CIRCUITS

e-Journal of the Computer & Technology Section of the State Bar of Texas

April 26

SECTION LEADERSHIP

Lavonne Burke Hopkins, *Chair*
Mitch Zoll, *Chair-Elect*
Grecia Martinez, *Treasurer*
Sally Pretorius, *Secretary*
Aaron Woo, *e-Journal Co-Editor*
Katie Stahl, *e-Journal Co-Editor*
Sally Pretorius, *CLE Committee Chair*
William Smith, *Imm. Past Chair*

COUNCIL MEMBERS

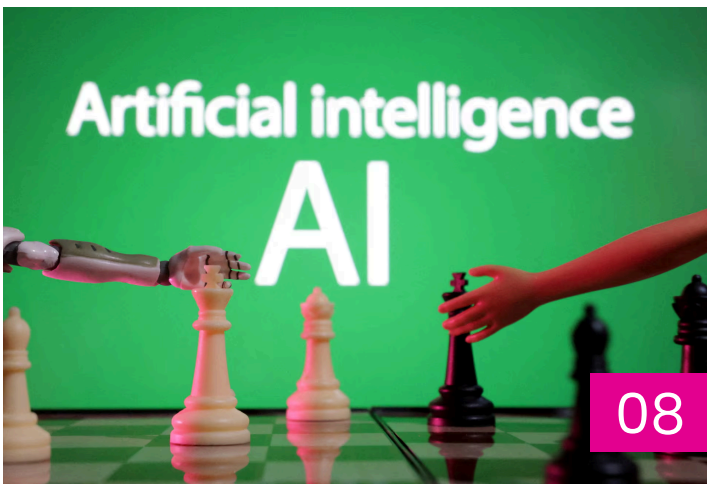
Sean T. Hamada
Sanjeev Kumar
Katherine L. Stahl
Lori B. Bellows
Elizabeth Sandoval Cantu
Aaron W. Woo
Fatima Naeem
Marshall S. Sales
Lea R. Williams

JUDICIAL APPOINTMENTS

Hon. Karin Crump
Hon. Xavier Rodriguez

In This Issue:

Table of CONTENTS



Welcome to the Spring 2026 issue of Circuits! We're easing into the birth of spring to examine recent legal trends, industry insights, and practice tips surrounding technology that section members should be aware of.

AI and the collection of data is changing the technology landscape and the practice of law.

This edition of Circuits examines some of the most current issues and best practices regarding the use of artificial intelligence that practitioners can apply, including:

- Trust, Not Technology: Understanding Where You Are on the AI Adoption Curve
- Federal Trade Commission and Artificial Intelligence
- Nonsecure Technology Platforms and Elements of Human Anatomy: Privacy Under the Krutz Rule
- Generative Artificial Intelligence and Legal Ethics – A Foundational Approach
- Where AI Risk Actually Lives: Liability, AI Governance, and Automated Decisions
- Helping More Clients with Less: AI and Limited Scope Practice -
- South Carolina Supreme Court upholds Stored Communications Act's good faith provision
- Statistical disparity fails to establish a claim under the Fourteenth Amendment's Equal Protection Clause
- The Hidden Exposure in Your Supply Chain: What Corporate Counsel Need to Know About Vendor Risk

These articles will delve into a wide spectrum of topics pertaining to technology and the practice of law that practitioners will find useful. From effectively advocating for your clients to streamlining your law firm operations, our contributors have graciously shared their thoughtful insights that will improve your practice.

If you have an idea for an article or a topic you'd like to see covered, please reach out and raise awareness to our membership. We'd love to hear from you!

Enjoy the issue!

Aaron Woo and Katherine Stahl

Co-Editors, Circuits

Computer & Technology Section

State Bar of Texas

Trust, Not Technology: Understanding Where You Are on the AI Adoption Curve

Chad Atlas
Chief Legal Officer and Head of Growth at an AI-native company

If you are like most lawyers, your relationship with artificial intelligence has settled into a wary rhythm. You probably use ChatGPT occasionally—to summarize a dense article, brainstorm a marketing hook, or draft a polite email to difficult opposing counsel. You know it's useful. You also know it sometimes lies. You treat it like a brilliant but unreliable colleague: capable of flashes of insight, but never to be trusted without verification.

This is reasonable. It's also incomplete.

The technology has advanced faster than the conversation about it. While the profession has been debating the ethics of chatbots, a new generation of artificial intelligence (AI) tools has emerged—ones that don't just answer questions but execute multi-step tasks within existing workflows. The shift matters, but not because the AI got smarter. The limiting factor for AI adoption in legal practice was never technical capability. It's trust.

And trust, as it turns out, needs to be developed in stages.

Consider how most lawyers currently use AI: search assistance, summarization, first drafts. The lawyer remains firmly in control. If the tool suggests something wrong, the lawyer catches it and moves on. The risk is low because the oversight is total. Call this Phase I—AI as a supervised assistant.

This is also where the specialized legal-tech platforms have largely stalled. They required new interfaces, new habits, new data hygiene—parallel systems that never quite fit the realities of practice. Generic workflows bolted onto specific needs. For many lawyers, the value never justified the cognitive overhead.

Phase II looks different. AI tools can now operate within existing file systems, read native documents, and follow persistent rules that lawyers have defined. Rather than migrating to a vendor platform, lawyers can build workflows incrementally within their own environments. The AI adapts to how they already work—not the reverse.

Here's what this looks like in practice. Over the past few weeks, I've been building a persistent working relationship with an AI assistant. It starts with a memory file—plain text instructions that teach the AI how I organize my files, what my naming conventions are, and what principles govern my workflow. From there, I built custom commands: one to scaffold new projects with the structure I actually use, another to systematically close completed work while extracting lessons learned for future reference, a third to archive abandoned projects with context about why they stalled.

Each command ends with a feedback question: "How did this work? Any improvements?" When I answer, the AI updates its own instructions. When it makes a mistake, I tell it to fix its memory. When a workflow is clunky, I tell it to revise the process. The learning compounds. It's the closest thing I've experienced to training an associate—except the training persists across sessions and never needs to be repeated.

None of this required code. The instructions are markdown files (simple text files) I can read, edit, and share. The AI adapts to how I already work; I don't migrate to a new platform or learn a new interface. This is what Phase II looks like: tools that operate within your existing environment, learning your preferences rather

than imposing generic workflows.

But we're still early. These tools require careful scoping. Tasks must be broken into discrete steps. Outputs need verification. It's not "handle this closing"—it's training the AI on discrete, repeatable skills: "review this section, flag these issues, draft this summary." The delegation is real but bounded.

Phase III remains aspirational: genuine autonomous delegation. The lawyer defines objectives and constraints; the AI executes end-to-end—managing a due diligence process, coordinating document production, or shepherding a routine filing through to completion. We aren't there yet. And getting there will depend less on improvements in AI capability than on lawyers developing the judgment to delegate safely—judgment that can only be built through Phase II experience.

Why hasn't adoption been faster? Three concerns recur in conversations with colleagues.

First, accuracy. The original "ChatGPT lawyer" who cited fabricated cases became the profession's cautionary tale. The fear of hallucination is legitimate. But the lesson wasn't that AI is unusable—it's that AI outputs are drafts, not answers. The workflow must account for verification.

Second, confidentiality. Privilege, client data, training on inputs. These concerns are real but manageable. Lawyers already use cloud-based email, practice management software, and e-discovery vendors. The same vetting discipline applies: sandbox experiments with non-client data, understand what the tool does with inputs, choose providers with appropriate data handling commitments.

Third, utility. If the time spent learning and configuring exceeds the time saved, the math doesn't math. This is where the newer tools have an advantage—they integrate into existing environments rather than requiring wholesale changes.

AI developers are now releasing open-source legal workflows—skills for contract review, non-disclosure agreement (NDA) triage, compliance analysis, and similar tasks. An NDA triage skill, for instance, categorizes incoming agreements as green (approve), yellow (needs review), or red (significant issues) based on configurable playbooks. A contract review skill checks terms against an organization's standard positions and escalation triggers. These skills are written in plain text, readable and modifiable. Lawyers can inspect the logic and adjust the thresholds. This is not a black box—it's transparent infrastructure that encodes judgment rather than replacing it.

The signal here is significant: even AI developers recognize that legal judgment cannot be automated away. The tools encode your risk tolerances and standard positions. They implement professional judgment; they do not substitute for it (yet).

This leads to an observation the profession may find uncomfortable: effective AI use requires something beyond legal knowledge. Call it taste—judgment about which tasks benefit from AI assistance, where verification burdens outweigh time savings, and what "good enough" looks like in different contexts. These are decisions that cannot be delegated. No improvement in model capability will make them disappear.

Ethan Mollick, a Wharton professor whose research on AI and work is worth following, describes AI capability as a "jagged frontier"—reliable in some domains, unreliable in others, with the boundaries shifting unpredictably. AI excels at recall, cross-referencing, and narrowing review. It struggles with nuanced legal conclusions and rarely surfaces its own uncertainty. Mapping these edges is becoming part of professional competency.

The gap between what AI can do and what most lawyers use it for is substantial—and widening faster than many expect. The lawyers who benefit most won't be the most technically sophisticated. They'll be the ones who learn early where the tools work, where they don't, and how to build workflows that reflect those boundaries.

The alternative—waiting for perfect tools or official guidance—carries its own risk. By the time AI is reliable enough to use without judgment, it may not need lawyers at all.

AI does not threaten the profession by thinking. It challenges lawyers by forcing decisions about how work gets done.

The question is not whether to engage with these tools. It's whether you'll be the one setting expectations—or scrambling to meet them.

ABOUT THE AUTHOR:
Chad Atlas is Chief Legal Officer and Head of Growth at an AI-native company focused on funding transactions, a strategic advisor to select startups, and a coach for luddite lawyers. He writes about law and technology at No Vehicles in the Park on Substack.

Federal Trade Commission and Artificial Intelligence

Fatima Naeem

While there is no overarching federal law regarding Artificial Intelligence (AI), using AI inappropriately can lead to a violation of a plethora of other laws, such as Equal Employment Opportunity Commission, Fair Housing Act, Federal Trade Commission Act (FTCA), etc. In fact, the Federal Trade Commission (FTC) has begun taking action "against deceptive or unfair conduct that harms consumers as part of its new initiative, Operation AI Comply."[1] As of September 2024, the FTC has taken action against five different companies. We will focus on two of these for now.

To begin, let's discuss DoNotPay's issues with the FTC. DoNotPay "claimed to offer an AI service that was "the world's first robot lawyer" but "could not deliver on the promise."[2] The FTC alleged that "the company did not test whether its 'AI lawyer' operated to the level of a human lawyer when generating legal documents and giving advice, and the company did not hire or retain attorneys to test the quality and accuracy of its service's law-related features.[3] In January 2025, the parties entered into a Consent Agreement Order.[4] According to the Consent Order, DoNotPay was found to be in violation of the FTCA and settled for $193,000.00.[5] The lesson here is that: do not make claims regarding AI that cannot be supported as well as make sure that the AI is tested by professionals in the field to guard against biases and hallucinations. If you are asked to review an AI tool as counsel for the company, ask lots and lots of questions. Find out how the company is planning on advertising its AI.

The FTC is starting to crackdown on inappropriate use of AI to deceive consumers. In another case, the FTC filed a complaint against Rytr. According to FTC's complaint, Rytr is a company that "bills itself as [AI] enabled 'writing assistant' service" and "generates written content for its users under 43 distinct 'Use Cases,'" charging its clients some of its service."[6] One of the Use Case services was offered as "Testimonial & Review" that allowed "users to generate written content for reviews."[7] The FTC alleged that these reviews "contain specific, often material details that have no relation to the user's input" and these "would almost certainly be false for the user who copy the generated content and publish it online. In many cases, these false reviews feature details that would deceive potential consumers deciding to purchase the service or products described."[8] In 2024, the parties entered into an Agreement Consent Order for a violation of the FTCA,[9] barring Rytr from "engaging in similar illegal conduct in the future" and "advertising, promoting,

[1] FTC Announces Crackdown on Deceptive AI Claims and Schemes | Federal Trade Commission
[2] FTC Announces Crackdown on Deceptive AI Claims and Schemes | Federal Trade Commission
[3] FTC Finalizes Order with DoNotPay That Prohibits Deceptive 'AI Lawyer' Claims, Imposes Monetary Relief, and Requires Notice to Past Subscribers | Federal Trade Commission
[4] DoNotPay | Federal Trade Commission
[5] DoNotPay | Federal Trade Commission
[6] Rytr: Complaint
[7] Rytr: Complaint
[8] Rytr: Complaint
[9] Rytr: Decision and Order

marketing, or selling any service dedicated to – or promoted as – generating consumer reviews or testimonials."[10] Rytr should have tested the AI on multiple occasions and it is possible if they had audited the tool throughout its use, the company may have found the problem and taken steps to correct the matter. It might have been more beneficial for them to stop this specific tool for the time being if they discovered the problem, while they resolved the issue rather than allowing it to run continuously. Now, they face reputational damage which will not be an easy fix to rebuild trust in their consumers.

These instances show that while we may not have one specific rule regarding AI, we still need to be diligent in advising our clients because they may inadvertently violate another law. All in all, the good news for lawyers is that our profession is safe from AI taking over our jobs, at least for the time being.

ABOUT THE AUTHOR:

Fatima Naeem is the founding attorney of Naeem Law Firm, PLLC, where she focuses on cyber law, data privacy, healthcare compliance, mediations, arbitrations, and guardianships. With a commitment to staying at the forefront of legal developments, she earned her LLM in Cyber Law and Data Privacy from Drexel University in 2023 and became Certified in Healthcare Compliance in 2024. Since graduating from Texas Tech University School of Law in 2015, she has dedicated herself to serving the community, starting with Lone Star Legal Aid before hanging her own shingle in 2019. Starting in June 2021, Fatima has served as the Chief Compliance Officer for HealthPoint, a Federally Qualified Health Center, and also as its General Counsel from 2023-2024. Find more about Naeem Law Firm at www.naeemlawfirm.com.

[10] Rytr LLC, In the Matter of | Federal Trade Commission

NONSECURE TECHNOLOGY PLATFORMS AND ELEMENTS OF HUMAN ANATOMY: PRIVACY UNDER THE KURTZ RULE

Gerard Reinart

CONSIDER THE RECENTLY ANNOUNCED KURTZ RULE: A user has no privacy rights in either the content or metadata associated with nonsecure internet searches or, by corollary, nonsecure email transmissions.

A nonsecure search platform is generally one that logs search queries, IP addresses, or click behavior, uses cookies, shares data with advertisers or data brokers, and lacks encryption. Google is an example of a nonsecure search platform, and Gmail, Hotmail, and Yahoo are examples of nonsecure email platforms.

PRIVACY, TECHNOLOGY, AND THE THIRD-PARTY DOCTRINE

The scope of the Fourth Amendment privacy right has occasionally morphed in view of technology developments. The "third-party doctrine" has emerged as an important factor in analyzing the scope of the Fourth Amendment right in cases involving technology. This doctrine holds that, generally, a person lacks a reasonable expectation of privacy in information or materials when that person exposes that information to a third party. For example, the third-party doctrine has been invoked to negate any basis for reasonable expectation of privacy in checks written against bank accounts[1], and in telephone numbers dialed and later retrieved by pen register.[2]

Conversely, in Carpenter v United States[3], the U.S. Supreme Court held that obtaining cell-site location information ("CSLI") data from a wireless carrier to track the location of a person is a Fourth Amendment search requiring a warrant. The court's holding was based on its conclusion that cell phone location information is not truly "shared" because users do not effectively consent to such disclosures. Cell phones were characterized as being "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society". The court noted that individuals "compulsively carry cell phones with them all the time, and characterized them as "almost a 'feature of human anatomy'"[4] (emphasis added). Furthermore, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user's part beyond powering up.[5]

A prior 5th Circuit court held to the contrary under the business records exception.[6]

THE KURTZ DECISION

The Pennsylvania Supreme Court has recently issued an opinion that extends the third-party doctrine to nonsecure online searches, holding that dragnet reverse keyword searches violate neither the Fourth Amendment, nor the Pennsylvania Constitution.[7]

In reviewing a defendant's objection to the

[1] U.S. v Miller, 425 U.S. 435 (1976).
[2] Smith v. Maryland, 442 U.S. 735 (1979).
[3] Carpenter v. United States, 585 U.S. 296 (2018).
[4] Carpenter at 311, quoting, Riley v. California, 573 U.S. 373, 385 (2014).
[5] Id, at 298.
[6] In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, (5th Cir 2013).
[7] PA. CONST. art. 1, §8.

admissibility of the results of the reverse keyword search, the Pennsylvania Supreme Court[8] addressed the Fourth Amendment right to privacy in view of the third-party doctrine.

The court distinguished *Campbell* by noting that unlike smart phones, the internet is not a "feature of human anatomy" and that users willingly transmit data to a third party whenever they type terms into a search engine and hit the "Enter" key.[9]

The court also observed that the reasonableness of an expectation in privacy in the routine use of the internet is highly suspect, stating that "It is common knowledge that websites, internet-based applications, and internet service providers collect, and then sell, user data."[10]

The court further noted that the terms that Google applies to the use of its search engine undermine any reasonable expectation of privacy in the metadata associated with such searches. These terms explicitly reserve to Google the rights to collect user data, including device-specific information, search queries, and IP addresses. These terms are readily available to users via the "Privacy" button on the Google website.

This reasoning seems to be readily applicable to content and metadata associated with nonsecure email systems (e.g., Gmail) as well as prompts, uploads, and results of artificial intelligence platforms (e.g., Gemini).

A contrary holding from the Colorado Supreme Court sets up jurisdiction for a Supreme Court[11] challenge. Short of that, other states may adopt the *Kurtz* Rule, via either statute or judicial action.

ARE ONLINE USERS COMPETENT TO MAKE DECISIONS REGARDING TECHNOLOGY?

The U.S. Supreme Court recently granted certiorari in a case set up to determine whether dragnet geolocation warrants violate the Fourth Amendment.[12] The Fourth Circuit has held that a person voluntarily provided his location data to Google by opting into Location History, and thus under the third-party doctrine, he lacked a reasonable expectation of privacy in those data.[13]

BROADER IMPLICATIONS OF THE KURTZ RULE

Based on the reasoning behind the Kurtz Rule, its adoption could raise some thorny questions outside the close of reverse keyword searches, in a range of disparate legal areas including privilege, ethics, and intellectual property.

- Attorney-Client Privilege: Attorney-client privilege is generally waived if a confidential communication has been disclosed to a third party, unless the communication is made to further a common legal interest.[14]

  Will attorney-client communications transmitted via a nonsecure email system (perhaps the client's Gmail account) undermine the privilege?

  In case of such a failed privilege claim, would a malpractice action against the attorney who used a nonsecure email platform survive a motion to dismiss?

- Ethics: Is transmission of confidential client information via a nonsecure email system a violation of an attorney's ethical duty to maintain the confidentiality of such information[15]?
- Trade Secret: "The owner of a trade secret will lose his secret by its disclosure unless it is done in some manner by which he creates a duty and places it on the other party not to further disclose or use it in violation of that duty."[16]

  Is transmission of a trade secret via a nonsecure email system a failure of the owner to take reasonable measures to maintain the secrecy of the trade secret?

[8] Commonwealth of Pennsylvania v. Kurtz, J-36A-2024, No. 98 MAP 2023 (PA Sup. Ct., Dec. 16, 2025).
[9] Kurtz, at 20.
[10] Id, at 22.
[11] Colorado v Seymour, 2023 CO 53, 23SA12 (CO Sup. Ct. 2023).
[12] Chatrie v. United States, No. 25-XXXX, U.S. cert. granted Jan. 16, 2026.
[13] Chatrie v. United States, 22-4489, 2025 WL ___, 4th Cir. Apr. 30, 2025.
[14] Luckenbach Tex., Inc. v. Engel, 2022 U.S. Dist. LEXIS 187911, *5, 2022 WL 9530041 (WDTX 2021).
[15] See Texas Disciplinary Rules of Professional Conduct. § 1.05.
[16] Hoover Panel Sys. v. Hat Contract, 2021 U.S. Dist. LEXIS 239482, *27, 2021 WL 5829515 (WDTX 2021).

- Copyright: Is transmission of an expressive work via a nonsecure email system a publication under the Copyright Act[17], which could impact the availability of statutory damages in case of infringement by a third party?

CONSIDERATIONS FOR ATTORNEYS

Prudent attorneys may wish to consider the following items, which are offered in an abundance of caution:

- Avoid the use of nonsecure emails (e.g., Gmail) in communications with clients, colleagues, experts, and vendors. If a client currently uses such an email, urge the use of a secured email platform (e.g., Proton).
- In any questions concerning a legal matter, avoid the use of any nonsecure search engines or AI platforms.
- In contractual notice provisions, specify only secured, encrypted email addresses.
- In contracts, include representations that no party has used nonsecure emails, search engines, or artificial intelligence tools to generate or communicate any material within the scope of the confidential material provision. Recite the secure modalities that may be so used. Include corresponding warranties.
- In conducting due diligence of a transaction involving Intellectual Property, explore the questions above regarding implications for patents, copyrights, and trade secrets. These questions will similarly apply in litigation.
- In discovery requests, specify that any email entries on a privilege log include the email platform, and if it is a nonsecure platform (e.g., Gmail, Hotmail, Yahoo), challenge the privilege based on the third-party doctrine.

ABOUT THE AUTHOR:

Gerard Reinhardt is an attorney with over 25 years of experience in Intellectual Property. He is licensed to practice law in Texas, Florida, New York, and the District of Columbia. He is also registered to practice before the US Patent and Trademark Office. Gerard has litigated complex patent cases with the NY IP boutique Morgan & Finnegan for such clients as Exxon, IBM, and Bombardier, and practiced in-house with Merck in the life sciences and Hatch-Waxman spaces. In addition to a JD and MBA, Gerard holds BS and MS degrees in Chemical Engineering. Prior to starting the practice of law, Gerard practiced engineering for 15 years with Raytheon.

Gerard@ReinhardtIP.com
Call or text: 516-672-3988
ReinhardtIP.com
FruitsofGenius.com

[17] See 17 USC §412.

Generative Artificial Intelligence and Legal Ethics – A Foundational Approach

Karla Pascarella

Introduction: AI's Entry Into Legal Practice

The release of legal-specific generative AI tools by major technology companies signals a meaningful shift in how legal services may be delivered. The introduction of tools like Anthropic's AI plugin, capable of contract review, risk flagging, and workflow automation,[1] raises important questions about both market disruption and professional responsibility. Whether or not such tools displace existing legal-technology vendors, their availability underscores a broader reality: artificial intelligence has become an unavoidable part of modern legal practice, and lawyers remain responsible for ensuring that innovation enhances, rather than undermines, professional judgment, client trust, and ethical compliance.

From headlines highlighting hallucinations in legal briefs to in-house legal teams prioritizing use of AI to reduce the cost of legal services, the landscape is changing and requires lawyers not only to keep up but, in the absence of prescribed governance structures, to help chart the course using existing ethical foundations as a base.

II. The Technical Foundations of Large Language Models

To use generative AI responsibly, lawyers benefit from a foundational understanding of how large language models (LLMs) function. The following provides a brief overview of key technical and practical points summarized by Gemini from my original draft.

A. LLMs

1. Next-Word Prediction: At their core, LLMs are statistical systems that predict the next "token" (numerical representations of text) based on patterns found in massive datasets.
2. Machine Learning & Optimization: Models improve through gradient descent, which is an algorithm that uses derivatives to adjust mathematical parameters and reduces prediction errors over billions of iterations.
3. Mathematical Structure: LLMs are high-dimensional mathematical objects. They do not possess "intent" or "understanding"; they simply optimize for statistical likelihood.

B. GPTs and Alignment

1. Generative Pre-trained Transformers (GPTs): These represent a leap in encoding language into "vector spaces," allowing for complex numerical modeling of word relationships.
2. The Need for Alignment: Raw models are initially "unaligned," meaning they can produce fluent but untruthful or inappropriate text. Developers use reinforcement learning and human feedback to steer the AI toward useful and safe outcomes.
3. Software Layers: Legal professionals usually interact with AI through intermediate software that uses filtering and "pre-prompting" to improve consistency, though these do not eliminate the need for oversight.

C. Capabilities and Limitations

1. The Hallucination Risk: Because LLMs prioritize language patterns over factual verification, they can "hallucinate" by generating fabricated legal authorities or false statements with high confidence.
2. Augmentation vs. Substitution: While input quality

[1] https://legaltechnology.com/2026/02/03/anthropic-unveils-claude-legal-plugin-and-causes-market-meltdown/

2. (prompting) significantly affects the output, generative AI is a tool to augment legal work, not a substitute for professional judgment or human review.

III. Ethical Duties Implicated by AI Use

The ethical obligations implicated by generative artificial intelligence are not new; rather, AI magnifies long-standing duties imposed by professional conduct rules. Both the ABA Model Rules of Professional Conduct and the Texas Disciplinary Rules of Professional Conduct (TDRPC) apply fully to AI-assisted legal work.

A. Duty of Competence and Technological Proficiency

The duty of competence requires lawyers to understand the tools they use in representing clients. ABA Model Rule 1.1 defines competent representation as requiring the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation. Comment 8 expressly extends this obligation to understanding "the benefits and risks associated with relevant technology." In the context of generative AI, this means lawyers must possess a functional understanding of how these systems operate, including their probabilistic nature, susceptibility to hallucinations, and limitations in factual verification. Reliance on AI-generated outputs without independent review or verification risks violating Rule 1.1 by substituting statistical prediction for professional judgment.

Texas imposes a parallel obligation through Texas Rule 1.01, which requires competent and diligent representation. In Texas Ethics Opinion 705 (2025), the Professional Ethics Committee confirmed that Rule 1.01 applies fully to generative AI tools and cautioned that attorneys must understand AI systems sufficiently to evaluate their outputs critically. Opinion 705 makes clear that a lawyer's duty of competence is not satisfied by superficial familiarity with AI tools; rather, attorneys must appreciate both their efficiencies and their risks before integrating them into legal work. This now could extend to local counsel despite their knowledge of lead counsel's use or misuse of AI tools.[2]

B. Duty of Diligence, Verification, and Candor

Lawyers have an ongoing duty to act with diligence and to ensure that representations made to courts and third parties are accurate. ABA Model Rule 1.3 requires reasonable diligence and promptness in representing a client, while ABA Model Rule 3.3 imposes a duty of candor toward tribunals, prohibiting false statements of fact or law. When generative AI is used in drafting briefs, pleadings, or memoranda, these duties require lawyers to verify all legal authorities and factual assertions, regardless of the tool's apparent fluency or confidence.

Recent sanctions decisions have underscored that submitting AI-generated hallucinations—particularly fabricated case citations—violates these duties not because AI was used, but because the lawyer failed to exercise diligence and verification. The non-delegable nature of these responsibilities means that attorneys remain fully accountable for accuracy even when AI contributes to the drafting process.

Texas law mirrors these obligations. Texas Rule 3.03 requires candor toward the tribunal and prohibits false statements of material fact or law. Texas Ethics Opinion 705 expressly warns that reliance on unverified AI outputs may expose lawyers to Rule 3.03 violations if inaccurate information is presented to a court. Taken together, these rules confirm that AI does not mitigate a lawyer's duty to verify; instead, its use heightens the need for human oversight. Most recently, Texas Courts have found lawyers responsible for failure to disclose the use of AI in preparing legal briefs even though no hallucinations were involved.[3]

---

[2] See Wadsworth et al. v. Walmart Inc. et al., No. 2:23-cv-00118 (D. Wyo.) where the court found local counsel responsible for hallucinations in a court filing and rejected the idea that being "local counsel" absolved her of the duty to ensure the accuracy of court filings, emphasizing that Rule 11 of the Federal Rules of Civil Procedure imposes a non-delegable gatekeeping duty on every attorney who signs a filing. Wadsworth v. Walmart Inc., No. 2:23-cv-00118, 2025 WL 608073, at *8 (D. Wyo. Feb. 24, 2025).

[3] See, e.g., Wilson v. KIPP Texas Inc., No. 3:24-cv-02578, where the court found that counsel's failure to disclose the use of generative AI in preparing a pleading despite the absence of fake citations violated the court's Civil Local Rules (see L. Civ. R. 7.2(f)) and F.R.C.P 11 by effectively making a false certification that no AI was used. Wilson v. KIPP Texas Inc., No. 3:24-cv-02578 (N.D. Tex. Oct. 31, 2025.

C. Duty of Confidentiality and Data Security

Confidentiality obligations apply with equal force to AI-assisted legal work. ABA Model Rule 1.6 prohibits revealing information relating to the representation of a client without informed consent and requires lawyers to make reasonable efforts to prevent unauthorized disclosure or access. Because generative AI systems typically involve transmitting prompts to third-party servers, inputting client information may constitute disclosure if adequate safeguards are not in place.

This risk is heightened where AI vendors retain user inputs or use them for model training. Accordingly, Rule 1.6 requires lawyers to evaluate a provider's data-handling practices, retention policies, and security controls before using generative AI with confidential material. Even enterprise-grade or "legal-specific" AI tools do not eliminate this obligation.

Texas Rule 1.05 provides similar protections for confidential information and was expressly applied to generative AI use in Texas Ethics Opinion 705. The opinion cautions that attorneys should not input confidential client information into AI systems without reasonable assurances regarding confidentiality and data security. The ethical inquiry therefore turns not on convenience or efficiency, but on whether the lawyer has taken reasonable steps to protect client information.

D. Duty of Supervision and Responsibility for Non-Lawyer Assistance

Lawyers remain responsible for work performed with the assistance of non-lawyers and technological tools. ABA Model Rule 5.3 extends supervisory responsibility to non-lawyer assistance, a category that reasonably includes generative AI systems used in legal work. Under this rule, attorneys are accountable for ensuring that AI-assisted outputs comply with professional obligations, just as they would be for work performed by paralegals or other staff.

Supervisory duties are reinforced by ABA Model Rule 5.1, which requires firm leaders to implement measures giving reasonable assurance that all lawyers and staff comply with ethical rules. In the AI context, this supports the adoption of written AI-use policies, training programs, and review protocols.

Texas Rules 5.01 through 5.03 impose parallel supervisory obligations. Texas Ethics Opinion 705 emphasizes that lawyers may not abdicate responsibility to technology and must supervise AI-assisted work in the same manner as human assistance. Ethical compliance therefore depends on governance, review, and accountability rather than automation.

E. Communication, Fees, and Transparency

Ethical use of generative AI also implicates duties of communication and reasonable fees. ABA Model Rule 1.4 requires lawyers to keep clients reasonably informed about the means by which their objectives are pursued, while ABA Model Rule 1.5 prohibits unreasonable fees. When AI materially affects how legal services are delivered—or significantly reduces the time required to perform work—lawyers must consider whether disclosure is appropriate and whether billing practices remain reasonable.

Texas Rules 1.03 (Communication) and 1.04 (Fees) impose similar constraints. Texas Ethics Opinion 705 observes that efficiencies achieved through AI should inure to the client's benefit, particularly in hourly billing arrangements, and that charging unreasonable fees for AI-assisted work may violate Rule 1.04. Transparency and fairness therefore remain core ethical touchstones even as technology evolves.

IV. Conclusion

Generative AI presents both opportunities and risks for the legal profession. When used thoughtfully, it can enhance efficiency and support higher-value legal work. When used carelessly, it can undermine trust, compromise confidentiality, and expose lawyers to ethical violations.

Ultimately, lawyering remains a fundamentally human endeavor. Generative AI should be understood not as a replacement for professional judgment, but as a tool that demands heightened responsibility, transparency, and ongoing education.

ABOUT THE AUTHOR:
Karla is a dynamic and forward-thinking legal strategist. She specializes in proactive identification and resolution of complex legal issues for both international and domestic corporations. Her approach transcends traditional legal frameworks, emphasizing innovation and strategic foresight to build robust and resilient organizations by leveraging technology.

Where AI Risk Actually Lives: Liability, AI Governance, and Automated Decisions

Maria Castro

Artificial intelligence (AI) is here, and already embedded in everyday professional life. Don't doubt that. Many of us have had the moment of pausing over an email, a credit decision, a résumé screen, or a compliance report and wondering, was this done by a person or by an algorithm? Increasingly, the answer is that it was done, at least in part, by AI. [1]

These systems are no longer sitting quietly in the background. They shape who is hired, who receives credit, how insurance claims are evaluated, which patients are prioritized, and even how compliance reviews and litigation strategies unfold. As automated decision-making becomes routine, the legal fiction that AI is too complex to be accountable is disappearing.

When automated systems make or influence decisions that cause harm, the question courts and regulators now ask is not how the algorithm works, but whether the organization using it exercised reasonable care in selecting, deploying, and overseeing it.[5][6]

The end of the black box defense

For years, organizations argued that because AI models were opaque and that they could not be meaningfully supervised. That argument is losing force. In negligence, fiduciary-duty, and professional-responsibility cases, liability turns on what the organization did to manage risk, not on how complicated the technology was.

If an automated system denies credit, filters applicants, flags patients, or drives compliance decisions, the organization remains responsible for ensuring that those outputs align with legal, ethical, and contractual obligations. As we know, "The AI made the decision" is no more a defense than "the spreadsheet calculated it."[7] Opacity may explain how a mistake occurred, but it does not excuse failing to prevent it.[4]

Why contracts cannot absorb AI liability

Many enterprises try to shift AI risk to vendors through disclaimers, indemnities, and limitation-of-liability clauses, but most core legal duties are non-delegable. A law firm cannot outsource confidentiality. A hospital cannot outsource patient care. A lender cannot outsource fair-lending compliance.[2]

When an AI system produces biased, inaccurate, or unlawful results, legal exposure almost always flows to the organization that relied on it. *Vendor contracts may affect who ultimately pays*, but they do not eliminate the duty to supervise, validate, and control the technology in the first place.[5]

In litigation and regulatory inquiries, the focus is not on what the vendor promised. It is on what the organization did to govern the system.[6]

Governance as the new standard of care

AI governance is becoming the legal benchmark for reasonableness.[7] and regulators and courts are increasingly ruling that **using AI without a formal**

[1] Akerman LLP, The AI Legal Landscape in 2025: Beyond the Hype
[2] Cooley LLP, AI in the Workplace: U.S. Legal Developments
[3] K&L Gates, AI in Recruiting and Employment Decision-Making: New California AI Regulations
[4] White & Case, Automated Decision Making Emerges as an Early Target of State AI Regulation
[5] Duane Morris LLP, Gen AI Class Action Key Decisions and Trends in 2025
[6] Reuters, Old Laws, New Tech: The Massive Litigation Poised to Define 2026
[7] National Law Review, Artificial Intelligence Legislative Update

governance framework is per se unreasonable

Regulators and courts increasingly look for documented model-selection and validation processes, risk and bias assessments, monitoring and escalation procedures, and clearly defined human accountability for automated outcomes. These governance structures now play the same role that internal controls, supervision, and compliance programs have long played in other regulated contexts. They are how organizations prove they acted responsibly.[4][8]

An enterprise that deploys powerful automated systems without governance is no longer innovative, it is exposed. Automation without accountability doesn't create advantage; it magnifies blind spots. Decisions scale faster than understanding, risks compound silently, and control is given to systems no one fully owns. What looks like speed is often just momentum, and momentum without direction is failure waiting to surface.

Where AI risk concentrates

Across industries, the most serious AI liability does not arise from futuristic edge cases. It comes from three very ordinary failures.

1. Oversight gaps: Failing to review outputs or verify that automated decisions comply with existing legal and ethical standards.[3]
2. Delegation errors: Allowing systems to make or materially influence decisions without clearly defined human authority, review, and override. State Bars, like California and New York, have already initiated disciplinary actions against attorneys who delegated brief-writing to AI without verifying citations, establishing a clear precedent for "delegation errors" in professional services.
3. Governance voids: Deploying advanced AI outside any compliance, audit, or risk-management framework. In 2025, a landmark class-action suit against Workday over its AI-powered applicant screening made the risk clear. Deploying automated tools without an audit trail for bias creates real exposure. Without a governance framework,
3. companies lack a paper trail and cannot show that discrimination was anticipated, tested for, or meaningfully prevented.

These are not hypothetical risks. They are already appearing in enforcement actions, discrimination claims, consumer-protection cases, and professional-discipline matters.

Accountability in delegated judgment

Ultimately, AI has not displaced established legal principles. It has reinforced them. Duties of care, supervision, and professional responsibility apply with equal force when decisions are made by automated systems as when they are made by human actors. The mechanism has changed, but the obligations have not.

AI is not a future risk, it is a present condition. Automated systems already influence hiring, credit, pricing, and access at scale, often outside formal oversight. The central question in emerging AI liability is not how an algorithm functions, but whether the humans who selected, deployed, and relied on it exercised reasonable judgment and control.

Governance, not technical opacity, will determine outcomes. It is the line between defensible innovation and unmanageable legal exposure.

ABOUT THE AUTHOR:

Maria Jose Castro is the founder and managing attorney of Castroland Legal, PLLC, a Texas-based firm concentrating on business and emerging technologies. She advises startups, MSPs, and law firms on regulatory compliance, helping modern organizations meet rising expectations around data protection and operational accountability.

[8] National Conference of State Legislatures (NCSL), Summary of Artificial Intelligence 2025 Legislation

Helping More Clients with Less: AI and Limited Scope Practice

Marshall Sales

In courtrooms across Texas, one thing is constant. Most people cannot afford full legal representation. Many do not qualify for legal aid. And increasingly, even middle income families find themselves priced out of hiring a lawyer for an entire case. Judges see it. Clerks see it. Lawyers see it. Clients feel it.

In my practice, and in conversations with colleagues around the state, I hear the same story. For many Texans, the choice is no longer between hiring a lawyer and representing themselves. It is between representing themselves and walking away from important legal rights altogether.

Limited scope representation, sometimes called unbundled legal services, was designed to help fill that gap. Instead of hiring a lawyer for an entire case, a client hires one for specific tasks such as drafting pleadings, representing the client at a single hearing, reviewing an agreement, or receiving advice on next steps. Texas lawyers are permitted to structure these engagements under Rule 1.02 of the Texas Disciplinary Rules of Professional Conduct, which allows attorneys to limit the scope of representation with informed client consent.

In theory, the model makes sense. In practice, it can be hard to implement.

Limited scope work creates real challenges. Intake takes time. Clients misunderstand what is covered. Scope creep happens. Withdrawal can feel uncomfortable. Many lawyers worry about responsibility without full control of the case. I hear these concerns often, even from attorneys who care deeply about access to justice.

At the same time, artificial intelligence tools have quietly become part of daily legal work. Many lawyers already use them for drafting, editing, and organizing information. The question is not whether these tools exist. The question is whether they can responsibly support limited scope practice. From what I have seen, they can, if used carefully.

Where Limited Scope Works Best

Limited scope representation extends across many areas of practice. In family law, lawyers assist with uncontested divorces, agreed modifications, and drafting final decrees. In estate planning, they prepare wills and powers of attorney. In small business work, they review contracts and operating agreements. In landlord tenant and consumer matters, they help with notices, pleadings, and negotiated resolutions.

In each of these settings, many clients do not need full representation. They need focused help at key moments.

Why Limited Scope Needs Better Infrastructure

Most limited scope problems are not legal problems. They are workflow problems.

Too much time is spent gathering basic information. Clients are unsure what happens next. Documents arrive incomplete. Deadlines slip. By the time legal advice begins, much of the energy has already been spent. This is not bad lawyering. It is the reality of limited time and limited resources.

The demand for limited scope services is not driven only by low income needs. It is driven by economics. Hourly rates have risen. Litigation has become more complex. Even families with stable incomes struggle to justify spending tens of thousands of dollars on relatively straightforward matters. As a result, many middle income Texans appear in court without lawyers, not by choice but by necessity. Limited scope representation offers a way to

reconnect this group with professional guidance. This is where technology can help.

Where AI Can Add Real Value

You do not need to be a software programmer to use these tools. If you can use email and Word, you can use AI assisted software. Think of it as a very fast assistant who can read, summarize, and organize information. It does not replace your judgment; it supports it.

In my practice, AI has been particularly helpful in intake and triage. Guided questionnaires can organize timelines and flag obvious issues. This allows me to spend less time gathering facts and more time thinking about solutions.

Document support is another area. Many limited scope matters involve standard pleadings or agreed orders. AI can help generate first drafts based on templates, format documents, and create filing checklists. Lawyers still need to review and edit everything. The difference is starting with a structure instead of a blank page.

Consider an uncontested divorce where the parties agree on property division. They may own a home, vehicles, or retirement accounts. They do not need prolonged litigation. They need accurate documents. A lawyer can review the agreement, prepare a final decree, and draft related transfer documents such as deeds or refinancing provisions. With organized intake and AI assisted drafting, the lawyer can review and refine rather than build from scratch. The result is efficient, responsible service that protects the clients and produces a clean, enforceable order.

AI can also improve client education. Clear explanations of hearings, deadlines, and next steps reduce confusion and follow up calls. Case management improves when systems help track tasks and deadlines. None of this is glamorous. All of it is practical.

Ethical and Professional Limits

Using AI does not reduce your ethical responsibilities. It increases them.

Lawyers remain responsible for competence, confidentiality, and supervision. Every output must be reviewed. Sensitive information must be handled carefully. Clients should understand how technology is being used in their case. AI does not give legal advice. Lawyers do.

A Practical Model for Limited Scope Practice

A technology supported limited scope workflow can be straightforward. The client completes a guided intake. The lawyer reviews the information and confirms the scope in writing. AI assisted tools help prepare drafts and explanations. The lawyer edits and advises. The representation ends clearly, with written confirmation of next steps.

This structure protects both lawyers and clients.

Conclusion

Limited scope representation is one of the most promising tools we have for narrowing the justice gap in Texas. But it will not succeed on goodwill alone. It requires systems that make it workable for lawyers and understandable for clients.

Used responsibly, AI can be part of that system. Not as a replacement for lawyers. Not as a shortcut around ethics. But as practical infrastructure that helps us deliver focused legal help more efficiently.

Technology will not solve every problem in our profession. But it can help us serve more people without losing what makes this work meaningful. If it allows us to help more clients with less friction and more clarity, it is worth thoughtful attention.

ABOUT THE AUTHOR:

Marshall Sales is an Austin based trial lawyer with Hennan | Culp PLLC, where he focuses on high-conflict divorce and custody matters, complex property disputes, international child abduction cases, and related appeals. He earned his undergraduate degree from Texas A&M University and his J.D. from the University of Texas School of Law. He serves as a representative for the Texas Young Lawyers Association, as co-chair of the Communications and Outreach Committee of the Texas Access to Justice Commission, and as a board member of the State Bar of Texas Computer and Technology Section. Outside of practice, he enjoys spending time with his wife, Barb; playing live shows as the guitarist for his band, Blah Spa; catching comedy shows; adopting senior dogs; and competing as a croquet enthusiast.

South Carolina Supreme Court upholds Stored Communications Act's good faith provision

Pierre Grosdidier

In State v. Carter, the South Carolina Supreme Court applied the good faith exception to the exclusionary rule to deny the suppression of evidence secured through a warrantless cell site location information (CSLI) search performed pursuant to the Stored Communications Act's § 2702(c)(4) (the "SCA").[1] This section states that an electronic communication service provider:

> (a) may divulge a record or other information pertaining to a subscriber to or customer of such service [excluding contents] . . . (4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency[2].

Reshawn Vertez Carter and his confederates, looking for drug money, staged a pre-dawn home invasion on a stash house occupied by a lone woman, whom they threatened with a gun. The invasion ended when one of the intruders was shot in the head by a third-party intervening on behalf of the woman's alerted boyfriend,[3] and the remaining acolytes flitted. Authorities soon zeroed in on Carter and his cell phone number and co-opted his service provider to share real-time CSLI to locate and arrest him. Authorities secured the CSLI by completing and submitting an "'Exigent Circumstance Request Form'" pursuant to the SCA's § 2702. A detective stated on that form that authorities were searching for a suspect involved in a home invasion during which a man was fatally shot. The form contained the boilerplate language that "The urgency of the situation (and/or other factors) renders it unfeasible to obtain a search warrant."[4]

A jury convicted Carter of a plethora of criminal offenses. At trial and on appeal, Carter argued that authorities obtained the CSLI in violation of the Fourth Amendment of the United States Constitution and of article I, section 10, of the South Carolina Constitution. The trial court denied the motion and both higher courts affirmed, albeit for different reasons.

The general rule that the United States Supreme Court established in Carpenter v. United States is that "'an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.'"[5] Carpenter's implication is that authorities normally require a warrant to secure CSLI. But the rule allows exceptions under emergency conditions and exigent circumstances, such as when pursuing a fleeing suspect, or protecting a person from imminent harm or evidence from imminent destruction.[6] In Carter I, the Court of Appeals of South Carolina applied the exigent circumstances exception to the exclusionary rule because authorities were chasing suspects at large following a violent home invasion that ended with a fatality. Alternatively, the court held that the authorities' conduct was protected by the ood faith exception to the exclusionary rule, which applies "'when investigators act

[1] State v. Carter, 912 S.E.2d 264, 267–68 (S.C. 2025) (Carter II) (citing 18 U.S.C. 2702(c)(4)).
[2] 18 U.S.C. 2702(c)(4).
[3] The boyfriend allegedly owned the money stashed in the apartment.
[4] Carter II, 912 S.E.2d at 266.
[5] State v. Carter, 884 S.E.2d 195, 199 (S.C. App. 2022) (Carter I) (citing Carpenter, 135 S. Ct. 2206, 2217 (2018).
[6] Id. (citing Carpenter, 135 S. Ct. at 2223).

with an objectively reasonable good faith belief that their conduct is lawful.'"[7] In that case, authorities relied on the SCA's §§ 2703(c)(1)(B) and (d), which operate on the basis of a court order and without the element of good faith.

The South Carolina Supreme Court also affirmed on different grounds , without opining on the lower courts' otherwise "sound" analyses. The court instead relied on the SCA's § 2702(c)(4), which grants leave to providers to disclose CSLI to authorities based on the good faith belief that an emergency justifies it. The court held that the SCA's plain language makes it "irrefutably clear that the good faith exception to the exclusionary rule applies." Thus, in this case, even if a constitutional violation occurred in this case—an issue the court did not decide—the detective that signed the form relied in good faith on the SCA and had "'an objectively reasonable good faith belief'" that he acted lawfully.[8]

The court held that the investigator's good faith justified the exclusionary rule. Section 2702(c)(4)is clear that the provider must believe in good faith in the emergency at hand. The court's ruling did not explain how an investigator's good faith belief is seemingly automatically ascribed to the provider. But one federal district court decision cited in Carter II did. In United States v. Caraballo, the United States District Court for the District of Vermont found that the service provider in that case acted in good faith after it received a warrantless § 2702(c)(4) request from the Vermont police.[9] The provider's testimony was that its "practice and policy [was] to rely on law enforcement certification under oath subject to the penalties of perjury that the information provided" on its § 2702(c) CSLI request form was "true and accurate." The provider's analysts who handled these requests did not perform their own determination of exigent circumstances. The reasoning was that an analyst sitting in an office was not in a position to second-guess the jurat of a law enforcement officer in the field calling a situation an emergency.[10]

ABOUT THE AUTHOR:

Pierre Grosdidier is a litigation attorney in Houston. He is board certified in construction law by the Texas Board of Legal Specialization. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, a Fellow of the Texas Bar Foundation, and a registered P.E. in Texas (inactive). He was the State Bar of Texas Computer & Technology Section Chair for 2022–23 and was elected Medium Section Representative to the State Bar of Texas for the 2023–26 term.

[7] Id. and n.6 (citing United States v. Chavez, 894 F.3d 593, 608 (4th Cir. 2018)) (internal quotations omitted).
[8] Carter II, 912 S.E.2d at 267–68 (citing Davis v. United States, 564 U.S. 229, 238 (2011).
[9] Id. at 268 (citing United States v. Caraballo, 963 F. Supp. 2d 341, 349 (D. Vt. 2013)).
[10] Caraballo, 963 F. Supp. 2d at 349.

Statistical disparity fails to establish a claim under the Fourteenth Amendment's Equal Protection Clause

Pierre Grosdidier

Richmond, Virginia, police officers arrested Keith Moore after he fled a traffic stop triggered by his manifestly fake vehicle tag.[1] Authorities indicted Moore, a convicted felon, after they found a gun in his vehicle. At trial, Moore's expert witness presented statistical evidence that Black drivers in Richmond were 5.13 times more likely to be stopped by the police than their White counterparts because 77 percent of the stops involved Black drivers versus only 14.16 percent for Whites. Black drivers also tended to be stopped throughout the city, whereas White drivers tended to be stopped in predominantly white neighborhoods. Still, the expert expressly denied opining that Moore was stopped because he was Black. The government's expert, for his part, derided Moore's expert's statistical techniques as "elementary" and his conclusions as "unsupported by the data and analysis."[2]

The trial court dismissed Moore's indictment after concluding that Richmond's allegedly racially selective law enforcement violated the Fourteenth Amendment's Equal Protection Clause (EPC), even though it acknowledged that the officers had probable cause to stop him. The Fourth Circuit Court of Appeals disagreed and directed the trial court to reinstate the indictment.[3] The case demonstrates once again that weak statistics will not suffice to prove a selective enforcement claim.

The EPC bars selective law enforcement based on racial criteria. To prove his claim, Moore had to show, "by clear evidence, that his traffic stop had a discriminatory effect and was motivated by a discriminatory purpose or intent." It is a demanding standard because such a claim asks a court to exercise its power over law enforcement, a prerogative of the Executive.[4]

The circuit court first categorically rejected the claim that the officers acted with discriminatory purpose. They had probable cause to stop Moore, and the video of the encounter showed that they treated him very respectfully. Thus, there was "a complete absence of evidence" that Moore's stop was discriminatory. The circuit court next addressed the trial court's conclusion that the higher frequency at which Black drivers were stopped, along with "evidence of Richmond's history of discrimination," evinced a discriminatory purpose by the Richmond Police Department.[5]

The circuit court reiterated the black-letter rule that discriminatory intent in a specific case, as in Moore's, can only rarely be inferred from statistical disparities. The fact that many charged defendants in a class of cases are Black does not mean that any individual prosecution was racially motivated.[6] Moreover, by Moore's expert's admission, his statistical evidence linking race and traffic stops was "somewhat weak," yet it largely formed the basis for the trial court's conclusion that Moore was stopped because of his race.[7]

The expert's data also did not account for the racial composition of Richmond drivers. The fact that, for

[1] United States v. Moore, 145 F.4th 572, 574 (4th Cir. 2025).
[2] Id. at 575–77 (internal quotations omitted).
[3] Id. at 575.
[4] Id. at 579 (citing Whren v. United States, 517 U.S. 806, 813 (1996)).
[5] Id. at 580–81. Richmond's alleged history of discrimination was placed in evidence by Moore's second expert witness.
[6] Id. at 582 (citing cases).
[7] Id. at 581–82.

example, 65 percent of stopped drivers are Black cannot reveal a disparity if 65 percent of all drivers are also Black. As the circuit court noted, "'raw data' lacking 'an appropriate basis for comparison' cannot satisfy any element of an Equal Protection claim."[8]

The expert also conceded that his data and analysis could not control for confounding variables, i.e., hidden factors that distort relationships and lead to erroneous cause-and-effect conclusions. Some studies have shown that accounting for confounding variables—such as poverty, residence in crime-prone neighborhoods, and pending arrest warrants—can negate apparent racial disparities in traffic stops.[9] This omission could be particularly detrimental in this case because Richmond police clustered their traffic stops in high-crime areas.

In rejecting the expert's data and reinstating the indictment, the circuit court reiterated that officers acting with clear probable cause, as in this case, are unlikely to be driven by discriminatory purpose. It also noted that accepting the expert's data and conclusion would result in the untenable dismissal of "every prosecution" of Black drivers stopped in Richmond.[10]

ABOUT THE AUTHOR:

Pierre Grosdidier is a litigation attorney in Houston. He is board certified in construction law by the Texas Board of Legal Specialization. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, a Fellow of the Texas Bar Foundation, and a registered P.E. in Texas (inactive). He was the State Bar of Texas Computer & Technology Section Chair for 2022–23 and was elected Medium Section Representative to the State Bar of Texas for the 2023–26 term.

[8] Id. at 582.
[9] Id. at 582–83.
[10] Id. at 583–84 (emphasis in original).

The Hidden Exposure in Your Supply Chain: What Corporate Counsel Need to Know About Vendor Risk

Zandra Robinson

Why vendor risk matters now. Vendor-originated incidents are no longer "IT issues." They are legal, governance, market-moving events. Under the rules of the Securities and Exchange Commission (SEC) in 2023 , public companies must disclose a material cybersecurity incident on Form 8-K within four business days of determining materiality. The trigger is the materiality determination, not the date of discovery, which compresses decision cycles for legal, security, finance, and disclosure controls.[1]

The rule also added Item 106 to Regulation S-K, which requires companies to describe processes to assess, identify, and manage cybersecurity risks, including those that arise from third-party service providers, as well as the board's oversight and management's role.[2]

Why Texas counsel should care about NYDFS

I get it. New York rules in a Texas article can feel like wearing boots to Broadway. But, hear me out. Three reasons.

1. Your customers span jurisdictions, including New York, where many may be considered covered entities under the New York Department of Financial Services (NYDFS). They frequently require security and incident coordination terms that align with their programs, creating indirect obligations for you.[3]
2. Benchmarking "reasonable" security. Even if you are not a covered entity, Section 500.11's lifecycle approach, including risk-based due diligence, minimum controls, contractual protections, and periodic reassessment, functions as a durable benchmark for vendor governance that aligns with investor and regulatory expectations.[4]
3. Convergence in expectations. Federal disclosure requirements under the SEC and consumer-protection enforcement by the Federal Trade Commission (FTC) both emphasize continuous third-party oversight. As a result, NYDFS-style controls map cleanly to national expectations for governance and transparency.[5]

Important Texas context. There is no Texas statute as detailed as NYDFS § 500.11 for third-party cybersecurity governance. Texas has breach-notification and consumer-privacy laws, and Texas DIR standards for public entities, but none approach Section 500.11's specificity for private-sector vendor cybersecurity controls.[6]

With that context in place, it is useful to ground the conversation in the specific frameworks that shape expectations for vendor oversight today.

The Legal Framework Behind Modern Vendor Oversight

So, what actually sets the bar for vendor oversight? The answer lies in the frameworks that shape expectations

[1] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Securities Act Release No. 33-11216, 88 Fed. Reg. 51,896, 51,903 (Aug. 4, 2023).
[2] 17 C.F.R. § 229.106.
[3] 23 N.Y.C.R.R. § 500.11
[4] 23 N.Y.C.R.R. § 500.11(a)–(b).
[5] 17 C.F.R. § 229.106; see also generally FTC Section 5 enforcement analyses (reasonable security).
[6] Tex. Bus. & Com. Code chs. 521, 541.

today:

- NYDFS § 500.11 as a benchmark. Covered financial institutions must implement written policies and procedures to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers. This includes risk-based identification and assessment, minimum cybersecurity practices, due diligence, periodic assessments, and specified contractual protections, such as multi-factor authentication, encryption, breach notification, and security representations and warranties.[7]
- FTC Section 5 as an industry-agnostic enforcement signal. Across industries, the FTC has used its Section 5 under Unfair or Deceptive Acts or Practices (UDAP) to pursue companies that fail to implement 'reasonable security,' including lapses in third-party diligence and monitoring and lapses in truthful security representations. For counsel, this functions as a defensible baseline. Conduct risk-based vendor oversight and ensure your public commitments match operational reality.[8]
- SEC disclosure framework. Companies must be prepared to describe how third-party cyber risks are assessed and governed in annual reports and, if materiality is met, to file an Item 1.05 Form 8-K within four business days. The Division of Corporation Finance has clarified that only material incidents belong under Item 1.05 and that voluntary disclosures of non-material or undetermined incidents should use Item 8.01 to avoid confusing investors.[9][10]

With those frameworks in view, it becomes easier to see how a vendor incident can cascade into legal, operational, and even bankruptcy risks for the enterprise.

How vendor outages become legal, operational, and bankruptcy risks

When a critical supplier suffers a cyber event or outage, the first-order effects include service disruption, data exposure, and missed SLAs. The second-order effects include notice obligations, regulatory inquiries, indemnity disputes, and reputational harm. The SEC has emphasized that materiality assessments must consider not only financial impact but also qualitative factors, such as reputational damage and impacts on customer or vendor relationships, which are common in third-party failures.[11]

If the vendor enters financial distress or insolvency, counsel may need to preserve evidence, assert contractual rights, and protect access to hosted assets or environments. These business-continuity realities intersect with disclosure duties when the impact rises to materiality, and they should be anticipated within governance and contingency planning.[12]

Practical steps for Texas corporate counsel

Understanding these risk pathways sets up the practical steps counsel can take to reduce exposure before, during, and after an incident.

1. Contract for resilience. Incorporate specific controls and cooperation duties. Specify multi-factor authentication and encryption requirements, patching and vulnerability service levels, evidence preservation, incident notification content and timelines, audit rights, regulator-cooperation clauses, and data portability and exit terms. Treat NYDFS § 500.11 as a model checklist, not a mandate.
2. Operationalize SEC readiness. Build a materiality playbook with roles, evidence standards, and decision logs. Align disclosure controls so that material incidents are filed under Item 1.05, while non-materialor undetermined events are disclosed, if at all, under Item 8.01, which is consistent with Corporation Finance guidance.[13][14]
3. Make governance disclosures match reality. Ensure

[7] 23 N.Y.C.R.R. § 500.11(a)–(b)
[8] See generally FTC Section 5 enforcement summaries and analyses
[9] 17 C.F.R. § 229.106(b)(1)(iii)
[10] Statement of Erik Gerding, Director, Division of Corporation Finance (May 21, 2024)
[11] 88 Fed. Reg. at 51,904–05.
[12] 17 C.F.R. § 229.106(b)–(c).
[13] 88 Fed. Reg. at 51,903–07.
[14] Statement of Erik Gerding, Director, Division of Corporation Finance (May 21, 2024).

3. your board and management oversight narratives are supported by minutes, dashboards, and escalation procedures. Explicitly include third-party risk in enterprise risk management and cybersecurity governance.[15]
4. Tier vendors and test contingencies. Risk-tier third parties and scale diligence accordingly. Run table-top exercises for supply-chain incidents, including scenarios where a provider's outage, breach, or insolvency affects regulated obligations or triggers SEC reporting. Maintain exit plans, escrow or keys for data and code access, and pre-vetted alternates for truly critical services.[16][17]
5. Align Texas privacy, security, and commercial terms (as applicable). Harmonize contract provisions with TDPSA controller and processor requirements and with FTC Section 5 expectations (as applicable) for 'reasonable security.' Require suppliers to evidence consent provenance and sound data-handling practices where sensitive data is involved.[18]

Conclusion

Vendor incidents now surface as legal, governance, and business continuity events that demand counsel's direct engagement. By aligning your governance and disclosures to SEC Item 106, using NYDFS § 500.11 as a model checklist, and integrating Texas-specific privacy and breach requirements into your vendor lifecycle, you shift vendor oversight from reactive firefighting to a predictable, defensible program. The practical path forward is to embed these expectations into contracting, due diligence, monitoring, and incident response, so that your organization is positioned to navigate scrutiny with clarity and confidence when a third-party failure occurs.

Author's Notes

Texas references you still must navigate.

- Breach notification. Texas requires notice to affected individuals without unreasonable delay and no later 60 days after determining a breach occurred, with
- Attorney General notice if 250 or more residents are affected.[19]
- Privacy and vendor contracts. The Texas Data Privacy and Security Act imposes controller and processor duties, requires data protection assessments, and mandates processor contracts that mirror controller instructions. These are important touchpoints for vendor governance, even though the statute is not as prescriptive as NYDFS on cybersecurity controls.[20]
- Public-sector frameworks. Texas's DIR TAC 202 is a robust cybersecurity framework for state agencies and public universities. It is intentionally not addressed in this article, which focuses on private-sector corporate counsel and SEC-governed entities.[21]

ABOUT THE AUTHOR:

Zandra Robinson is an award-winning Senior Counsel at Dell Technologies, where she leads legal strategy for the company's global third-party risk management portfolio. Her work sits at the intersection of security, privacy, data governance, and responsible AI, integrating these principles into systems that must scale, interoperate, and perform under real-world pressure while also building governance frameworks that enable resilience, clarity, and accountable decision-making across a globally distributed vendor landscape.

Zandra also serves as Co-Lead of the CCWC® AI + Legal Tech + Innovation Advisory Council, contributing to a national dialogue among senior in-house counsel, law firm partners, and legal tech innovators who are shaping the future of the profession.

[15] 17 C.F.R. § 229.106(b)–(c).
[16] 23 N.Y.C.R.R. § 500.11.
[17] 17 C.F.R. § 229.106(b)(1)(iii).
[18] Tex. Bus. & Com. Code ch. 541; see also FTC Section 5 enforcement analyses.
[19] Tex. Bus. & Com. Code § 521.053.
[20] Tex. Bus. & Com. Code §§ 541.104–.105
[21] Tex. Dep't of Info. Res., Texas Administrative Code Chapter 202