints on the author's career with the certainty of fame that would come with having cured insomnia.

So, instead, the Aerotek case from Texas will be used as a single sample of how e-signatures can face varied and unique challenges.

---

[116] *See Holmes v. Air Liquide USA LLC*, No. H-11-2580, 2012 U.S. Dist. LEXIS 10678, 2012 WL 267194, *3 (S.D. Tex. Jan. 30, 2012), aff'd on other grounds, 498 Fed. Appx. 405 (5th Cir. 2012)).
[117] *Id*. at 9-10.
[118] *Id.*
[119] *Kmart v. Ramirez*, 510 S.W.3d 559 (Tex. App.— El Paso 2016, pet. denied).
[120] *See Dittman v. Cerone*, No. 13-11-00196-CV, 2013 Tex. App. LEXIS 13404 (Tex. App. Corpus Christi Oct. 31, 2013).
[121] *City of Houston v. Williams*, 353 S.W.3d 128, 137 (Tex. 2011) (citing *Fort Worth Indep. Sch. Dist., 22* S.W.3d at 840) [*11] (internal quotations omitted).
[122] *Id*. at 137 n.9 (citing the Restatement (Second) of Contracts § 132).
[123] *Id*. at 137.

On May 28, 2021, the Texas Supreme Court decided the Aerotek case. The issue before the court was "how the efficacy of a security procedure is shown and, once it is, whether the alleged signatory's simple denial that he signed the record is sufficient to prevent attribution of an electronic signature to him".[124]

Why Aerotek Matters

What makes Aerotek important is that the court took the opportunity to hear this case, a task it had been leaving to lower courts to decide for years. First, the Court settled the question of whether an employee's affidavit denying the intent to create an electronic agreement to arbitrate, without any further evidence, is sufficient to overcome an employer's showing of that employee's use of a Computer program and/or Electronic agent backed by Security procedures to authenticate and record the acts of individual users and company policy, pattern, and practice. Spoiler Alert: It isn't. Second, the Court reaffirmed the Texas UETA and used its analysis to demonstrate the relationship between the Texas UETA and other applicable law. The Texas UETA provides the set up. Common law fills in the blanks. Third, the opinion confirms that, for the most part (except for in this case), Texas lower courts have gotten it right.

Factual Background. Aerotek is an employment agency that supplies contract labor to its clients. Aerotek's hiring process is all electronic. Job candidates may only apply online using Aerotek's proprietary Computer program and Electronic agent that it purchased from Smart ERP and hired a developer to create it as an add-on to its existing HRIS system.

> Aerotek's hiring application automatically sends a welcome email to the email address the candidate has provided during the recruitment and initial interview process. The welcome email includes a unique hyperlink for the candidate to use to navigate to the hiring application's online account-registration page. Once there, the candidate creates a unique user ID and password and selects security questions. To later log in to the hiring application, the candidate must enter this user ID, password, and security-question combination correctly. This login process takes place each time the candidate leaves and returns to the hiring application.[125]

Four men applied for contract positions at Aerotek using the online application process. One of them needed assistance and so went into Aerotek's corporate office to complete his online application. The Court described the online process as follows:

> The first document requiring an electronic signature is an Electronic Disclosure Agreement (EDA). By signing the EDA, the candidate consents to "be bound" by Aerotek's electronic hiring documents "as though . . . signed . . . in writing." After the candidate signs the EDA, the application presents other documents to the candidate for completion and signature. These documents ask for personal information, such as addresses and emergency contacts. The application requires candidates to complete and electronically sign the documents in a particular order. After the candidate completes the initial documents, the application unlocks four additional documents, including a Mutual Arbitration Agreement (MAA). The candidate may electronically sign these documents in any order, but he must complete all four before the computerized application will allow him to continue and complete the hiring process.[126]

All four men were hired and fired by Aerotek in short order. Thereafter, they sued Aerotek (and others) for racial discrimination and retaliation. Aerotek filed a motion to compel arbitration attaching a copy of all four electronically signed Electronic Disclosure Agreements and Mutual Arbitration Agreements.

---

[124] *Aerotek, Inc. v. Boyd*, 624 S.W.3d 199 (Tex. 2021).
[125] *Id*. at 201.
[126] *Id.*

Procedure. The trial court, after hearing testimony and weighing the evidence, denied Aerotek's motion to compel arbitration. The appeals court affirmed. The supreme court reversed the judgment of the court of appeals and remanded the case back to the trial court for further proceedings.

The Opinion (and Dissent). The court found that Aerotek conclusively established that the Employees signed, and therefore consented to, the MAAs by providing uncontroverted evidence of the Security procedures it uses to authenticate electronic records. The court began by stating that "[t]he efficacy of the security procedure provides the link between the electronic record stored on a computer or in a database and the person to whom the record is attributed. A record that cannot be created or changed without unique, secret credentials can be attributed to the one person who holds those credentials".[127]

From there, the court turned to the evidence presented by the parties, noting that it must defer to the trial court's factual finding that the Employees did not sign the MAAs if that finding is "supported by evidence". The court found that the employees admitted to completing Aerotek's computerized hiring application and electronically signing all other documents but the MAA.

> Aside from their denials, the employees offered no evidence to support their allegation that they did not electronically sign the MAAs that Aerotek introduced into evidence. Instead, they simply argue that Aerotek's evidence fell short of establishing the efficacy of the hiring application's security procedures. According to the Employees, the trial court was free to disregard Aerotek's witnesses.
>
> Aerotek's evidence showing the security procedures its hiring application used to verify that a candidate electronically signed his MAA was uncontroverted. To enter the application, a candidate was required to create for himself a unique identifier, a user ID, a password, and security questions, all unknown to Aerotek. The candidate was required to Texas Electronic Signatures enter personal information and sign documents by clicking on them. The application recorded and timestamped the candidate's every action. The application's business rules made it so that the application could not be submitted until all steps were completed and all required signatures provided, including on the MAA. Once a candidate submitted his application, Aerotek could not modify its contents. Aerotek provided the signed MAAs marked with timestamps identical to those in its database records showing each Employee's progress through the application.[128]

In finding that Aerotek had met its burden, the court established that the testimony of Aerotek's program manager and administrative assistant was not diminished because they were not experts. Moreover, the court was persuaded by the program manager's demonstration of the security procedures built into the platform in open court, along with testimony that the hiring application's rules would have prevented the employees from completing the hiring process until all documents were electronically signed. Likewise, the administrative assistant's testimony that "hundreds of times" she used the same "very strict" and "very structured" procedure to help applicants apply for jobs, specifically by showing the how to: i) retrieve Aerotek's welcome email, ii) create username and password, iii) input biographical information, and iv) sign the arbitration agreement. After the process is complete, she made sure everything was entered and signed electronically making sure to get renew consent to continue with each step of the process to completion.[129]

From here, Aerotek looks like the lineup of trial and appellate cases holding that a valid electronic signature supported by Security procedures to authenticate and record the acts of individual users; and

---

[127] *Id*. at 200 (quoting TEX. BUS. & COM. CODE § 322.009(a)).
[128] *Id*. at 205.
[129] *See Id.* at 207-208.

further supported by pattern, practice, policy and procedure results will prevail over an affidavit that does not challenge those Security procedures.

It is worth noting that Aerotek's dissenting opinion issued a pointed rebuke of the Aerotek majority.

> To put things bluntly, someone here testified under oath to facts that cannot be true. Either the employees were wrong (or lying) when they denied that they ever saw or signed the arbitration agreement, or Aerotek's program manager was wrong (or lying) when she described how the electronic-onboarding process works.
>
> Under our well-established standard of review, this Court's assessment of the truth is irrelevant.[130]

Last Words on Aerotek. Four months after Aerotek was decided, it was heavily relied on in *Knox Waste Serv., LLC v. Sherman*, where the court held, consistent with Aerotek, that an affidavit of denial alone is not sufficient to create a fact issue to be decided by a trial court.[131]

In the author's sole opinion, the Aerotek case sets the stage for a battle of the evidence in future cases. You do not need the best evidence to trump the worst (or no) evidence, but prepared Texas Electronic Signatures practitioners will know to produce something more than an affidavit of denial. How much evidence is enough? I guess we'll just have to wait and see.

Lessons Learned And Best Practices From The Aerotek Case

Practitioners should avoid the temptation to dismiss Aerotek as just another arbitration case. This supreme court decision affects all electronic signatures and transactions in some way. Attorneys use Computer programs and Electronic agents every day to correspond with clients, conduct business, and communicate legal issues via document preparation, client management software, and email, to name a few.

After Aerotek, what we know is:

1. A sworn affidavit denying the existence of an electronic agreement will not stand up against Computer programs or Electronic agent with verifiable Security procedures for attributing and electronic signature to a person coupled with evidence of policy, pattern, and practice that back up those procedures;
2. Plaintiffs seeking to challenge electronic signatures obtained through a Computer program or Electronic agent must produce evidence that discredits the technology or the reliability of the policy pattern, or practice;
3. Expert testimony (or even testimony by the architect of a Computer program or Electronic agent) is not necessary.
4. While the Texas UETA itself is technology neutral, certain Security procedures have been upheld by the courts. Some examples are assigning a unique identifier to a user and then tying that identifier to the user's actions; maintaining a single, secure system for tracking user activities that prevents unauthorized access to electronic records, business rules that require users to complete all steps in a program before moving on or completing it; and timestamps showing when users completed certain actions. These examples are illustrative and not exclusive under Section 322.009(a).[132]
5. It is still true that Texas courts have upheld electronic signatures and transactions based on less than the most sophisticated Computer programs and Electronic agents. As noted by the Aerotek court, While handwritten signatures are unique to an individual, electronic signatures sometimes

---

[130] *Id*. at 212.
[131] *Knox Waste Serv., LLC v. Sherman*, 2021 Tex. App. LEXIS 8010 (Tex. App. Eastland Sept. 30, 2021).
[132] *Aerotek, Inc. v. Boyd,* 624 S.W.3d 199, 205-206.

involve nothing more than clicking a box online and recording the information in an electronic database.[133]

Practice Tips. Among the ways practitioners can protect themselves and their clients from the unintended consequences of engaging in electronic transactions (e.g., creation of unintended contracts and discoverable evidence) are the following.

1. **Get it in writing!** Making sure that all electronic agreements include a consent to engage in electronic transactions and to be bound by the terms of the electronic agreement. While some state UETA statutes do not require a disclosure similar to that required by ESIGN, case law holdings show that parties with written or system documented evidence of an electronic agreement tend to prevail.
2. **Reviewing company or law firm electronic communication methods for risk exposure**. Deciding if there is a need for permission levels, limitations of use, or agreements (both internally (think HR) and externally) to limit any discovered risk. For example, if a firm uses an electronic document vendor so that clients can electronically sign contracts and engagement letters, review the consent agreement attached to each transaction and revise it as necessary.
3. **Creating an email use and communication policy that describes the circumstances under which electronic signatures can be used**. Ensuring that the written policy is consistent with internal operations. *See also Developing an Effective Electronic Signature Policy* published by Adobe and accessible at: https://www.adobe.com/content/dam/dx-dc/pdf/ue/wp-document-cloud-esignature-policy-ue.pdf
4. **Training** employees on acceptable forms of communication when using customer facing Electronic agents, such as emails and customer relationship management (CRM) platforms.
5. **Security Procedures and Features**. Ensuring that Computer programs or Electronic agents used by the firm for hiring, contracts, engagements, etc., include Security procedures and features found to be acceptable by statute and applicable case law. If outsourced, asking the vendor for substantiation of the Security procedures, whether they have ever been breached, and whether there is a notification procedure in place to advise (or prepare a report for) the firm if there ever is a breach of the Security procedures.
6. **Review.** Reviewing Computer program and Electronic agents used by the firm to ensure that they supply the best evidence of consent to enter into electronic transactions. For example, figure out whether the user should be required to sign every document, scroll to the bottom of the page and sign before moving on to the next document, etc. Note that in the Aerotek case, the employees did not challenge the Electronic Disclosure Agreement, which was the first document they signed, set apart from all others, and required their consent to be bound by the electronic documents before advancing to the next group of documents.
7. **Storage & Retrieval.** Reviewing electronic records to ensure they follow the storage and retrieval requirements of the UETA.
8. **Choice of Law**. Considering the law governing electronic transactions when drafting (or reviewing) choice of law provisions in contracts.

Electronic Documents & Signatures - Conclusion

There is no question that electronic signatures make our lives easier. Attorneys using electronic technology can engage clients, draft documents, work, and litigate cheaper, faster, and more efficiently in today's world. Although technology innovation moves at a faster pace than the laws regulating it, practitioners with a working knowledge of the laws affecting electronic signatures are better positioned to reap the benefits of engaging in electronic transactions without experiencing the burdens of the unintended consequences we see in case law. The good news is that resources abound for attorneys to conduct safe and

[133] *See id.* at (quoting *Realogy Holdings Corp. v. Jongebloed,* 957 F.3d 523, 527 & n.1, 528, 532 (5th Cir. 2020)).

efficient electronic transactions; and there are good, cost-effective vendors that outsource electronic platforms specifically designed for law firm management, legal services, document drafting, document execution, and more.

V. ELECTRONIC NOTARIES

A. Background

As you might expect, with the proliferation of electronic signatures has come the same demand for electronic notarization. Because practically, what use is an electronic signature if the document must be physically notarized? Zero. The answer is zero.

Notaries are generally governed by a combination of statutory authorities and regulations imposed by the Secretary of State (or equivalent office) in each state.

Currently, 47 states and the District of Columbia have laws allowing remote e-notarization.[134] The National Association of Secretaries of State has adopted e-notarization standards to provide guidance to the states and many of the state laws incorporate those standards, but of course specific requirements and procedures vary among states.[135]

Federally, legislation has been introduced in the House (HR 1777) to authorize e-notaries and remote notarization nationwide.[136]

The National Association of Secretaries of State ("*NASS*") has published an *eNotarization Implementation Guide ("iGuide")*.[137] NASS also provides numerous resources regarding the *Revised Uniform Law on Notarial Acts (2021) ("RULNA")*.

Although RULNA is intended to be a uniform law, because notary publics are regulated by the individual states, the implementation of e-notarization varies widely and many states substantially deviate from the RULNA provisions or heavily supplement them with regulation.

B. General Requirements

Although there are numerous nuances to the requirements for licensure of e-notaries and use of e-notarization, a brief recitation will likely serve you best at this point. So, here is a brief summarization of the requirements for online notaries based upon the e-notarization law of Texas[138]:

(1) Many states require that e-notaries already be a licensed Notary Public (and have met all of those licensure requirements).
Example - **Texas**:
(a) Notary identification number assigned by Secretary of State
(b) Date of birth;
(c) Last four digits of social security number;
(d) Last name; and
(e) Valid email address; and
(f) Must not have been convicted of a felony or a crime involving moral turpitude.

(2) Must have or obtain the following the proper electronic certificates, seals, and markings etc.:
Example – **Texas**:
(a) Digital Certificate

---

[134] *Remote Electronic Notarization*, NAT'L ASS'N OF SEC'YS OF STATE, https://www.nass.org/initiatives/remote-electronic-notarization (last visited May 2, 2026).
[135] *Id*.
[136] *Id*.
[137] *NASS eNotarization Implementation Guide*, *Version 1.0*, NAT'L ASS'N OF SEC'YS OF STATE (Feb. 18, 2017), https://www.nass.org/sites/default/files/surveys/2017-08/NASS-NPA-iGuide-v1.0-0217.pdf.
[138] TEX. GOV'T CODE ANN. §§ 406.101-113; 1 TEX. ADMIN. CODE §§ 87.40-87.44; TEX. ADMIN. CODE §§ 87.50-87.54.

(i) Must be issued by a third-party provider
(ii) Must use Public Key Infrastructure (PKI) technology and be X.509 compliant
(iii) Must make any changes to a document, made after the Certificate is affixed, evident.

(b) Electronic Seal

(i) Requirements elements/contents:

(A) The words "Notary Public, State of Texas" around a star of five points;
(B) The notary public's name;
(C) The notary public's identifying number; and
(D) Date the notary public's commission expires
(online notary public commissions expire on the same date as the notary public's traditional commission).

(ii) Appearance:

(A) circular form no more than two inches (2 inches) in diameter; or
(B) rectangular form not more than one-inch (1 inch) width by two-and-one-half inches (2.5 inches) length; and
(C) must have a serrated or milled edge border

(c) Ability to do the following:

(i) Maintain an electronic record of the online notarization, including a recording and backup of the audio-visual conference.

(A) Record Keeping:

(1) the date and time of the notarization;
(2) the type of notarial act;
(3) the type, the title, or a description of the electronic document or proceeding;
(4) the printed name and address of each principal involved in the transaction or proceeding;
(5) evidence of identity of each principal involved in the transaction or proceeding in the form of:

(a) a statement that the person is personally known to the online notary public;
(b) a notation of the type of identification document provided to the online notary public;
(c) a record of the identity verification made under Section 406.110, if applicable; or
(d) the following:

(i) the printed name and address of each credible witness swearing to or affirming the person's identity; and
(ii) for each credible witness not personally known to the online notary public, a description of the type of identification documents provided to the online notary public;

(6) a recording of any video and audio conference that is the basis for satisfactory evidence of identity and a notation of the type of identification presented as evidence; and
(7) the fee, if any, charged for the notarization.

(ii) Use a third party to perform ***Identify Proofing*** and ***Credential Analysis***

(A) Third-party provider (Sec. of State SOS will not provide or suggest one); and
(B) Using ***Dynamic Knowledge-Based Authentication*** (KBA) technology

(3) Must acknowledge they will comply with the required procedures (as they generally administer oaths also):
Example – **Texas**:
(a) Will comply with the standards for *Identify Proofing and Credential Analysis*.
(b) Will use a third-party provider meeting the requirements for such provider
(c) Will, upon request by the secretary of state, promptly provide any necessary instructions or techniques supplied by a vendor that allow the online notary public's digital certificate and seal to be read and authenticated.
(d) Meet the eligibility requirements to be commissioned as a Texas notary public by being at least 18 years of age, a resident of the State of Texas, and having not been convicted of a felony or a crime involving moral turpitude.

(4) Some states also require the notary to execute their own oath of office. Example – Texas – download, and sign (digitally), save, and upload back to the Secretary of State the ***Statement of Officer***.

(5) Upload or submit seal, meeting the requirements for such seal.

(6) Pay the applicable fees – if any.

C. Terms & Technologies of E-Notaries

1. Digital Certificates - "Electronic notarial certificate"

There is no definition of "***Electronic notarial certificate***" under RULNA. In Texas, "***Electronic notarial certificate***" means the portion of a notarized electronic document that is completed by an online notary public and contains the following:

(A) the online notary public's electronic signature, electronic seal, title, and commission expiration date;
(B) other required information concerning the date and place of the online notarization; and
(C) the facts attested to or certified by the online notary public in the particular notarization.[139]

2. Official Stamps & Electronic Seals

RULNA uses the terms "***Official Stamp***," which means "a physical image affixed to or embossed on a tangible record or an electronic image attached to or logically associated with an electronic record."[140]

"***Electronic seal***" means information within a notarized electronic document that confirms the online notary public's name, jurisdiction, identifying number, and commission expiration date and generally corresponds to information in notary seals used on paper documents.[141]

---

[139] TEX. GOV'T CODE ANN. § 406.10(4).
[140] RULNA § 2(8).
[141] TEX. GOV'T CODE ANN. § 406.101(5).

3. Identify Proofing and Credential Analysis & Dynamic Knowledge-Based Authentication (KBA) Technology

"***Identity proofing***" means a process or service by which a third person provides a notary public with a means to verify the identity of a remotely located individual by a review of personal information from public and private data sources. RULNA § 14A(a)(3).

There is no definition for "***Credential analysis***" under RULNA. In Texas, "***Credential analysis***" means a process or service operating according to criteria approved by the secretary of state through which a third person affirms the validity of a government-issued identification credential through review of public and proprietary data sources. TEX. GOV'T CODE ANN. § 406.101(1)

There is no definition for "***Dynamic Knowledge-Based Authentication (KBA) Technology***" in RULNA or any express obligation to use it. "***Dynamic Knowledge-Based Authentication (KBA) Technology***" is "a process in which the principal is asked a series of questions about the principal's identity and personal history. In order to pass, the principal must answer at least 80% of the questions correctly. If the principal fails their first attempt, they may retake the quiz once within 24 hours. If the principal fails a second attempt they are prohibited from retrying with the same notary for at least 24 hours." Identity Proofing and Credential Analysis, Texas Secretary of State, https://www.sos.state.tx.us/statdoc/identityproofing.shtml (last visited 5.26.2022).

4. Other Definitions

NASS provides a brief summation of common e-notary terms, which can be found here as part of the *NASS eNotarization Implementation Guide* ("*iGuide*") (adopted February 18, 2017), which can be found online here: https://www.nass.org/sites/default/files/surveys/2017-08/NASS-NPA-iGuide-v1.0-0217.pdf .

D. Other Electronic-Notary Resources

1. NASS and individual Secretary of State Offices

As previously mentioned, NASS has numerous resources regarding eNotarization which may provide you with useful insights. Additionally, your state's Secretary of State (or equivalent) office, which commonly holds regulatory authority over notaries in your state, likely has resources with specific authorities applicable to your practice.

2. Third-Party Online Notary Vendors

In addition, there are numerous third-party vendors that can provide online-notary services for a fee. However, many of these vendors, and their prices, are focused on high-volume clientele – such as title companies, banks, and other high-volume users. So, you may need to shop around before you find a provider with reasonable and useful pricing and services for your practice.

E. Practice Tip

If this all seems overwhelming to you, don't worry. Any vendor worth their salt should be able to verify that their service meets each of these requirements. You should request confirmation from your e-Notary vendor, in writing, of each of the requirements above or as provided in your state's laws and regulations or resources provided by your Secretary of State (or equivalent authority).

VI. ELECTRONIC RECORDING

A. Background

So, now you have an electronic document, with an electronic signature, which is electronically notarized. All these technological advances can be useful, but if a court, clerk, or other authority will not recognize them, what good are they? Zero. We are back to zero.

This is a challenge practitioners must face on a daily basis. To this day, you will find many courts, clerks, or other authorities refusing electronic documents, signatures, or other "new-fangled" filings or recordings. However, there is statutory authority supporting the authenticity and enforceability of electronic documents, signatures, and transactions.

In addition to the UETA, ESIGN, and RULNA there is a uniform law regarding electronic recordings – as in recording documents in the county records, not Taylor Swift re-recording her hit albums. ***The Uniform Real Property Electronic Recordings Act*** or "***URPERA***" ("***URPERA***" or "***Recording Act***") provides a baseline template for states to consider when implementing e-recording capabilities.

Currently, 38 states, as well as the U.S. Virgin Islands and District of Columbia, have enacted some version of URPERA.[142] Massachusetts has introduced a bill substantially adopting URPERA.[143]

The following definitions apply under URPERA:

(1) "***Document***" means information that is:
  (A) inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form; and
  (B) eligible to be recorded in the real property records maintained by the [recorder].
(2) "***Electronic***" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
(3) "***Electronic document***" means a document that is received by the [recorder] in an electronic form.
(4) "***Electronic signature***" means an electronic sound, symbol, or process attached to or logically associated with a document and executed or adopted by a person with the intent to sign the document.
(5) "***Paper document***" means a document that is received by the [recorder] in a form that is not electronic.[144]

B. General Requirements

The Recording Act provides that a recorder **may** conduct the following actions:

(1) receive, index, store, archive, and transmit electronic documents;
(2) provide for access to, and for search and retrieval of, documents and information by electronic means;
(3) convert paper documents accepted for recording into electronic form;
(4) convert into electronic form information recorded before the [recorder] began to record electronic documents;
(5) accept electronically any fee [or tax] that the [recorder] is authorized to collect; and
(6) agree with other officials of a state, a political subdivision thereof, or the United States on procedures or processes to facilitate the electronic satisfaction of prior approvals and conditions precedent to recording and the electronic payment of fees [and taxes].[145]

---

[142] *Real Property Electronic Recording Act*, UNIF. LAW COMM'N https://www.uniformlaws.org/committees/community-home?communitykey=643c99ad-6abf-4046-9da4-0a6367da00cc (last visited April 18, 2026).

[143] *Id.*; An Act relative to uniform real property electronic recordings, H. 1602, 194th Sess. (Mass. 2026), https://malegislature.gov/Bills/194/H1602/BillHistory (latest action: "Accompanied a study order, see H5281 (under House Rule 27)" as of March 26, 2026).

[144] URPERA §§ 2(1)-(4), 4(a).

[145] URPERA § 4(b)(2)-(3),(5)-(8).

However, recorders **must** (1) conduct these actions pursuant to rules and standards established by the applicable commission or agency having authority over the recorder in the applicable state.[146] For example, in Texas, the *Texas State Library and Archives Commission* sets recording standards.[147]

Additionally, the recorder **must** (1) continue acceptance of paper documents and (2) record electronic and paper documents into the same index.[148]

The Recording Act provides that if a law requires an "original" document to "be on paper or another tangible medium, or be in writing" for recording purposes, that an electronic document meets those requirements, so long as it meets the other requirements of the Act.[149] This may seem a bit counter-intuitive since a digital document is not "on paper" or generally "tangible."

Additionally, the Recording Act provides that if a law requires a document to be signed for recording purposes, an electronic signature satisfies the signature requirement – essentially incorporating or, at least, supporting the purposes of UETA and ESIGN.[150]

Finally, the Recording Act provides that if a law requires a document to be notarized, acknowledged, verified, witnessed, or made under oath for recording purposes, an electronic signature of the notary or witness, etc. satisfies the requirement. However, the electronic document or signature must also contain all of the other information required, such as a date, etc., to be "attached to or logically associated with the document or signature."[151] No stamp, impression, or seal is necessary for the electronic signature.[152]

The Recording Act supersedes ESIGN (15 U.S.C. Section 7001 *et seq*.), with the exception of (1) Section 101(c) (15 U.S.C. Section 7001(c)) and (2) notices described in Section 103(b) (15 U.S.C. Section 7003(b)).[153]

C. Practice Tip

Notice that implementation of electronic recording is **optional** for recorders. URPERA § 4(b). So, if you have documents that you ultimately intend to record, before you have a client execute electronic versions, you should investigate whether the recorder in each applicable jurisdiction will accept electronic recordings. Additionally, if a recorder's office has not implemented electronic recording, you likely **cannot force the issue** – at this time or under the current statutory language.

You will also need a vendor or program to provide you with electronic-recording capabilities. There are multiple vendors with varying prices. However, you generally will be charged a fee per recording in addition to the recording fees assessed by the recorder.

Finally, as previously discussed, an electronic notary is required to have and apply an electronic seal. Therefore, regardless of URPERA § 3(c), it is likely best practice to ensure that a seal **is included** with the notary block.

VII. ARTIFICIAL INTELLIGENCE

A. Background

Use of artificial intelligence in the practice of law is in an on-going stage of fluctuation. So, my goal is to provide you with, at least, some food-for-thought in how A.I. could be implemented into your practice, or if it should be implemented at all.

A.I. is not a new technology, but it has recently hit its large-scale, mass-adoption stride. However, it still has many "kinks" to be resolved. Specifically, from a legal perspective, A.I. generators or engines do

---

[146] URPERA § 4(b)(1).
[147] *See* TEX. LOC. GOV'T CODE ANN. § 191.009 (Electronic Filing and Recording); TEX. LOC. GOV'T CODE ANN. CHAPTER 195 (Electronic Filing of Records with and Recording by County Clerks); and 13 TEX. ADMIN. CODE §§ 7.141-145 (Electronic Filing and Recording).
[148] URPERA § 4(b)(4).
[149] URPERA § 3(a).
[150] URPERA § 3(b).
[151] URPERA § 3(c).
[152] *Id*.
[153] URPERA § 7.

not have a perfect record of informational accuracy or reliability. So, let's review some A.I. Wins and Losses.

A.I. can have many definitions, but the American Bar Association utilizes the following definition:

> [I]ntelligence displayed by machines such as when a machine mimics human cognitive functions like reasoning, learning, or natural language processing.[154]

Although news coverage of the prolific spread of A.I. seems to be endless and ubiquitous, A.I. adoption in the law has progressed at a slow pace, although it does still progress. Brace for statistical stimulus.

Law firms utilizing A.I. tools crossed the 30% threshold in 2024 (30.2%).[155] Firms with the highest adoption employ 500 or more lawyers (47.8% A.I. adoption). Adoption decreases for firms with 10-49 lawyers (29.5%), and the lowest adoption rates are held by firms with 2-9 attorneys (24.1%) and solo practitioners (17.7%).[156]

The most-common A.I. tools for these groups were as follows: ChatGPT® (52.1%), Thomson Reuters® CoCounsel® (26.0%), and Lexis+ AI® (24.3%).[157]

Tools utilized by small firms (less than 50 lawyers), but not larger firms were as follows: Westlaw® AI, Microsoft Copilot®, Summize™, DocDraft™, and Alexi™. [158]

Tools utilized by large firms (50 or more lawyers), but not by small firms were as follows: Paxton AI™, Henchman™, Blue J Legal®, and Robin AI®.[159]

Benefits of A.I. Adoption	***Percentage of Respondents***
Saving time/increasing efficiency	54.4%
Document management/document review	9.1%
Reducing costs	4.5%
Not enough information to answer the question	17.4%

[160]

Concerns about A.I. Adoption	***Percentage of Respondents***
Accuracy	74.7%
Reliability	56.3%
data privacy and security	47.2%
costs of implementation	22.1%,
amount of time required to learn	21.3%

[161]

Role playing Nostradamus, attorneys' predictions of the adoption of A.I. are as consistent as your favorite college football's team's championship record – ranging from precarious to nonexistent.

---

[154] Mark Calaguas, *2024 Artificial Intelligence Tech Report*, American Bar Association (April 25, 2025), https://www.americanbar.org/groups/law_practice/resources/tech-report/2024/2024-artificial-intelligence-techreport/.

[155] *Id*.

[156] *Id*.

[157] *Id*.

[158] *Id*.

[159] *Id*.

[160] *Id*.

[161] *Id*.

A.I. Adoption Prediction	*Percentage of Respondents*
Already "mainstream"	12.8%
"watershed moment" within 3 years	45.3%
"mainstream" within 4 to 5 years	16.3%
"mainstream" within 6 to 10 years	6.4%

[162]

B. A.I. Terminology

Below are only a few of terms applicable to the A.I. industry.

Artificial Intelligence – Generally

Artificial Intelligence

> Artificial Intelligence (AI) is a term coined in 1955 by John McCarthy, Stanford's first faculty member in AI, who described it as "the science and engineering of making intelligent machines." Today it is a broad term for computer systems that can perform tasks with human-like intelligence, such as understanding language, recognizing images, learning from data, reasoning, and making decisions. Modern AI often works by finding patterns in large amounts of data and using those patterns to generate predictions or responses. It can be narrow (good at a specific task) or more general-purpose, like today's large language models that can handle many tasks.[163]

Artificial General Intelligence:

> [M]eans an AI system with general, human-level (or beyond) ability to learn, reason, and apply knowledge across a wide range of tasks and domains. AGI systems conceivably could handle novel situations, not just perform well on a single, narrow task. The term is controversial in several ways, including that different people mean different things by "human-level intelligence," and there's no universally accepted test, so claims are hard to verify. There are also safety and ethical concerns debated by AI experts.[164]

Types of Artificial Intelligence

Agentic AI – Agentics or Agents

> Agentic AI refers to AI systems designed to act as autonomous or semi-autonomous agents: they can set or interpret goals, plan and sequence actions, use tools (like web browsers, code, or APIs), make decisions based on feedback, and adapt over time to complete tasks. Unlike a purely reactive chatbot that only responds turn-by-turn, agentic AI is oriented around ongoing task execution—breaking down objectives, coordinating steps, and sometimes operating with minimal human oversight within defined constraints.[165]

---

[162] *Id*.

[163] *What is Artificial Intelligence (AI)?,* STANFORD UNIVERSITY HUMAN-CENTERED ARTIFICIAL INTELLIGENCE, (https://hai.stanford.edu/ai-definitions/what-is-artificial-intelligence-ai) (last visited May 2, 2026).

[164] *What is AGI (Artificial General Intelligence)?,* STANFORD UNIVERSITY HUMAN-CENTERED ARTIFICIAL INTELLIGENCE, (https://hai.stanford.edu/ai-definitions/what-is-agi-artificial-general-intelligence) (last visited May 2, 2026).

[165] *What is Agentic AI?,* STANFORD UNIVERSITY HUMAN-CENTERED ARTIFICIAL INTELLIGENCE, (https://hai.stanford.edu/ai-definitions/what-is-agentic-ai) (last visited May 2, 2026).

Generative AI

Generative AI (or GenAI) refers to AI systems that can create new content like text, images, music, code, or video. These systems learn patterns from training data and generate novel outputs that resemble the original data, often powered by architectures like GANs, transformers, diffusion models, and variational autoencoders. These models power applications including chatbots, code generation, and creative tools. They also raise questions about the potential for misuse including creating misinformation and deepfakes.[166]

Large Language Model (LLM)

A Large Language Model is an AI system trained on massive amounts of text data to understand and generate human-like language. It uses deep learning techniques, specifically neural networks with billions of parameters, to predict and produce coherent text, answer questions, translate languages, write code, and perform various other language-based tasks.[167]

Artificial Intelligence - Processes, Procedures, and Pitfalls

Hallucination

Hallucinations in AI refers to instances where an artificial intelligence system generates information or responses that are incorrect, misleading, or entirely fabricated but presented as factual. This often happens in language models or image generation when the AI produces outputs not supported by the training data or real-world facts.[168]

Inference

In artificial intelligence, Inference is when a trained AI model makes predictions or decisions on new data it hasn't seen before. More specifically, it is the step where the model takes what it knows and gives you answers, suggestions or results in real-world situations.[169]

Synthetic Data

Synthetic Data is artificially generated information created by algorithms or simulations rather than collected from real-world events or observations. It's used to train AI models when real data is scarce, expensive, privacy-sensitive, or difficult to obtain, while mimicking the statistical properties and patterns of authentic data. Synthetic data is particularly valuable for addressing data gaps, testing edge cases, and protecting privacy in fields like healthcare, autonomous driving, and financial modeling. Critics say that Synthetic Data may introduce biases, fail to capture real-world complexity and edge cases, or create "model

---

[166] *What is Generative AI?,* STANFORD UNIVERSITY HUMAN-CENTERED ARTIFICIAL INTELLIGENCE, (https://hai.stanford.edu/ai-definitions/what-is-generative-ai) (last visited May 2, 2026).

[167] *What is a Large Language Model (LLM)?,* STANFORD UNIVERSITY HUMAN-CENTERED ARTIFICIAL INTELLIGENCE, (https://hai.stanford.edu/ai-definitions/what-is-a-llm) (last visited May 2, 2026).

[168] *What are Hallucinations (in AI)?,* STANFORD UNIVERSITY HUMAN-CENTERED ARTIFICIAL INTELLIGENCE, (https://hai.stanford.edu/ai-definitions/what-are-hallucinations) (last visited May 2, 2026).

[169] *What is Inference?,* STANFORD UNIVERSITY HUMAN-CENTERED ARTIFICIAL INTELLIGENCE, (https://hai.stanford.edu/ai-definitions/what-is-inference) (last visited May 2, 2026).

> collapse" when AI systems are trained predominantly on AI-generated content.[170]

Training Data

> Training Data is the collection of examples—such as text, images, audio, or other information—used to teach machine learning models how to perform specific tasks. The model learns by analyzing patterns, relationships, and features within this data, adjusting its internal parameters to make accurate predictions or decisions. The quality, quantity, and diversity of training data largely determine how well an AI system will perform, making it one of the most critical components of machine learning.[171]

C. A.I. Wins

A.I. has had plenty of success, including passing the Uniform Bar Exam ("***UBE***"). The A.I. generator out performed humans in five of seven subject areas of the Exam, scored an average of 4.2/6.0 on the Multistate Essay Exam ("***MEE***") and Multistate Performance Test ("***MPT***") portions of the UBE, and scored approximately 297/400 points – satisfying passage thresholds for all UBE jurisdictions.[172]

The A.I. generator not only exceeded the average score of the human test takers, but landed near the 90th percentile of test takers for both the multiple-choice Multistate Bar Exam ("***MBE***") and MEE sections.

> As demonstrated by the zero-shot performance results we report herein, GPT-4 can "pass the Bar" in all UBE jurisdictions.
> …
> As the demand for better, faster, and more affordable legal services is only increasing in society, the need for supporting technology is becoming more acute. Further research on translating the capabilities of LLMs like GPT-4 into real public and private applications will be critical for safe and efficient use. GPT-4, like prior models, may still hallucinate sources, incorrectly interpret facts, or fail to follow ethical requirements; for the foreseeable future, application should feature "human-in-the-loop" workflows or similar safeguards. However, it appears that the long-awaited legal force multiplier is finally here.[173]

D. A.I. Losses

Despite these advancements, A.I. has gained a reputation for "***hallucinating***" sources and results. Although it is a bit of an oversimplification, this means that the generator essentially invents the information – makes it up, lies, [insert synonym of your choice here].

1. Let the Lawsuits Begin

The first private action against the creator of an A.I. generator regarding this "hallucination" effect was filed on June 5, 2023, in the Superior Court of Gwinnett County, Georgia, by Mark Walters against Open AI, L.L.C., the owner and operator of Chat GPT®.[174]

A journalist used ChatGPT® to investigate a federal lawsuit pending in the Western District of Washington. The journalist asked ChatGPT® to summarize the accusations in the complaint filed in that

---

[170] *What is Synthetic Data?,* STANFORD UNIVERSITY HUMAN-CENTERED ARTIFICIAL INTELLIGENCE, (https://hai.stanford.edu/ai-definitions/what-is-synthetic-data) (last visited May 2, 2026).

[171] *What is Training Data?,* STANFORD UNIVERSITY HUMAN-CENTERED ARTIFICIAL INTELLIGENCE, (https://hai.stanford.edu/ai-definitions/what-is-training-data) (last visited May 2, 2026).

[172] *GPT-4 Passes the Bar Exam*, KATZ, DANIEL MARTIN AND BOMMARITO, MICHAEL JAMES AND GAO, SHANG AND ARREDONDO, PABLO (March 15, 2023) (Available at SSRN: https://ssrn.com/abstract=4389233 or http://dx.doi.org/10.2139/ssrn.4389233)

[173] *Id*. (internal citations omitted).

[174] *Walters v. OpenAI LLC*, Ga. Super. Ct., 23-A-04860-2.

lawsuit, and ChatGPT® responded with the following:

> [I]s a legal complaint filed by [Plaintiff], the founder and executive vice president of [Company], against ***Mark Walters***, who is accused of defrauding and embezzling funds from the [Company]. The complaint alleges that Walters, who served as the organization's treasurer and chief financial officer, misappropriated funds for personal expenses without authorization or reimbursement, manipulated financial records and bank statements to conceal his activities, and failed to provide accurate and timely financial reports and disclosures to the [Company]'s leadership. The plaintiff seeks various forms of relief, including the recovery of misappropriated funds, damages for breach of fiduciary duty and fraud, and removal of Walters from his position as a member of the [Company] 's board of directors.

The issue – Walters is not a party to that lawsuit or in any way associated with that lawsuit. When asked to substantiate this information ChatGPT® "hallucinated" a false Complaint that was completely fabricated and did not match the actual Complaint on file in the lawsuit. Summary Judgment was ultimately granted in OpenAI®'s favor in May 2025.

One primary legal issue and defense in tort cases against technology or internet-based platforms and companies is Section 230 of the *Communications Decency Act*.[175] Among other provisions, Section 230 provides that an "interactive computer service(s)" is "not the publisher or speaker of information provided by another information content provider" and provides protection regarding the following:

> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[176]

This same defense is frequently relied upon by social-media and internet giants such as X™, Facebook™, Google®, and others regarding claims filed against them based upon the content posted on their platforms.

Section 230 came before the United States Supreme Court twice in the October 2022 Term, but both cases were decided under provisions of the *Antiterrorism Act (ATA)* and Section 230 was never substantively addressed in either opinion.[177]

2. A.I. In the Practice of Law - Early Lessons Learned – *Mata*, *Payne*, & *Whiting*

a. Mata v. Avianca, Inc.

For lawyers utilizing A.I. in practice, "hallucinated" results can be a perilous pitfall. The seminal case for the perils of "hallucinated" A.I. results in legal practice is the ***Avianca*** case from New York, which has become the red-alert warning for lawyers.

In *Mata v. Avianca, Inc.*, the Plaintiff filed suit alleging that his left knee was struck by a metal serving cart during a flight from El Salvador to John F. Kennedy Airport.[178]

After numerous other filings and removal of the case from state to federal court, counsel for the Plaintiff Mata filed an *Affirmation in Opposition to a Motion to Dismiss*, which had been filed by Defendant,

---

[175] *See* 47 U.S.C.A. § 230.
[176] 47 U.S.C.A. § 230(c)(2).
[177] *See Gonzalez v. Google LLC*, 598 U.S. 617, 143 S. Ct. 1191, 215 L. Ed. 2d 555 (2023), *Twitter, Inc. v. Taamneh*, 598 U.S. 471, 143 S. Ct. 1206, 1209, 215 L. Ed. 2d 444 (2023). *See also* 18 U.S.C. § 233 (Antiterrorism Act (ATA)).
[178] *Mata v. Avianca, Inc.*, No. 22-CV-1461 (PKC) (S.D.N.Y. Jun. 22, 2023), *Opinion and Order on Sanctions*.

Avianca, Inc., on March 1, 2023.[179] In said Affirmation, the following nine cases were cited:

1. Varghese v. China Southern Airlines Co., Ltd., 925 F.3d 1339 (11th Cir. 2019).
2. Shaboon v. Egyptair, 2013 IL App (1st) 111279-U (Ill. App. Ct. 2013).
3. Peterson v. Iran Air, 905 F. Supp. 2d 121 (D.D.C. 2012).
4. Martinez v. Delta Airlines, Inc., 2019 WL 4639462 (Tex. App. Sept. 25, 2019).
5. Estate of Durden v. KLM Royal Dutch Airlines, 2017 WL 2418825 (Ga. Ct. App. June 5, 2017).
6. Miller v. United Airlines, Inc., 174 F.3d 366, 371-72 (2d Cir. 1999)
7. Zicherman v. Korean Air Lines Co., Ltd., 516 F.3d 1237, 1254 (11th Cir. 2008).
8. Ehrlich v. American Airlines, Inc., 360 N.J. Super. 360 (App. Div. 2003).
9. In re Air Crash Disaster Near New Orleans, LA., 821 F.2d 1147, I 165 (5th Cir. 1987).[180]

Counsel for the Defendant raised concerns about the validity of the cited cases in a *Reply Memorandum in Support* of the *Motion to Dismiss* filed on March 15, 2023.[181]

On April 11, 2023, the Court ordered counsel for Plaintiff to "file an affidavit annexing copies" of eight of these cases.[182] The Court issued another order adding an additional case to the list on April 12, 2023.[183]

Counsel requested an extension of time in order to produce the annexed copies because he was "currently out of the office on vacation and will be returning April 18, 2023."[184] This was later determined to be false.[185]

On April 25, 2023, counsel annexed copies or excerpts of cases which were purported to be the cases required by the Court's Orders of April 11 and 12, with the exception of the *Zicherman* cases, which counsel stated he was unable to locate.[186]

On May 25, 2023, counsel for Plaintiff filed an *Affidavit in Opposition* to the *Motion to Dismiss* in which they began to "***dribble out the truth***" according to Judge Castel.[187]

Ultimately, it was discovered that the cases cited were either completely fabricated or were cited for a proposition which the case did not actually state or support.[188] Counsel had used an A.I. Generator in drafting the Affirmation and the cases had been provided by that generator.[189] The generator created the false cases, or at least false citations to non-existent cases, but named real judges as the authors.[190]

The "Varghese", "Miller", "Peterse[o]n", "Shaboon", "Martinez", and "Durden" cases do not exist. These fabricated cases were set apart by quotation marks, while the other cases – cited for propositions they did not support – did not include quotations in their citations.[191]

Additionally, it was discovered that the "opinions" and "decisions" annexed and provided to the Court on April 25, 2023, had a litany of issues and were themselves fabricated.[192]

The drafting attorney stated at the sanctions hearing on June 8, 2023, that he was "operating under the false perception that this website [i.e., ChatGPT[®]] could not possibly be fabricating cases on its own."[193] However, the Court wholly rejects the counsel's numerous attempts to claim ignorance of the authenticity

---

[179] *Id*.
[180] *Id*.
[181] *Id*.
[182] *Id*.
[183] *Id*.
[184] *Id*.
[185] *Id*.
[186] *Id*.
[187] *Id*.
[188] *Id*.
[189] *Id*.
[190] *Id*.
[191] *Id*.
[192] *Id*.
[193] *Id*.

issue of the A.I. results because of the numerous issues raised by opposing counsel and the Court itself along this saga.[194]

Counsel also attempted to argue that he followed-up with the A.I. generator and asked "[i]s Varghese a real case" and "[a]re the other cases you provided fake", along with other prompts.[195] The generator responded that the Varghese case "does indeed exist" and provided other reassurances of its results.[196]

> Technological advances are commonplace and there is nothing inherently improper about using a reliable artificial intelligence tool for assistance. But existing rules impose a gatekeeping role on attorneys to ensure the accuracy of their filings. Rule 11, Fed. R. Civ. P. [Attorneys and firm] abandoned their responsibilities when they submitted non-existent judicial opinions with fake quotes and citations created by the artificial intelligence tool ChatGPT[®], then continued to stand by the fake opinions after judicial orders called their existence into question.
>
> Many harms flow from the submission of fake opinions. The opposing party wastes time and money in exposing the deception. The Court's time is taken from other important endeavors. The client may be deprived of arguments based on authentic judicial precedents. There is potential harm to the reputation of judges and courts whose names are falsely invoked as authors of the bogus opinions and to the reputation of a party attributed with fictional conduct. It promotes cynicism about the legal profession and the American judicial system. And a future litigant may be tempted to defy a judicial ruling by disingenuously claiming doubt about its authenticity.[197]

The Court ordered sanctions against both of the individual lawyers representing the Plaintiff, as well as their firm as a whole.[198] Part of the sanctions issued by Judge Castel included an obligation to send letters to the judges falsely identified as the authors of the fake opinions.[199] It is important to note that Judge Castel did not make the ruling exclusively on the use of A.I., but considered the specific conduct of the lawyers.[200]

> The narrative leading to sanctions against Respondents includes the filing of the March 1, 2023 submission that first cited the fake cases. But if the matter had ended with Respondents coming clean about their actions shortly after they received the defendant's March 15 brief questioning the existence of the cases, or after they reviewed the Court's Orders of April 11 and 12 requiring production of the cases, the record now would look quite different. Instead, the individual Respondents doubled down and did not begin to dribble out the truth until May 25, after the Court issued an Order to Show Cause why one of the individual Respondents ought not be sanctioned.
>
> …
>
> At no time has any Respondent written to this Court seeking to withdraw the March 1 Affirmation in Opposition or advise the Court that it may no longer rely upon it.[201]

---

[194] *See id*.
[195] *Id*.
[196] *Id*.
[197] *Id*.
[198] *Id*.
[199] *Id*.
[200] *Id*.
[201] *Id*.

Ultimately, Judge Castel found the attorneys had acted with "subjective bad faith" and issued numerous sanctions under Rule 11 and Rule 3.3(a)(1) of the New York Rules of Professional Conduct, 22 N.Y.C.R.R. § 1200.0. The sanctions included the following:

1. A $5,000 fine;
2. A letter to the opposing party; and
3. Letters to be sent to the judges falsely identified as authors of the fake cases - "Varghese", "Shaboon", "Petersen", "Martinez", "Durden" and "Miller" opinions.[202]

The law firm voluntarily imposed mandatory CLE programming on technology competence and A.I. programs, as well as training on notarization practices.[203]

b. ***Payne v. State of Georgia***

In *Payne v. State of Georgia*, the trial court's *Order Deny Motion for New Trial* contained multiple "hallucinations" including fabricated cases and real cases cited for legal propositions which are not established or supported by such cases. [204] During oral arguments, the District Attorney stated to the Georgia Supreme Court that although she prepared the Order for the trial court, such hallucinations were not contained in her draft order, to which the Court responds that the same such citations were also included in the State's initial Brief to the trial court opposing the *Motion for New Trial*.[205]

c. ***Whiting v. City of Athens, Tennessee***

In *Whiting v. City of Athens, Tennessee*, the United States Court of Appeals for the Sixth Circuit upheld the district courts denial of a *Motion to Recuse* as well as a *Sanctions Order* against the Plaintiff/Appellant regarding the filing of "frivolous" lawsuits.[206] The history of the cases was nothing short of a cascade of barbs between the Court and the counsel for Appellants.[207] By separate Order, the Court addressed sanctions against Appellant's counsel.[208]

Upon appeal from the trial court and receipt of initial briefs, the Sixth Circuit Court consolidated multiple cases.[209] The Court found the brief submitted by one Appellant "misrepresented the nature of the district court's sanctions" and contained "over two dozen" citations to cases that either (1) did not exist, (2) did not support the legal proposition for which they were cited, or (3) did not include the quotations stated in the Appellant's brief and attributed to such cases.[210] The Court issued a *Show Cause Order* instructing the attorneys to take the following actions:

> (1) explain why they should not be sanctioned for citing fake cases,
> (2) provide a copy from Westlaw® or LexisNexis® of all the cases and authorities cited in all of the briefs filed across the three appeals,
> (3) highlight any material that they quoted from those cases,
> (4) tell us who wrote the briefs in each case,
> (5) tell us whether the briefs were ghostwritten in whole or in part,
> (6) tell us whether they used generative AI to write the briefs, and

---

[202] *Id*.
[203] *Id*.
[204] *S26A0459 Payne v. State of Georgia Oral Arguments* at 32:45, SUPREME COURT OF GEORGIA, (https://www.gasupreme.us/oral-arguments-march-18-2026/).
[205] *Id*.
[206] *Whiting v. City of Athens, Tennessee*, 170 F.4th 439, 445, 454 (6th Cir. 2026).
[207] *See id.* at 445-446 n.4.
[208] *Id*. at 442 n.1.; *Whiting v. City of Athens Tennessee*, 170 F.4th 455 (6th Cir. 2026).
[209] *Whiting v. City of Athens Tennessee*, 170 F.4th 455, 458 (6th Cir. 2026).
[210] *Id*.

(7) explain how they cite-checked the briefs.[211]

In response, or lack thereof, the attorneys argued the *Show Cause Order* was "void on its face for failing to include a signature of an Article III judge," was "motivated by harassment of the Respondent attorneys," and "reflect[ed] illegal ex-parte [sic] communications within this Court."[212]

Ultimately the court issued the following sanctions

> 1. [Attorneys] must jointly and severally reimburse appellees in full for their reasonable attorneys' fees on appeal in all three appeals.
> 2. [Attorneys] must jointly and severally pay double costs to appellees for costs incurred under 28 U.S.C. § 1920 on appeal in all three appeals.
> 3. Appellees must file an accounting of their costs and attorneys' fees on appeal, with supporting documentation, no later than seven days from the date of this order. [Attorneys] shall file any responses or objections to appellees' requests for costs and attorneys' fees on appeal no later than seven days thereafter. There will be no replies.
> 4. [Attorneys] must each separately and individually pay $15,000 to the registry of this court as punitive sanctions for the proceedings in this court in all three appeals.
> 5. The clerk will forward a copy of this order to the chief judge to consider disciplinary proceedings under Sixth Circuit Local Rule 46.
> 6. If [Attorneys] are financially unable to comply with some or all of the requirements of this order, they must file an affidavit under seal describing their financial situation along with their objections to appellees' fee requests.[213]

The Court was less than pleased to say the least, and showed its frustration not only in its ruling, but also in its footnotes and Appendix.

> This is a conservative estimate. We call something a "fake citation" or "misrepresentation of fact" only when it is clearly so. We do not include typos or sloppy citations. "As those mistakes could be attributed to simple sloppiness in drafting, as opposed to a failure to comply with the basic obligations of legal counsel, they are not the subject of this" opinion. Davis v. Marion Cnty. Super. Ct. Juv. Detention Ctr., No. 1:24-CV-01918-JRS-MJD, 2025
> WL 2502308, at *1 n.1 (S.D. Ind. Sept. 2, 2025). If we included typos and other errors that are arguably, but not clearly, a misrepresentation or fake citation, we would be looking at far more misstatements of fact and law.[214]

The Court attempted to restrain their ire by only sanctioning the attorneys and not the Appellant himself and by foregoing a finding of contempt:

> [W]e choose not to sanction Whiting himself because we have no evidence that Whiting participated in the misconduct […] Finally, we could have held Irion and Egli in contempt because they flagrantly ignored our order to show cause.[]

---

[211] *Id*. at 459.
[212] *Id*.
[213] *Id*. at 466-67.
[214] *Id*. at 458 n.1.

> But we do not think additional sanctions are necessary to send the message we send here."[215]

However, it is not difficult to conclude that the Court wished for the ability to impose a more severe punishment:

> We could have gone much further. Other courts have dismissed cases, disqualified lawyers, or revoked their pro hac vice status for similar conduct.[] But only the chief judge can suspend or disbar a lawyer from practice before this court, see 6th Cir. Local Rule 46(c)(4)(C), so those sanctions are not available to us[.][216]

E. Court Orders & Rules

Multiple courts have imposed standing or local rules regarding the use of A.I. in their courts. Most of these rules involve some kind of signed statement by counsel, imposed under the "Duty of Candor" and proper pleadings, that they either (1) did not use A.I. technology in drafting the filing or (2) that if A.I. was used, the results were verified by a human. Conversely, some courts have specifically declined to impose A.I.-specific disclosures or procedures.[217]

> Some courts have issued standing orders or local rules prohibiting the use of generative AI to draft legal filings or at least requiring certain forms of disclosure; others have declined to issue any such rules at all. *Compare* N.D. Tex. LR 7.2(f) (disclosure rules for briefs prepared using generative artificial intelligence), *with* "Court Decision on Proposed Rule" (5th Cir. June 10, 2024) (declining to adopt special rule regarding the use of artificial intelligence in drafting briefs).[218]

Many of these rules are based – at least in part – on the "Duty of Candor" imposed by applicable ethic rules, such as ABA Model Rule 3.3:

> **Rule 3.3: Candor Toward the Tribunal**
> Advocate
> (a) A lawyer shall not knowingly:
>
> (1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;
>
> (2) fail to disclose to the tribunal legal authority in the controlling jurisdiction known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or

---

[215] *Id*. at 467 n.5.
[216] *Id*.
[217] *See* TEX. COMM. ON PROFESSIONAL ETHICS, Op. 705 (2025) (https://www.legalethicstexas.com/resources/opinions/opinion-705/) ("*Compare* N.D. Tex. LR 7.2(f) (disclosure rules for briefs prepared using generative artificial intelligence), *with* "Court Decision on Proposed Rule" (5th Cir. June 10, 2024) (declining to adopt special rule regarding the use of artificial intelligence in drafting briefs)").
[218] TEX. COMM. ON PROFESSIONAL ETHICS, Op. 705 (2025) (https://www.legalethicstexas.com/resources/opinions/opinion-705/).

> (3) offer evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.
>
> (b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.
>
> (c) The duties stated in paragraphs (a) and (b) continue to the conclusion of the proceeding, and apply even if compliance requires disclosure of information otherwise protected by Rule 1.6.
>
> (d) In an ex parte proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer that will enable the tribunal to make an informed decision, whether or not the facts are adverse.[219]

F. A.I. Guidance & the Ethics of A.I. Use

1. The Model Rules

Where do A.I. use and ethics rules collide? Off-the-bat, we have already discussed the "Tech Competency" obligations imposed by the ethics rules of many jurisdictions as well as the "Duty of Candor".[220] In addition, the following ABA Model Rules of Professional Conduct are directly implicated in A.I. use:

> **Rule 1.1: Competence**
> Client-Lawyer Relationship
> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.[221]
>
> **Rule 1.6: Confidentiality of Information**
> Client-Lawyer Relationship
> (a) 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 or the disclosure is permitted by paragraph (b).
>
> (b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:
>
> (1) to prevent reasonably certain death or substantial bodily harm;
>
> (2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of

[219] MODEL RULES OF PROF'L CONDUCT r. 3.3.
[220] *See* MODEL RULES OF PROF'L CONDUCT r. 3.3.
[221] MODEL RULES OF PROF'L CONDUCT r. 1.1.

another and in furtherance of which the client has used or is using the lawyer's services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(4) to secure legal advice about the lawyer's compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;

(6) to comply with other law or a court order; or

(7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.[222]

Rule 5.1: Responsibilities of Partners, Managers, and Supervisory Lawyers

Law Firms And Associations

(a) A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

(b) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.

(c) A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if:

(1) the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its

[222] MODEL RULES OF PROF'L CONDUCT r. 1.6.

> consequences can be avoided or mitigated but fails to take reasonable remedial action.[223]

For example, the United States District Court Northern District of Texas has issued the following Local Rule:

> LR 7.2 Briefs [New Rule]
> * * *
> (f) Disclosure of Use of Generative Artificial Intelligence.
> (1) A brief prepared using generative artificial intelligence must disclose this fact on the first page under the heading "***Use of Generative Artificial Intelligence***." If the presiding judge so directs, the party filing the brief must disclose the specific parts prepared using generative artificial intelligence.
> (2) "***Generative Artificial Intelligence"*** means a computer tool (whether referred to as "*Generative Artificial Intelligence*" or by another name) that is capable of generating new content (such as images and text) in response to a submitted prompt (such as a query) by learning from a large reference database of examples.
> (3) A party who files a brief that does not contain the disclosure required by subsection (f)(l) of this rule certifies that no part of the brief was prepared using generative artificial intelligence.[224]

Westlaw®, and likely numerous other platforms, has launched a search engine and database specific to orders and rules on A.I. use.[225] Currently the platform shows orders and rules from 28 states comprised of 186 state orders and 8 federal orders.[226]

2. Guidance? Maybe?

Many State Bar organizations across the country have attempted to tackle the "ethical-use of A.I." debate and to provide guidance to their members. One such effort was conducted by the State Bar of Texas "*Taskforce for Responsible AI in the Law (TRAIL).*"[227] The 2023-2024 Taskforce made several recommendations to the State Bar of Texas in its final report including the following: mandatory training for newly-licensed lawyers, continuing legal education on A.I. for current lawyers, negotiation by the State Bar of Texas with technology vendors regarding A.I. services and tools, publication of guidance regarding A.I. use for pro-se litigants, as well as recommendations for the judiciary and paralegals. The report also requested an ethics opinion to be issued by the Texas Professional Ethics Committee, to which the Committee complied by publishing Opinion 705.[228]

---

[223] MODEL RULES OF PROF'L CONDUCT r. 5.1.
[224] N.D. Tex. LR 7.2(f).
[225] *Thomson Reuters Westlaw Statutes & Court Rules: AI Court Rules*, THOMSON REUTERS (https://auth.thomsonreuters.com/u/login/identifier?state=hKFo2SBhenloRVNQeTRkT28zbVhGVDFyZGsxampwS1RteUt1OaFur3VuaXZlcnNhbC1sb2dpbqN0aWTZIFhIcUdPRFczRHhtaEpnSHliNm93TW9sOE5jdGQ2MWNBo2NpZNkgVDRLN0txa09Gb0NXNG4yenliekU4QVlYQkRCYVhPUmk&ui_locales=en).
[226] *Id*. (as of April 25, 2026).
[227] *See Taskforce for Responsible AI in the Law: 2023-2024 Year-End Report*, STATE BAR OF TEXAS (https://www.texasbarpractice.com/wp-content/uploads/2025/04/TRAIL-2023-24-Year-End-Report.pdf).
[228] *Id.*; TEX. COMM. ON PROFESSIONAL ETHICS, Op. 705 (2025) (https://www.legalethicstexas.com/resources/opinions/opinion-705/).

The 2024-2025 Taskforce then released an "AI Toolkit" for Texas lawyers (or really anyone with an internet connection) to utilize in implementing A.I. in legal practice.[229]

3. An Ethics Opinion Appetizer – the "*Texas Sampler*"

The Texas Professional Ethics Committee published Ethics Opinion 705, which posed the apex question:

> *What ethical issues are raised under the Texas Disciplinary Rules of Professional Conduct by a lawyer's use of generative artificial intelligence in the practice of law?*[230]

The Opinion cited numerous prior opinions as well as drawing upon guidance issued by other Bar associations, including those of the District of Columbia, Florida, and California. Unsurprisingly, the Opinion focused on the following ethical duties: (1) *Competence*, (2) *Confidentiality*, and (3) *Oversight*/*Supervision*.[231] However, somewhat surprisingly, the Opinion also addressed *Fees*.[232]

Some notable findings from the Opinion included the following:

1. *Competence*: Use isn't mandatory. However, if utilized, *proper* use is mandatory:

The Committee noted that "competence" under Rule 1.01(a) of the Texas Disciplinary Rules of Professional Conduct includes the obligation of "technological competence" (a/k/a "tech competency" as we have already discussed") as well as the preservation of client confidential information (essentially tying "competency" to the confidentiality ethical duty). [233]

> Rule 1.01 almost certainly does not *require* the use of generative AI for any particular purpose in the practice of law, especially at the present moment where the technology is still developing and the cost-benefit analysis remains somewhat unclear. Still, lawyers should not "unnecessarily retreat[] from the use of new technology that may save significant time and money for clients." Opinion 680; *see also* comment 8 to Rule 1.01. What's clear even now is that *if* a lawyer opts to use a generative AI tool in the practice of law, the lawyer must have a reasonable and current understanding of the technology—because only then can the lawyer evaluate the associated risks of hallucinations or inaccurate answers, the limitations that may be imposed by the model's use of incomplete or inaccurate data, and the potential for exposing client confidential information. *Cf.* Opinion 680 (lawyer should acquire a general understanding of how cloud computing works before using in practice of law); Opinion 665 (similar for metadata).[234]

2. *Confidentiality*: Client consent before use? Maybe:

---

[229] *AI Tookit*, State Bar of Texas (https://www.texasbarpractice.com/artificial-intelligence-toolkit/). *See also* Lowell Brown, *State Bar Board Update: State Bar of Texas Unveils AI Tookit, Texas Bar Journal*, September 2025 (https://lsc-pagepro.mydigitalpublication.com/article/STATE+BAR+BOARD+UPDATE/5026719/850944/article.html).

[230] TEX. COMM. ON PROFESSIONAL ETHICS, Op. 705 (2025) (https://www.legalethicstexas.com/resources/opinions/opinion-705/) .

[231] *Id*.

[232] *Id*.

[233] *Id* (citing TEX. COMM. ON PROFESSIONAL ETHICS, Op. 680 (2018) (addressing cloud-computing systems); TEX. COMM. ON PROFESSIONAL ETHICS, Op. 665 (2016) (addressing metadata in electronic documents).

[234] *Id*.

Regarding confidentiality specifically, the Committee notes that the "unthinking use" of A.I. in relation to client information is one the "greatest risks."[235] Texas Disciplinary Rules of Professional Conduct Rule 1.05 prohibits "knowingly" disclosing client information – whether privileged or otherwise – other than to permitted persons.

The compounding complexity of confidentiality and A.I. is that a practitioner must have a baseline understanding of how a particular A.I. tool works in order to assess whether their duty of confidentiality is implicated.[236]

I believe it is helpful to categorize A.I. use in practice into three categories: (1) research, (2) drafting or deliverables, or (3) brainstorming.

(a) Research

It is possible to use A.I. tools for "general research purposes" without revealing client confidential information, and in fact you likely will have little choice in the matter in the near future.[237] Many research databases have A.I. tools and systems which likely will become standard – or at least industry standard – in the future, such as LexisNexis® tools and Westlaw®'s CoCounsel® and AI Deep Research™. Eventually, you may have no choice but to allow A.I. into your research tasks.

In most instances, much like your current legal research, these searches can avoid the use of client information – other than your entry of a "client" in the tracking portion of those systems for billing purposes. However, you must of course check any results your receive. Many of these systems will contain disclaimers to that effect, including Westlaw® which states as follows:

> Westlaw AI Deep Research uses large language models - a type of agentic AI - and focuses the models on the language of cases, statutes, regulations, administrative law decisions, Practical Law content, select secondary sources and current awareness content to improve accuracy.
>
> All cited sources are referenced in the response with the actual language from the source and links to read the full document. Even with these and other precautions, Westlaw AI Deep Research can occasionally produce inaccuracies, so it should always be used as part of the research process, with additional research to fully understand the nuance of the issues and further improve accuracy.
>
> The AI-generated response can be extraordinarily useful for getting an overview of the issues and citations to authority, but it should ***never*** be used to advise a client, write a brief or motion for a court, or otherwise be relied on without doing further research.
>
> Use it to accelerate thorough research. Don't use it as a replacement for thorough research.[238]

(b) Drafting or Deliverables, but Oregonians beware (*Willams v. Honl*)

---

[235] *Id*.
[236] *See id*.
[237] *See id*.
[238] *Thomson Reuters Westlaw Advantage Westlaw AI Deep Research: how Westlaw AI Deep Research works*, THOMSON REUTERS (https://auth.thomsonreuters.com/u/login/identifier?state=hKFo2SBhenloRVNQeTRkT28zbVhGVDFyZGsxampwS1RteUt1OaFur3VuaXZlcnNhbC1sb2dpbqN0aWTZIFhIcUdPRFczRHhtaEpnSHliNm93TW9sOE5jdGQ2MWNBo2NpZNkgVDRLN0txa09Gb0NXNG4yenliekU4QVlYQkRCYVhPUmk&ui_locales=en).

From a bare-basics perspective, all A.I. tools require the user to input a prompt or request containing some level of relevant facts, information, and circumstances in order for the tool to generate the response or output sought.[239] That level of detail is heightened when you are requesting the A.I. tool generate a draft, document, or other deliverable. Many such requests could be anonymous or contain agnostic information, but many – such as a demand letter or settlement agreement (both examples used by the Committee) – will require a greater level of detail.[240]

For example, due to my math-skills deficiency, I requested Microsoft Copilot® to generate an amortization schedule with the following prompt:

> Can you create an Excel[®] amortization schedule using the following parameters?
> 1. Initial Principal of $1,527,973.20;
> 2. Interest of 4.57% annual percentage rate;
> 3. Ten-year (10 year) term;
> 4. Payments begin June 15th and continue monthly; and
> 5. Annual interest payments of accrued interest due and payable on or before each December 31?

The results? The program did generate an Excel® meeting my request with only minor deviations. Overall, it was what I needed. Note that none of the information provided would be considered "confidential."

However, conversely, consider if I had asked the tool to generate the Promissory Note, Security Agreement, or other documents for the transaction. In theory, I could either omit certain information about my client or use fictional information and manually edit the documents produced by the A.I. – which I should do regardless of the results. However, I must be cognizant of the information I am injecting into the A.I. system when making such a request.

Note, while many courts and jurisdictions permit A.I. drafting – subject to attorney review and disclosure under local rules as discussed above – at least one court has taken the position that ***any*** drafting by A.I. is not "competent practice of law."[241]

> Finally, so that the clear does not become cloudy, we state the obvious: Using generative artificial intelligence to generate legal briefs and then simply cite-checking them bears no resemblance to the competent practice of law. *See Mattox*, 807 F Supp 3d at 1353 ("When lawyers trade reflection for automation, they surrender the very quality that makes their words worthy of belief."). Although cite checking is, of course, an important part of producing reliable, competent briefs, it is not the type of work that requires a law degree. Law is a profession:
>
> > "a calling requiring specialized knowledge and often long and intensive preparation including instruction in skills and methods as well as in the scientific, historical, or scholarly principles underlying such skills and methods, maintaining by force of organization or concerted opinion high standards of achievement and conduct, and committing its members to continued study and

---

[239] *See* TEX. COMM. ON PROFESSIONAL ETHICS, Op. 705 (2025) (https://www.legalethicstexas.com/resources/opinions/opinion-705/).
[240] *See id*.
[241] *Williams v. Honl*, 348 Or. App. 505, 513 (2026).

> to a kind of work which has for its prime purpose the rendering of a public service—see LEARNED PROFESSION."
>
> *Webster's Third New Int'l Dictionary* 1811 (unabridgeded.2002) (defining "profession"). As veteran Oregon lawyers have advised new lawyers for years, an Oregon lawyer develops and maintains the specialized knowledge required of the profession by reading the cases relevant to the lawyer's practice in the Advance Sheets (in print or on the appellate courts' website) and discussing them with colleagues. A person who uses generative artificial intelligence in lieu of reading, writing, and talking about the law—the very processes by which a lawyer acquires and [] retains the specialized knowledge and skills required of the profession—risks losing claim to the title of lawyer.[242]

(c) Brainstorming

Perhaps one of the most useful applications of A.I. following research is for brainstorming points and counterpoints to your arguments. However, much like the discussion on drafting and deliverables, great care should be taken in regard to what information your "prompt" and responses with A.I. includes.

(d) Committee Summary – Confidentiality

> If a lawyer intends to use confidential information in conjunction with generative AI tools, the lawyer should consider informing clients about the associated risks and may need to secure client consent. The State Bar of California Standing Committee on Professional Responsibility and Conduct has recommended that lawyers inform their clients if generative AI tools will be used as part of their representation. *See* State Bar of California, Standing Committee on Professional Responsibility and Conduct, *Practical Guidance for the Use of Generative Artificial Intelligence in the Practice of Law* (Nov. 16, 2023). Ethics opinions from the ABA and the Florida Bar go a step further and suggest that lawyers should obtain informed consent before using these tools. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 512 (2024) ("Generative Artificial Intelligence Tools"); Florida Bar Ethics Opinion 24-1 (2024). This Committee, in Opinion 680 concerning the risks of cloud-computing software, stated "[i]n some circumstances it may be appropriate to confer with a client regarding these risks as applicable to a particular matter and obtain a client's input regarding or consent to using" such new technology. At a minimum, Texas lawyers should engage in the same thoughtful analysis with respect to generative AI tools.[243]

3. *Oversight/Supervision*: The Buck Stops here:

> A lawyer's failure to verify generative AI outputs can implicate a host of Rules, including Rule 1.01 (Competent and Diligent Representation), Rule 3.01 (Meritorious Claims and Contentions), Rule 3.03 (Candor Toward the Tribunal), and Rule 3.04 (Fairness in Adjudicatory Proceedings), among others. The best practice here, as with many other efficiency-enhancing tools in the law: AI-generated outputs can be used as a starting point for a lawyer's work, but must always be carefully analyzed for accuracy and quality. That said, a lawyer's duties require more than merely detecting and eliminating false AI-

---

[242] *Williams v. Honl*, 348 Or. App. 505, 513–14 (2026).

[243] TEX. COMM. ON PROFESSIONAL ETHICS, Op. 705 (2025) (https://www.legalethicstexas.com/resources/opinions/opinion-705/).

> generated results—the lawyer is ultimately responsible for ensuring that the content is accurate and supports the client's interests.[244]

4. *Fees*: Actual ~~Damages~~ [Time and Expenses]

> It's not hard to imagine how the effective use of generative AI tools might impact the fees that lawyers charge—after all, one of the most promising aspects of these tools is the possibility for lawyers to provide legal services more efficiently. In most typical hourly arrangements (depending on the agreement), a lawyer will likely be able to charge the client for the actual time the lawyer spends using a generative AI program for purposes of the representation, including to refine the program's outputs and check the work. A lawyer may not, however, charge hourly fees for the time that was "saved" by using the generative AI program. As the District of Columbia Bar Association explained:
>
> > '[I]t goes without saying that a lawyer who has undertaken to bill on an hourly basis is never justified in charging a client for hours not actually expended. If a lawyer has agreed to charge the client on this basis (i.e., hourly), and it turns out that the lawyer is particularly efficient in accomplishing a given result, it nonetheless will not be permissible to charge the client for more hours than were actually expended on the matter. When that basis for billing the client has been agreed to, the economies associated with the result must inure to the benefit of the client.'[245]
>
> If the lawyer pays per use for a particular generative AI program, the lawyer may be able to collect those expenses from the client, as allowed by law and if the client accepts that arrangement. See Opinion 594. When a lawyer incurs per-use fees associated with a generative AI program, one could imagine a client agreeing to reimburse those expenses in much the same way some clients agree to pay for the use of traditional online research tools like Westlaw® and LexisNexis®. The lawyer will generally not be permitted to recover more than the amount of expenses actually incurred and paid to the generative AI provider.[246]

4. Whodunit? When the Client Uses A.I. – *U.S. v. Heppner*

Beyond a lawyer's use of A.I. within their practice, what happens when a client takes information, documents, or advice from a lawyer and inputs that information, document, or advice into a third-party A.I. tool? Well, at least one outcome is the potential loss of Attorney-client Privilege.[247]

In *United States v. Heppner*, the United States District Court for the Southern District of New York faced the following question of first impression:

> [W]hether, when a user communicates with a publicly available AI platform in connection with a pending criminal investigation, are the AI user's communications protected by attorney-client privilege or the work product doctrine?[248]

---

[244] *Id*.
[245] *Id*. (quoting D.C. Legal Ethics Opinion 388 (2024)).
[246] *Id*. (citations omitted).
[247] *United States v. Heppner*, No. 25 CR. 503 (JSR), 2026 WL 436479, at *2-3 (S.D.N.Y. Feb. 17, 2026).
[248] *Id.* at *1.

The answer?

> For the reasons that follow, the answer is no.[249]

In October 2025, Heppner, an executive for multiple corporate entities, was indicted for several fraud and conspiracy charges in relation to his alleged misconduct in defrauding investors "out of more than $150 million by making false representations about, and causing [the corporation] to enter into undisclosed self-serving transactions concerning, two privately held companies that Heppner controlled[.]"[250]

In November 2025, Heppner was arrested and plead guilty to the charges. The FBI seized documents and electronic devices from Heppner's home, including 31 documents containing communications between Heppner and Anthropic®'s Claude® A.I. platform.[251] These A.I. communications occurred after Heppner had received a grand jury subpoena and after "it was clear with discussions with the government that Mr. Heppner was the target of this investigation."[252]

> Without any suggestion from counsel that he do so, Heppner "prepared reports that outlined defense strategy, that outlined what he might argue with respect to the facts and the law that we anticipated that the government might be charging." []Thus, counsel asserted, Heppner "was preparing these reports in anticipation of a potential indictment."[][253]

Heppner and his counsel claimed privilege over the A.I. documents based on the following:

> (1) Heppner had input[] into Claude[®], among other things, information that Heppner had learned from counsel; (2) Heppner had created the AI Documents for the purpose of speaking with counsel to obtain legal advice; and (3) Heppner had subsequently shared the contents of the AI Documents with counsel.[254]

Heppner's counsel "did not direct" Heppner to utilize the A.I. tool.[255]

The Court began its analysis by reiterating that attorney-client privilege is narrowly construed and consists of three elements:

> It is well established that the attorney-client privilege attaches to, and protects from disclosure, "communications (1) between a client and his or her attorney (2) that are intended to be, and in fact were, kept confidential (3) for the purpose of obtaining or providing legal advice.[256]

Ultimately, the Court held that the communications were not privileged and provided three bases for its reasoning: (1) Claude® is not an attorney, (2) the communications were not confidential, and (3) the communications were not for the purpose of obtaining legal advice.[257]

---

[249] *Id.*
[250] *Id.*
[251] *Id.*
[252] *Id.*
[253] *Id.* (citations omitted).
[254] *Id.* at *2.
[255] *Id.*
[256] *Id.* (quoting United States v. Mejia, 655 F.3d 126, 132 (2d Cir. 2011)).
[257] *Id.* at *2-3.

> Applying these principles here, the AI Documents lack at least two, if not all three, elements of the attorney-client privilege.[258]

The Court's first basis is both simple and dispositive.

> In the absence of an attorney-client relationship, the discussion of legal issues between two non-attorneys is not protected by attorney-client privilege.[259]
> […]
> Because Claude® is not an attorney, [] that alone disposes of Heppner's claim of privilege.[260]

Commentators argued that A.I. was similar to "other Internet-based software, such as cloud-based word processing applications[.]" but the Court not only was unconvinced by these arguments, but reiterated that those applications too call into question attorney-client privilege.[261]

Second, the Court reasoned that the communications were not confidential, both because they were communicated with the third-party A.I. platform and because of that platform's privacy policy.[262]

> [T]he written privacy policy to which users of Claude[®] consent provides that Anthropic[®] collects data on both users' "inputs" and Claude[®]'s "outputs," that it uses such data to "train" Claude[®], and that Anthropic[®] reserves the right to disclose such data to a host of "third parties," including "governmental regulatory authorities."[263]

Meaning, not only is the attorney's or client's conduct relevant to the evaluation of privilege, but also the conduct (or policies dictating conduct) of the third-party.[264] If an A.I. tool is to be utilized, you may be responsible for a more in-depth or comprehensive understanding of how the data you input is stored, utilized, or shared.[265]

Finally, although admitting this to be a "closer call," the Court ultimately determined that the communications were not for the purpose of obtaining legal advice.[266] While you might be tempted to reason that with all of A.I.'s risks – many we have discussed in this paper – it would be dangerous to recommend a client utilize A.I., the Court's reasoning here cuts against the grain. The Court found that because Heppner utilized the A.I. tool "of his own volition" and without the express direction of counsel to do so, he could not have been obtaining legal advice.[267]

---

[258] *Id.* at *2.
[259] *Id.* at *2 (quoting *In re OpenAI, Inc.*, Copyright Infringement Litig., 802 F. Supp. 3d 688, 699 (S.D.N.Y. 2025)).
[260] *Id.* (citation omitted).
[261] *Id.* ("[T]he argument that [Claude®] is like any other form of software only cuts against the invocation of privilege because all '[r]ecognized privileges' require, among other things, 'a trusting human relationship,' such as, in the attorney-client context, a relationship 'with a licensed professional who owes fiduciary duties and is subject to discipline.' See Ira P. Robbins, Against an AI Privilege, JOLT Dig., Harvard L. Sch. (Nov. 7, 2025), https://jolt.law.harvard.edu/digest/against-an-ai-privilege.")
[262] *Id.*
[263] *Id.* (citing Anthropic, Privacy Policy (as of February 19, 2025), https://www.anthropic.com/legal/archive/a2eecf43-807a-4a53-89dd-04c44c351138).
[264] *See id.*
[265] *See id.*
[266] *Id.* at *3.
[267] *Id.*

> Claude[®] disclaims providing legal advice. Indeed, when the Government asked Claude[®] whether it could give legal advice, it responded that "I'm not a lawyer and can't provide formal legal advice or recommendations" and went on to recommend that a user "should consult with a qualified attorney who can properly assess your specific circumstances."[268]

G. Practice Tips

So, if you are going to use A.I. in your practice, here are few tips:

5. Double check results.
6. Use for ideas only, not submission-ready documents or drafting.
    a. Ex: the first prompt used by counsel in *Avianca* was "argue that the statute of limitations is tolled by bankruptcy of defendant pursuant to [M]ontreal [C]onvention". That likely would have been acceptable to generate counter-arguments for counsel to consider when making his arguments. However, in this instance the generator made up law and made assertions without legal citations. When the generator was pressed to substantiate its stated positions, it hallucinated information.
7. Be careful about disclosing confidential information or breaching other ethics rules when submitting prompts or questions to the generator.
8. Discuss the use of A.I. with your clients both from a consent (your use of A.I.) and educational (their use of A.I. in relation to their legal matter) standpoint – ex: *U.S. v. Heppner*.
9. Be careful of breaching local rules or standing orders, etc.

H. A.I. Headlines

A.I. is rapidly changing. From the time this section is drafted to the date of the conference, several A.I. advancement will likely have been announced. So, here are a few headlines of A.I. news from the past few months:

1. A.I. & the Labor Market: A.I. Companies Self-report & Tattletale

Two of the most iconic A.I. companies in the world have published reports on the impacts of the technology and tools they are producing.

In March 2025, Anthropic® (the producer of "Claude®" A.I. systems) published a report titled "*Labor market impacts of AI: A new measure and early evidence*."[269] Anthropic® utilized data from the following sources: (1) The O*NET database, which is operated by the U.S. Department of Labor, Employment and Training Administration, (2) Anthropic®'s own data, and (3) estimates from research conducted and published by Tyna Eloundou, Sam Manning, Pamela Mishkin, and Daniel Rock entitled *GPTs are GPTs: An Early Look at the Labor Market Impact Potential of Large Language Models (2023)*.[270]

The report covers several topics, but some of the key takeaway statements were as follows:

> AI is far from reaching its theoretical capability: actual coverage remains a fraction of what's feasible

---

[268] *Id.*

[269] Maxim Massenkoff and Peter McCrory, *Labor market impacts of AI: A new measure and early evidence*, ANTHROPIC (March 5, 2026) (https://www.anthropic.com/research/labor-market-impacts) (available in PDF: https://cdn.sanity.io/files/4zrzovbb/website/2b5bbaf2c1eb81dbf6e6fb813c1a24e35a64d376.pdf).

[270] *Id.* at 3. *See also* O*NET 30.2 Database and the U.S. Department of Labor, Employment and Training Administration (https://www.onetcenter.org/database.html#overview); TYNA ELOUNDOU, SAM MANNING, PAMELA MISHKIN, and DANIEL ROCK, *GPTs are GPTs: An Early Look at the Labor Market Impact Potential of Large Language Models*, Cornell University (August 22, 2023) (https://arxiv.org/abs/2303.10130) .

> Occupations with higher observed exposure are projected by the BLS to grow less through 2034
>
> Workers in the most exposed professions are more likely to be older, female, more educated, and higher-paid
>
> We find no systematic increase in unemployment for highly exposed workers since late 2022, though we find suggestive evidence that hiring of younger workers has slowed in exposed occupations[.][271]

One interesting aspect of the report was Anthropic®'s attempt to compare A.I.'s "theoretical LLM capability" and the "actual automated usage" occurring in various occupations.[272] In other words, what is expected to be possible for A.I. in a given industry – say, legal services – versus how much A.I. technology is actually be utilized in that industry. Anthropic® admits that there remains a "large gap" between what A.I. is anticipated to provide and what it is currently providing, including in the legal industry.[273]

The report indicated that 68% of work tasks – as categorized by O*NET – could be fully automated to A.I., with just 3% of work tasks being "not feasible" for A.I. use.[274] This means that "97% of the tasks observed […] fall into categories rated as theoretically feasible by Eloundou et al. (β=0.5 or β=1.0)."[275] The "most exposed occupations" according to the report were as follows:

> Computer programmers
> Customer service representatives
> Data entry keyers
> Medical record specialists
> Market research analysts and market specialists
> Sales representatives, wholesale and manufacturing, except technical and scientific products
> Financial and investment analysts
> Software quality assurance analysts and testers
> Information security analysts
> Computer user support specialists[276]

As for the legal industry specifically, the report showed that law is exposed, but far-less than some other occupations.[277]

> [M]any tasks, of course, remain beyond AI's reach—from physical agricultural work like pruning trees and operating farm machinery to legal tasks like representing clients in court.

Roughly one month later, Anthropic®'s primary competitor – OpenAI® – published a report titled "*Industrial Policy for the Intelligence Age: Ideas to Keep People First*", which proposes "a slate of people-

---

[271] *Id.* at 2.
[272] *Id.*
[273] *Id*.
[274] *Id.* at 4.
[275] *Id.* at 5.
[276] *Id.* at 7.
[277] *Id.* at 8 (BLS projected employment growth from 2024-2034 vs. AI exposure).

first policy ideas" for governments to consider implementing in response to "superintelligence" tools.[278] It is notable that this report was published shortly after OpenAI® received immense public backlash for rushing to the altar to ink a deal with the U.S. Department of Defense after Anthropic® and the administration had a "falling out" over how the military intended to use Anthropic®'s technology.[279] Anthropic® filed a lawsuit in federal court in San Francisco on March 9, 2026, regarding its dispute with the Defense Department.[280] So if you are thinking this OpenAI® report might be a public-relations crisis-management tool, this author would agree. Regardless, the report does have some useful insights.

> While we strongly believe that AI's benefits will far outweigh its challenges, we are clear-eyed about the risks—of jobs and entire industries being disrupted; bad actors misusing the technology; misaligned systems evading human control; governments or institutions deploying AI in ways that undermine democratic values; and power and wealth becoming more concentrated instead of more widely shared.[281]

The report makes several recommendations, including – notably – proposals for mass restructuring of the U.S. economy akin to the New Deal and including increases of capital-gains and corporate taxes.[282]

> On this path to superintelligence, there are clear steps we need to take today. People are already concerned about what AI will mean for their lives—whether their jobs and families will be safe, and whether data centers will disrupt their communities and raise energy prices. AI data centers should pay their own way on energy so that households aren't subsidizing them; and they should generate local jobs and tax revenue. Governments should implement common-sense AI regulation—not to entrench incumbents through regulatory capture but to protect children, mitigate national security risks, and encourage innovation.[283]

2. A.I. Legislation or Regulation?

Governmental bodies around the globe have taken action to address the exponential evolution of A.I. – such as the EU Artificial Intelligence Act[284] However, thus far, legislation and regulation of A.I. in the United States has been largely disregarded, with the exception of some individual states.[285] There is a growing friction between states that wish to impose regulations and the current administration's preference to permit A.I. to grow unhindered.

---

[278] *Industrial Policy for the Intelligence Age: Ideas to Keep People First*, OPEN AI (April 2026) (https://openai.com/index/industrial-policy-for-the-intelligence-age/) (available in PDF: https://cdn.openai.com/pdf/561e7512-253e-424b-9734-ef4098440601/Industrial%20Policy%20for%20the%20Intelligence%20Age.pdf).

[279] *E.g.*, MICHAEL LIEDTKE and DAVID KLEPPER, What to know about the clash between the Pentagon and Anthropic over military's AI use, Associated Press (Updated 4:30 PM CDT, February 28, 2026) (https://apnews.com/article/anthropic-pentagon-ai-dario-amodei-hegseth-0c464a054359b9fdc80cf18b0d4f690c).

[280] *Anthropic PBC v. U.S. Department of War et al*, 3:26-cv-01996-RFL (N.D.C.A. (San Francisco) filed March 9, 2026).

[281] *Supra* note 278, at 3.

[282] *E.g.*, *id* at 3-4, 6.

[283] *Id.* at 4.

[284] Artificial Intelligence Act (Regulation (EU) 2024/1689) (available at https://eur-lex.europa.eu/eli/reg/2024/1689/oj). *See also* https://artificialintelligenceact.eu/.

[285] *E.g.*, *Texas Responsible Artificial Intelligence Governance Act, HB 149, 89th Reg. Sess. (Tex. 2025); See generally,* TEX. BUS. & COM. CODE ANN. §§ 551.001-554.103.

3. **A.I. in Education, Law Schools, and Early Careers**
   - "Cognitive offloading is described as a phenomenon where people want to offload cognitive tasks and have AI help them do it rather than doing it themselves"[286]
   - "How are law schools using AI and how will AI shape the future of legal practice?"[287]
   - "Perfect homework, blank stares: Why colleges are turning to oral exams to combat AI"[288]
   - "AI case study for law professors: How to build complimentary teaching tools"[289]

4. **A.I. in Agriculture – a few examples…**
   - Virtual Fencing[290]
   - Packers and processors - mass production operations, monitoring, testing, logistics, inspections, etc.[291]

5. **A.I.'s Next Leap**
   - Launch of Anthropic®'s Mythos™ model and "Project Glasswing" for a limited set of institutional, industrial, and governmental users. Prompting an emergency meeting of the U.S. Federal Reserve, U.S. Department of the Treasury, and numerous CEOs of America's largest banks.[292]

VIII. SUMMARY

Now, [take a breath], if you are feeling a bit overwhelmed by the lightning pace of these changes to the practice of law, do not fret.

> One step at a time is all it takes to get you there.[293]

You can do this.

---

[286] Mandie Haney, *Tech students question AI's cognitive impact*, THE DAILY TOREADOR (https://www.dailytoreador.com/article/74508eb5-e616-4920-8824-5582499030cd) (March 31, 2026) (quoting Shan Xu, Associate Professor for Public Relations & Strategic Communication Management, Texas Tech University).

[287] Clarity, *How are law schools using AI and how will AI shape the future of legal practice?* (Feb. 23, 2026) (https://podcasts.apple.com/us/podcast/how-are-law-schools-using-ai-and-how-will-ai-shape/id1415134527?i=1000751121385).

[288] Jocelyn Gecker, *Perfect homework, blank stares: Why colleges are turning to oral exams to combat AI*, Associated Press (April 22, 2026) (https://apnews.com/article/college-oral-exam-ai-chatgpt-77954a19f5304bfc6e76dc92d4bef3ad).

[289] Natalie Runyon, *AI case study for law professors: How to build complimentary teaching tools*, Thomsom Reuters (March 17, 2026) (https://www.thomsonreuters.com/en-us/posts/legal/ai-law-professors/).

[290] *E.g.*, https://www.halterhq.com/.

[291] *E.g.*, Cargill, *Artificial Intelligence* (https://www.cargill.com/about/artificial-intelligence) (last visited May 1, 2026).

[292] Aimee Picchi and Richard Escobedo, *Fed Chair Jerome Powell, Treasury's Bessent and top bank CEOs met over Anthropic's Mythos model*, CBS News MoneyWatch (April 10, 2026) (https://www.cbsnews.com/news/mythos-anthropic-ai-cybersecurity-risks-powell-bessent/); ANTHROPIC, Project Glasswing (https://www.anthropic.com/glasswing).

[293] Emily Dickinson.