



COMPUTER AND
TECHNOLOGY
SECTION

CIRCUITS

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



July 2025

SECTION LEADERSHIP

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

COUNCIL MEMBERS

Maria Moffett
A. Dawson Lightfoot
Sally Pretorius
Sean Hamada
Kellye Hughes
Sanjeev Kumar
Katie Stahl
Lori Bellows
Tyler Bridegan
Liz Cantu
Aaron Woo

JUDICIAL APPOINTMENTS

Hon. Xavier Rodriguez
Hon. Roy Ferguson
Hon. Karin Crump

In This Issue:

Letter from the Editors By Katherine Stahl and Aaron Woo

Articles:

The Continued Rise of Class Actions – Considerations for Practitioners by **Elizabeth Sandoval Cantu**

Fleeing the Scene: The Technology Sector's Reaction to Reciprocal Tariffs by **Jacob Barefield**

South Carolina Supreme Court upholds Stored Communications Act's good faith provision by **Pierre Grosdidier**

Free Guy: A Lesson in Video Game Law by **Megan Frederick**

Embracing the Digital Operational Resilience Act: Transforming Indirect Obligations into Opportunities for ICT Providers by **Zandra Robinson**

The Ethical and Transparent Integration of AI Tools and Systems in Legal Writing and Pedagogy: Balancing Innovation with Integrity by **Lea Williams**

Simple AI for Lawyers by **Robert "Tony" Ray**

Short Circuits:

Genius Act by **Aaron Woo**

Texas Cyber Command by **Aaron Woo**

Table of CONTENTS



4 Letter from the Editors
by Katherine Stahl and Aaron Woo

ARTICLES

5 The Continued Rise of Class Actions –
Considerations for Practitioners
by Elizabeth Sandoval Cantu

9 Fleeing the Scene: The Technology Sector’s
Reaction to Reciprocal Tariffs
by Jacob Barefield

12 South Carolina Supreme Court upholds Stored
Communications Act’s good faith provision
by Pierre Grosdidier

14 Free Guy: A Lesson in Video Game Law
by Megan Frederick

19 Embracing the Digital Operational Resilience
Act: Transforming Indirect Obligations into
Opportunities for ICT Providers
by Zandra Robinson

22 The Ethical and Transparent Integration of AI
Tools and Systems in Legal Writing and Pedagogy:
Balancing Innovation with Integrity
by Lea Williams

25 Simple AI for Lawyers
by Robert “Tony” Ray

SHORT CIRCUITS

29 Genius Act
by Aaron Woo

29 Texas Cyber Command
by Aaron Woo

Welcome to the July 2025 issue of Circuits! We're entering into the heat of summer to explore recent legal trends, industry insights, and practice tips surrounding technology that section members should be aware of.

The high-tech landscape is constantly evolving, and so is the legal industry.

This edition of Circuits examines some of the most pressing issues affecting practitioners, including:

- The Continued Rise of Class Actions – Considerations for Practitioners
- Fleeing the Scene: The Technology Sector's Reaction to Reciprocal Tariffs
- South Carolina Supreme Court upholds Stored Communications Act's good faith provision.
- Free Guy: A Lesson in Video Game Law
- Embracing the Digital Operational Resilience Act: Transforming Indirect Obligations into Opportunities for ICT Providers
- The Ethical and Transparent Integration of AI Tools and Systems in Legal Writing and Pedagogy: Balancing Innovation with Integrity
- Simple AI for Lawyers
- Recent Technology-related Legislation

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!

Katherine Stahl and Aaron Woo

Co-Editors, Circuits

Computer & Technology Section

State Bar of Texas

The Continued Rise of Class Actions – Considerations for Practitioners



Elizabeth Sandoval Cantu

Class action lawsuits are on the rise. Since the US Supreme Court decided the TransUnion case in 2021, class action

lawsuits have reached an all-time high of 1,488 cases filed in 2024, up from 1,320 in 2023, 604 in 2022 and 108 in 2018. That is an increase of 1,300% in 6 years.^[1]

A search of data breaches of large and/or well-known entities, just in April 2025, reveals more than 15 high profile breaches, as reported by Cyber Management Alliance^[2]. These include the City of Lubbock, Port of Seattle, Hertz, Yale New Haven Health, Blue Shield of California and the City of Long Beach, CA—all of whom reported data leaks affecting millions of people. *Id.* With the rise of data loss or compromise, many of us may have clients who suffer data breaches, whether as the data holder or affected consumers. Mass data breaches are likely to result in class action litigation, so this article focuses on one of the many notification considerations, and revisits the seminal case on the legal challenges to class certification.

Texas Data Breach Notification Law, Texas Business and Commerce Code §521.053

One of the statutes^[3] governing notice to affected

individuals is section 521.053 of the Texas Business and Commerce Code which states that:

“A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information **shall** disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, **or is reasonably believed to have been**, acquired by an unauthorized person. The disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system” (emphasis added). Tex. Bus. & Comm. Code §521.053.

The notice must be written notice and to the last known address of the individual or may be electronic (as governed by this section and 15 U.S.C. §7001). If however, the “person” required to give the notice demonstrates that the cost of providing the notice would exceed \$250,000 or more than 500,000^[4] people are affected or the person does not have sufficient contact information, the notice can be provided by:

1. electronic mail, if the person has electronic mail addresses for the affected persons;
2. conspicuous posting of the notice on the person's website; or
3. notice published in or broadcast on major statewide media.

Notification can be delayed if a law enforcement agency

[1] Data Failures and Lawsuits Are Piling Up | Leader's Edge Magazine

[2] April 2025: Major Cyber Attacks, Ransomware Attacks and Data Breaches.

[3] Other applicable statutes and references include the Texas Rules of Professional Conduct, the American Bar Association Model Rules, Texas Medical Records Privacy Act and the Federal Health Insurance Portability and Accountability Act.

[4] Tex. Bus. & Comm. Code §521.053(h) also requires additional notification to consumer reporting agencies.

determines that the notification will impede a criminal investigation but must be provided as soon as the law enforcement agency determines the notification will no longer compromise it. *Id.* Further, if more than 250 Texas residents are affected, the breach must be reported to the Texas Attorney General as soon as possible, but no later than 30 days of the date the breach is determined to have occurred. Tex. Bus. & Comm. Code §521.053(i).

Notices to the Texas Attorney General must be made electronically through the Attorney General's website, and must include the following:

- 1.a detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;
- 2.the number of residents of this state affected by the breach at the time of notification;
- 3.the number of affected residents that have been sent a disclosure of the breach by mail or other direct method of communication at the time of notification;
- 4.the measures taken by the person regarding the breach;
- 5.any measures the person intends to take regarding the breach after the notification under this subsection; and
- 6.information regarding whether law enforcement is engaged in investigating the breach.

Id.

Those notifications, excluding sensitive information, are then posted on the Texas Attorney General's website, which is updated every 30 days^[5].

As to be expected, with the required public notifications, the ease of identifying breaches, potential impacted consumers and collecting a potential class is easier.^[6] If you represent a class or a "person" sued by a class, here are a few considerations.

LAWSUITS AND CLASS ACTIONS

Classes of affected individuals can allege negligence, negligence per se, invasion of privacy, breach of

contract, defamation, unjust enrichment as well as state consumer protection law violations. In order to bring a class action, the Courts will look to whether certain elements are met including whether:

- 1.A sufficiently large group of individuals have been similarly harmed by the breach;
- 2.The class members must have had their information accessed by bad actors; and
- 3.They suffered an injury in fact/ "concrete injury".

THE SEMINAL CASE : *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021)

In *Transunion*, Plaintiff brought an action on behalf of himself and a class whose credit reports contained erroneous "potential match" designations to a list maintained by the United States Treasury Department's Office of Foreign Assist Control of terrorists, drug traffickers and others criminals. *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021). Here, the Court considered the question of what constitutes an "injury in fact" for standing. *Id.*

A class of 8,185 individuals sued *TransUnion* under the Fair Credit Reporting Act for failing to use reasonable procedures to ensure the accuracy of their credit report. *Id.* at 413. However, of the original class, it was determined only 1,853 had their inaccurate credit reports disseminated to third parties. *Id.* The remaining 6,332 did not. The trial court rules all the Plaintiffs had standing on their statutory claims, and the jury returned a verdict for damages, including punitive damages. *Id.*

On appeal, the United States Supreme Court opined that standing required evidence of a "concrete injury". *Id.* at 414. The ability to sue did not equal an injury in fact. *Id.*

Thus, those Plaintiffs whose reports were actually shared, the Court said, suffered a harm with a "close relationship" to the harm caused by defamation. However, for those whose credit reports were not shared, the mere existence of inaccurate or false information was not sufficient basis for their claims. *Id.* Specifically, the Court said:

[5] A notification is removed from the listing not later than the first anniversary of the date the attorney general added the notification to the listing if the person who provided the notification has not notified the attorney general of any additional breaches during that period.

[6] Data Failures and Lawsuits Are Piling Up | Leader's Edge Magazine

The plaintiffs advance a separate argument based on their exposure to the risk that the misleading information would be disseminated in the future to third parties. The Court has recognized that material risk of future harm can satisfy the concrete-harm requirement in the context of a claim for injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial. See *Spokeo*, 578 U. S., at 341–342, 136 S.Ct. 1540 (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 133 S.Ct. 1138, 185 L.Ed.2d 264).

Here, however, TransUnion was able to establish that there was no risk of future harm, nor did Plaintiffs establish independent harm by the risk of exposure. *Id.* at 415.

DEFENSES

Lack of standing- No Injury in Fact

In *TransUnion*, Rodriguez had standing evidence of a concrete injury because he was denied the sale of a car when the dealership ran his credit and was advised Rodriguez was on a “terrorist list”. The Nissan dealership would not sell him a car. *Id.* at 419. His wife had to purchase the vehicle in her name. *Id.* At trial, Rodriguez testified about his experience at the dealership but did not present evidence about the experiences of the other members. *Id.* After the jury returned an award of \$984.22 for each class member and \$6,353.08 in punitive damages (more than \$60 million dollars), TransUnion appealed.

The Supreme Court acknowledged that though reputational harm, “intrusion upon seclusion” and disclosure of private information are intangible but concrete harms, Plaintiffs must maintain standing for each claim they assert and for each claim of relief. *Id.* at 431. Thus, for the claim of defamation, publication was essential for recovery. *Id.*

The mere existence of inaccurate information, absent dissemination, was not a concrete injury in fact. *Id.* And, though Plaintiffs argued “risk of future harm” was a concrete injury, the Court opined that risk might suffice for injunctive relief, but not retroactive damages.

Id. at 435.

A practitioner, therefore, should consider a motion to dismiss or a motion for summary judgment on lack of standing/lack of injury in fact. A cyber security expert is likely necessary to testify about the reasonableness of the system security and protocols, actual risk of injury, the remoteness of the injury (or, for Plaintiffs, the reasonable/substantial likelihood of dissemination/injury). Discovery and depositions should also focus on the remoteness of the risk or absence of evidence of dissemination.

In cases of targeted hacks where bad actors access protected information, the courts are split on the sufficiency of evidence to show injury in fact. In *Bohnak v. Marsh & McLennan Companies, Inc.*, the United States District Court in Louisiana addressed whether identity theft that results in unauthorized, but reimbursed, charges could confer standing. The Court opined that it did confer standing, as well as would financial injury that could be avoided or borne by a third party. *Merrell v. 1st Lake Properties, Inc.*, No. 23-1450, 2023 WL 6316257 at 4 (E.D. La. Sept. 28, 2023).

The Court also recognized that other courts have also opined that exposure, theft, and misuse of personally identifying information (PII) is sufficient to confer standing. *Id.* The Court went on to say:

Under *TransUnion LLC v. Ramirez*, a plaintiff need not show “that the level of harm he has suffered would be actionable under a similar, common-law cause of action,” only that “the type of harm he's suffered is similar in kind to a type of harm that the common law has recognized as actionable.” *Perez v. McCreary, Veselka, Bragg & Allen, P.C.*, 45 F.4th 816, 822 (5th Cir. 2022). Unauthorized disclosure of plaintiff's PII to third parties is analogous to the common-law tort of invasion of privacy based on public disclosure of private facts. See *Restatement (Second) of Torts* § 652D (Am. Law Inst. 1977). (outlining elements of tort); 9 Alfred Gans et al., *American Law of Torts* § 30:29, Westlaw (database updated March 2023) (discussing history of tort);

Courts across the country have relied on and adopted

other authorities in deciding that exposure and misuse of PII constitute concrete and particularized injuries-in-fact for redress. *Id.* It's the nature of the imminent and certainly impending injury or where there is a substantial risk of future harm that the Courts will accept standing. *Id.*

As for connecting the data breach to Defendant, the Court determined it was only required Plaintiff's injury be fairly traceable to the Defendant's conduct, especially where the only data breach notification Plaintiff received was from Defendant. *Id.*

Lack of Standing-Differences in damages

Because class certification requires a showing of commonality in the class, practitioners can focus on distinguishing the Plaintiffs impacts from the breach, the inadequacy of the named Plaintiffs to represent the class, and the lack of evidence to support the claims of other plaintiffs.

CONCLUSION

Regardless of which side of the bar you are on, you should identify what type of data breach you are dealing with, what evidence you need to secure, which experts you will need, how the class can survive a challenge, and what the courts are opining-as this litigation continues to grow and evolve. **Good luck!**

ABOUT THE AUTHOR:

Elizabeth Cantu is an insurance defense attorney in Edinburg, Texas. She is a founding member of Ramon Worthington Nicolas & Cantu, PLLC, and has 25 years of experience in litigation. She is a frequent author and speaker on cyber security issues and related litigation and is a council member of the Computer & Technology Section.

Fleeing the Scene: The Technology Sector's Reaction to Reciprocal Tariffs



Jacob Barefield

Associate Attorney at Schulz Trade Law PLLC

O Peace of Mind's Magic Trick

On April 2, 2025, otherwise known as “Liberation Day,” President Trump and his Administration used the International Emergency Economic Powers Act (IEEPA) to liberate businesses and employees from their peace of mind – specifically as it pertains to international trade – by implementing reciprocal tariffs on over 100 countries, thereby upending the once multilateral state of international trade.^[1]

And while a 90-day “pause” to the country-specific reciprocal tariffs was announced a week later, which temporarily set the reciprocal tariff to 10% for all countries, the same announcement declared that China, Hong Kong, and Macau would be subject to an overwhelming reciprocal tariff of 125%.^[2] This tariff would be stacked on top of the 20% IEEPA tariffs previously imposed on China, resulting in the total IEEPA tariff rate on China to equal 145%.^[3]

To further aggravate circumstances for



businesses operating in China, IEEPA tariffs would also be stacked on top of preexisting including Section 301 tariffs, which range between 7.5% and 100%. Hence, certain goods with China origin could be subject to tariffs as high as 245%.

As such, peace of mind has remained fleeting for many, but especially for those operating in the technology sector of the global economy, seeing as China has solidified itself as the global leader in goods manufactured.^[4]

A benchmark China made possible from 2001 to 2013, particularly when it increased its share of global manufacturing value added from 6% to 24%^[5] while simultaneously drawing foreign direct investment (FDI) from the likes of Apple, Microsoft, and Amazon.

The President's Truth

Yet the President and his Administration's 145% IEEPA tariffs have sought to dethrone China as the outright leader in manufacturing; and the President himself has taken a keen interest in the technology sector's supply chain and manufacturing, evidenced in his Truth Social post on April 13,

[1] See Exec. Order No. 14527, 90 *Fed. Reg.* 15041 (Apr. 2, 2025).

[2] See Exec. Order No. 14266, 90 *Fed. Reg.* 15625 (Apr. 9, 2025).

[3] See The White House, Apr. 15, 2025, Fact Sheet: President Donald J. Trump Ensures National Security and Economic Resilience Through Section 232 Actions on Processed Critical Minerals and Derivative Products

[4] See Brent, Stephen, How China Rode the Foreign Technology Wave, *The Am. Int.*, (Oct. 22, 2019)

[5] *Id.*

2025, where he stated:

“We [the Trump Administration] are taking a look at Semiconductors and the **WHOLE ELECTRONICS SUPPLY CHAIN** in the upcoming National Security Tariff Investigations. What has been exposed is that we need to make products in the United States, and that we will not be held hostage by other Countries, especially hostile trading Nations like China...We cannot let them abuse us on trade...”^[6]

Though the Administration has provided some exemptions for products, such as exemptions for some smartphones and computers,^[7] it remains unclear how long those exemptions will last, as the President stated in the same Truth Social post:

“NOBODY is getting “off the hook” for unfair Trade Balances, and Non-Monetary Trade Barriers...”^[8]

Yet, this “dethroning through tariffs” approach has left tech companies in complete disarray; a frenzy to find a solution for Chinese imports entering the U.S.

So where does a solution lie?

Ultimately, tech companies have resorted to looking inward, at their own FDI, manufacturing, and/or production, in an attempt to change the origin of their goods.

Even then, it remains speculative as to whether changes in manufacturing and production will permanently curb heightened tariff rates.

Apple...and then Oranges

Since President Trump’s first term, and carrying through

the Biden Administration to current date, tech companies have made the decision to move some, but not all production out of China. In addition, tech companies such as Dell and Intel have refrained from giving forthright answers for their exit from China, only citing “diversification” and “national manufacturing strategy” as reasons for their departure.^[9]

Nevertheless, the current reciprocal tariffs have created a clear rationale for exiting China – and Asia altogether. Apple recently released plans to relocate 40% of its supply chain outside of China,^[10] along with it making a mass exodus out of India by shipping five planes fully loaded with smartphones to United States, all before the reciprocal tariffs went into effect.^[11]

But not every company is equipped like Apple, and an immediate mass exodus is not plausible for most companies, as the cost associated with relocating various factors of production – such as land, human capital, and physical capital – carries too heavy of a burden for small to medium tech enterprises to withstand.

Therefore, tech companies have begun exploring ways to either move or rearrange certain factors of production associated with the “substantial transformation” of an article, in hopes to avoid both the 145% IEEPA tariff scope and extensive relocation costs.

Substantial transformation is a “mixed question of technology and customs law, though mostly the latter,”^[12] which holds that a substantial transformation occurs, and therefore a new country of origin (COO) for an article is established when:

“An article emerges from a process with a new name, character, or use, different from that processed by the article prior to processing.”^[13]

Though Customs and Border Protection (CBP) considers

^[6] See Donald J. Trump, (@realDonaldTrump)(Apr. 13, 2025, 2:36pm)

^[7] See Halpert, Madeline, Trump exempts smartphones and computers from new tariffs, British Broadcasting Corporation, (Apr. 12, 2025)

^[8] Donald J. Trump, (@realDonaldTrump)(Apr. 13, 2025, 2:36pm)

^[9] See Cattle, Alice, Why These 27 Western Brand are Abandoning China, Yahoo Fin. (Mar. 1, 2024)

^[10] See John, Kenneth, Tariffs Push to Apple to Exit China, 40% Supply Shift Planned, The Network J., (Apr. 14, 2025)

^[11] See The Economic Times, Apple Shipped Five Plane-loads of iPhones and Other Products in Three Days to Beat US Tariff Deadline (Apr. 6, 2025)

^[12] See *Texas Instruments, Inc., v. United States*, 681 F.2d 778 (C.C.P.A. 1982).

^[13] *Id.*

the totality of the circumstances and makes substantial transformation determinations on a case-by-case basis, [14] reciprocal tariffs have spurred tech companies to explore production shifts to preexisting facilities, mainly those falling outside of China and offering the capabilities to substantially transform goods that previously underwent substantial transformation in China. As a result, a change in the location of the substantial transformation of an article will allow tech companies the ability to change their product's COO, thereby allowing tech companies to avoid additional duties of 145% imposed on China.

Final Thoughts

So why is a comprehensive or partial relocation of FDI, manufacturing, and/or production not a surefire solution?

Because if we have learned anything from the ensuing trade war, it is that we should always be certain of uncertainty.

Reciprocal tariffs are no exception. As of April 18, 2025, the United States has not established a trade agreement with any country affected by the IEEPA reciprocal tariffs.

As such, a relocation of technology manufacturing from China to another country may temporarily result in lesser duties owed; but besides relocation to the United States, only trade agreements with specific countries will fully inform tech companies where it may be most advantageous to relocate. In addition, the President and his Administration may never reach a trade negotiation with a particular country or countries. As a result, 10% for a country today may become 145% tomorrow.

So, whether it is peace or a piece of mind lost, it is certain that the options ahead remain uncertain. But regardless of such uncertainty, businesses operating within the technology sector should still consider the advantages of diversifying their various factors of production in order to change their good's country of origin and avoid additional duties.

Even if it means fleeing the scene...

ABOUT THE AUTHOR:

Jacob Barefield is an Associate Attorney at Schulz Trade Law PLLC. He advises clients on a wide range of import and export issues, including customs, Foreign Trade Zone (FTZ) compliance, and sanctions. He specializes in Harmonized Tariff Schedule (HTS) classifications, substantial transformation, and Section 301 and 232 duties analyses.

[14] *Id.*

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 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 Vertz 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 fled. 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. Alternately, the court held that the authorities' conduct was protected by the good faith exception to the exclusionary rule, which applies "when investigators act with an objectively reasonable

[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).

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 ground, 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 decisions 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.

Free Guy: A Lesson in Video Game Law



Megan Frederick

The protagonists Keys and Millie in the 2021 film *Free Guy* are the quintessential indie video game designers that viewers are sure to root for; it's hard not to, when their evil boss 'stole' their video game, disassembled it, and used the parts to create a soulless, violent imitation.^[1] In fact, while not specifically explained, the two protagonists are locked in a legal battle with the main antagonist, presumably over the theft of the underlying intellectual property. Now, most viewers likely took this legal argument at face value, believed what the writer and the director told them, and thought about the issue no further. The realm of intellectual property is actually quite complex, and the legal issues in this movie go much deeper than an over-powerful, ego-maniacal rich guy who steals the idea of two designers with hearts of gold. The movie touches briefly on a plethora of issues, all to be discussed further herein: copyright ownership, licensing, and transferring of licensing; video game developers and producers, and who has the rights to what; and AI and copyright ownership. Lastly, this article will examine the actual legal disagreement at the core of this movie, discuss alternatives to avoid litigation,

and posit whether or not Millie would have been successful in her suit.

The Plot of *Free Guy* and Legal Plot Holes

The movie does not fully explain the background of how Millie and Keys sold their game to the publisher, and does not examine the underlying publishing agreement. However, what can be understood is this: Millie and Keys created a game titled *Life Itself*, and sold some portion of the rights of that game to the publishing company, Soonami.^[2] Soonami decided not to release the game, but Millie believes that it used *Life Itself's* underlying source code to create a new Soonami game titled *Free City*, and is now involved in some sort of lawsuit against the publisher.^[3] The movie presents Soonami and its CEO, Antwan, as the thieving villain. However, depending on the publishing relationship and the specific publishing agreement between the developers and the publishers, Antwan's actions, while immoral, may not have been illegal.

Copyright in Video Game Law

An artist's rights to their creative work is enshrined in the 'Patent and Copyright Clause' of the Constitution, which states that one of America's founding goals is to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."^[4] Any individual's creative work is copyrighted upon creation, provided that it is an original piece of work in a tangible form.^[5] Initially, the only protected works were "books, maps, and charts."^[6]

[1] *Free Guy* (20th Century Studios 2021).

[2] *Id.*

[3] *Id.*

[4] U.S. Const. art. 1, § 8, cl. 8.

[5] 17 USCS § 201 (a).

[6] The 18th Century, U.S. Copyright Office

However, as American society evolved, a diverse array of creative works began to bolster culture, and copyright protection was extended to the art forms where artists were conglomerating and creating: musical works in 1831,[7] dramatic compositions and public performances in 1856,[8] photographs in 1865,[9] motion pictures in 1912.[10] and computer programs in 1980.[11] Technology offered a whole slew of new opportunities for artists and entertainment, and the first copyrighted video game was registered with the Copyright Office in 1978, for the game Space War.[12]

Video games are a unique art form, and contain two copyrightable parts: the underlying code that powers the program is registered as a literary work, [13] and the audiovisual elements are registered under audiovisual works.[14] An author, or owner of the copyright, has several exclusive rights that they can either keep, license out, or transfer: the right to make and distribute copies of the work, the creation of derivative works, and the right to perform or display the work publicly.[15] The copyrightable elements in the movie[16] include the underlying code of Life Itself, any visuals of the game—including important characters or settings—specific plotlines, sounds, and any music score.

However, not every character, plotline, or setting will be copyrightable. In order for copyright to vest at the moment of creation, the work must be original, or contain “at least some minimal degree of creativity.”[17]

However, the legal doctrine *scènes à faire* leaves some room for creatives to draw inspiration from “certain stories, tropes, character types, and narrative structures hold enduring appeal for audiences . . . creators return to these archetypal figures and situations partly because they can and partly because they must.”[18] Plots such as the damsel in distress, or characters such as the wise old wizard that are “necessary to the environment or setting of an action are not the material of which copyrightable originality consists.”[19] Therefore, in a video game, a generic plotline of a hero’s quest is not likely to be copyrightable. In the case of Life Itself, a lot of the characters would likely not rise to the level of originality to receive copyright protection, or at the very least, would require a strong argument. The premise of the game is that players observe the avatars as they go about their day, but the avatars are non-player characters, or NPCs, who are generic and most likely not original.[20]

If the NPCs in Life Itself are stereotypes, such as the barista or police officer[21] with no further characteristics, in order to receive copyright protection, they would have to have some sort of defining characteristic that breaks them out of the *scènes à faire* mold, and we simply lack the knowledge of whether most characters rise to that level.

AI Ownership

The titular character of the movie, Guy, is an NPC and by the end of the film, is a fully self-actualized artificially

[7] The 19th Century, U.S. Copyright Office

[8] *Id.*

[9] *Id.*

[10] 1900-1950, U.S. Copyright Office

[11] *Id.*

[12] Nicole McNew Chen, Find Video Games in Copyright, Copyright: Creativity at Work

[13] 7 A.L.R. Fed. 2d 269, 2.

[14] *Id.*

[15] 17 USCS § 106 et seq.

[16] The movie itself is copyrighted, and that opens up a whole other slew of questions of who owns what, between the studio, the director, the writer, etc. To keep it simple, any ‘copyrightable’ element discussed herein is based on the fictional elements in the movie, not the movie itself.

[17] Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340, 345 (1991).

[18] Zahr K. Said, Grounding the *Scènes à Faire* Doctrine, 61 Hous. L. Rev. 349 (2023).

[19] Cain v. Universal Pictures Co., 47 F. Sup. 1013, 1017 (S.D. Cal. 1942).

[20] Free Guy (20th Century Studios 2021).

[21] *Id.*

intelligent character. This begs the question, do Keys and Millie have any copyright ownership over the character “Guy” once he has become a fleshed-out creation of artificial intelligence? Unlike the rest of the NPCs in *Life Itself*, Guy might be original enough to receive copyright protection in the first place; he was very deliberately created by Keys as a ‘love letter’ to Millie, so Guy “liked bubble gum ice cream and swing sets, and [he] had this very cute but oddly specific habit of always humming this classic Mariah Carey track.”^[22] Since Guy was not just a bank security guard, and had a personality, likes, dislikes, and aspirations, he would likely be original enough to be copyrightable.

This copyright protection will not extend to any artificial intelligence. Towards the end of the film, Keys realizes that Guy has evolved from the simple NPC character that they coded, and instead, “is an algorithm who thinks he’s alive.”^[23] Guy, and two of the other NPC characters in the film, evolved past their source code and performed actions that were not written in for their characters: a barista learned how to make a cappuccino, and the stereotypical “Bombshell” character wrote a book.^[24] These three are examples of artificial intelligence, or AI. The United States Copyright Office has a very clear policy that artificially-generated content is “unclaimable,” as it lacks the human authorship required to be copyrightable.^[25] If a person were to register a work that was created using AI, they would only receive copyright protection of the parts they authored themselves.^[26] If Keys or Millie were to try to claim copyright ownership over Guy, the barista, or the ‘Bombshell,’ they would only own as much as they

created.^[27] As stated above, Guy would likely be protectable, up until he became artificially intelligent. Because the other two characters were stereotypical characters needed to advance the plot of the game, they likely would fall under *scènes à faire* and be deemed too generic to be copyrightable.

Video Game Developers and Publishers: Who Owns What?

Two of the most important players in the video game realm are the developers and the publishers. Game developers are the creative minds behind the games, and can range from one kid in a basement to one-hundred people in a million-dollar company working on a single game.^[28] Developers typically enter into contracts with publishers, who will fund, market, and distribute the game, among other things.^[29] The core of a publishing contract is the intellectual property, who owns what parts of it, and what they can do with it. While individual publishing agreements can vary widely, with different amounts of control for each party, most require that the developer grant to the publisher the ability to make and distribute copies of the game.^[30] This is done by “licensing where the developer keeps copyright ownership of the video game and grants the publisher rights to the game. Occasionally, the copyright rights may be given by an assignment, which means the developer actually transfers ownership of the copyright in the video game to the publisher.”^[31]

Generally, this is a symbiotic relationship; a developer decides to work with a publisher because a publisher likely has access to a larger market of consumers,

^[22] *Id.*

^[23] *Id.*

^[24] *Id.*

^[25] Transcript, Application Process for Registration of Works with Artificial Intelligence-generated Content, Copyright Office

^[26] The copyright office received a registration for a comic book, where the words and coordination of pictures were created by a human, but the pictures themselves were created by AI. The Copyright Office only registered the words and the selection and coordination of the pictures, but would not register the pictures. Therefore, the author only has copyright protection over the words and layout of their comic book. *Id.*

^[27] *Id.*

^[28] Understanding the relationship between game developers and publishers, Gaming Street

^[29] *Id.*

^[30] Brian Wasetis, An Overview of Video Game Publishing for Developers, Aspect Law Group

^[31] *Id.*

and a publisher relies on developers to keep their companies fresh. The amount of control a developer retains over their intellectual property varies with each relationship. In a contract where the publisher receives total copyright ownership by assignment, they would hold the power in the relationship, as they now have the right to decide what to do with the game, including when to publish it or what sequels, if any, to make. It is out of the developer's hands at that point, since they no longer have the right to the underlying intellectual property. However, some contracts where the developer retains their copyrights may still tip more in the publisher's favor. While a developer will reap the benefits of the publisher's work advertising and marketing the game, the publisher generally has all the power when deciding how to advertise and market the video game; in many cases, the developer has to give up a majority of the control over their project, and trust the publisher they choose to work with.

Video game publishing agreements vary wildly based on the publisher and the developer, but by analysing one, a general understanding is gained about the division of ownership. The following excerpts are from one video game publisher's contract, Raw Fury. In the Intellectual Property Section, it states that "developer shall retain all Intellectual property rights in and to the game, including all original elements of design and game software, and all rights in all source code and object code."^[32] While it may seem like a good sign that the developer retains all IP rights, this is misleading. In the Grant of License section, publishers "have the exclusive right to publish, distribute and market the Game and the Ancillary Products worldwide without any limitations."^[33] The specific language of 'exclusive' or 'non-exclusive' rights in a publishing agreement are of the utmost importance. If a developer grants a publisher an exclusive license, that means "ownership in one or more of the copyright owner's rights is

transferred by the copyright owner to a third party."^[34] However, if a non-exclusive right is granted, the owner retains their rights.^[35] The use of the word exclusive here is telling, as this is stating that the publisher has the sole right to control what happens to the game; while the developer may own the game in theory, the publisher is the one who decides what to do with the game. If a developer wanted to play the game on a certain platform, or sell it at a certain store, or stream it with a certain streamer, they no longer have the right to do so, as they licensed that right out to their Publisher.

The Likely Outcome of Millie's Litigation

Depending on the precise language of the publishing contract, Millie's lawsuit would potentially fail if she and Keys transferred their copyright ownership over to Soonami. There is language in the Raw Fury publishing agreement that deals with underlying source code, the issue of Millie's lawsuit: "Developer also hereby grants to Publisher a **non-exclusive** right to use and Generally, this is a symbiotic relationship; a developer decides to work with a publisher because a publisher likely has access to a larger market of consumers, reproduce the object code and source code."^[36] Millie's lawsuit would likely fail if the language of the publishing contract stated that the publisher had an **exclusive** right to use and reproduce the source code; as stated above, an exclusive right is a transfer of ownership. However, with this language here, a developer would still retain ownership if they granted to the publisher a non-exclusive right. If Millie still retained the right to the source code, but the publisher was granted a non-exclusive right to 'use and reproduce' the source code, the lawsuit might not go in Millie's favor.

Another key provision that would make or break the lawsuit is the publisher's obligation to make the game commercially available. The Raw Fury publishing agreement specifically states that the "Publisher is not

^[32] Raw Fury Publishing Agreement, Page 2.

^[33] *Id.* at page 1.

^[34] Exclusive vs. Non-Exclusive Licenses, Copyright Alliance

^[35] Raw Fury Publishing Agreement, Page 1

^[36] *Id.*

obligated to make or continue to make the Game commercially available.”^[37] If such a provision existed in Millie’s publishing agreement, Soonami may not be at fault for not making the game commercially available. Some publishing agreements may have provisions stating that a developer can develop a similar game, or use the same source code for a separate game, one year after the initial game is released (but not before).^[38] This might have been an option for Millie and Keys, had this provision been in their contract. Again, without knowing the specifics of their contract, it is hard to tell how this case would come out.

The film *Free Guy* is an enjoyable comedy that actually teaches the world a lot about a very obscure topic: video game law. While it is full of plot holes regarding this theoretical lawsuit, it is still a good example of why developers should carefully read any publishing agreements before starting to work with a publisher.

ABOUT THE AUTHOR:

Megan Frederick is a 2025 graduate of Quinnipiac University School of Law with a concentration in Intellectual Property. She graduated from the College of Saint Rose in 2022 with a Bachelor of Arts degree after double majoring in English and Criminal Justice with a writing minor. She is very interested in the field of Intellectual Property, specifically trademarks and copyrights. Special thanks to Professor Caroline Carroll who assisted in the development of this paper in her Video Game Law class at QU Law.

^[37] *Id.*

^[38] Developer shall not develop, manufacture or distribute a game so similar to the game that there is a risk to create consumer confusion, or a game using the same source code as the Game but with only minor esthetical changes, for itself or any third party other than Publisher, until the date of one (1) year following the date of release of the game.” *Id.* at 3

Embracing the Digital Operational Resilience Act: Transforming Indirect Obligations into Opportunities for ICT Providers



Zandra
Robinson

Effective January 16, 2025, The Digital Operational Resilience Act (DORA) establishes a framework for EU financial entities to manage threats related to Information Communication Technologies (ICT), which encompass technologies used for the collection, storage, processing, and dissemination of information. This article examines how these obligations can become opportunities for Third-party ICT providers (ICT Providers), enhancing their services and compliance.

Understanding DORA and Its Requirements

DORA establishes four main requirements: First, financial entities must establish a ICT risk management framework, aligning with business strategies and reporting to authorities.[1] Second, an incident management process is required to detect, manage, and report incidents, with specific timelines for major incidents.[2] Third, entities must conduct digital operational resiliency testing, excluding microenterprises, to assess preparedness.[3] Lastly, DORA emphasizes third-party risk management, necessitating a strategy for using third-party services and maintaining a register of contractual arrangements.

[4] While DORA primarily applies to financial entities, it indirectly impacts ICT Providers, offering them opportunities to align their services with DORA's standards, transforming these obligations into strategic advantages.

The Role of ICT Providers

ICT Providers offer essential services such as cloud computing, data analytics, and cybersecurity solutions. Under DORA, financial institutions must ensure that their ICT Providers adhere to stringent operational resilience standards. This indirectly obligates ICT Providers to align their services with DORA's requirements, similar to a team needing to adapt its strategy mid-game to stay competitive.[5]

Defining "Critical" and "Important" Services

DORA applies to ICT services supporting "critical" or "important" functions.[6] It distinguishes between "critical" services—those whose disruption could significantly impact financial stability—and "important" services—essential for operational continuity. Understanding these definitions is crucial for ICT Providers to assess their obligations and align their services accordingly.

Opportunities for ICT Providers

Some ICT Providers might consider playing it safe by avoiding 'critical' or 'important' functions to sidestep DORA's complexities. However, true innovation demands calculated risks. Those who avoid risks often lag behind, while others surge ahead. DORA's definitions unveil five key opportunities for ICT Providers to boost their

[1] Council Regulation 2022/2554, arts. 5-13, 2022 O.J. (L 333) 1 (EU).

[2] Council Regulation 2022/2554, arts.17-20, 2022 O.J. (L 333) 1 (EU).

[3] Council Regulation 2022/2554, arts. 21-27, 2022 O.J. (L 333) 1 (EU).

[4] Council Regulation 2022/2554, arts. 28-31, 2022 O.J. (L 333) 1 (EU).

[5] Anita, N., Edward W. N. B., & Christoph E. "The Digital Operational Resilience Act for Financial Services: A Comparative Gap Analysis and Literature Review." European, Mediterranean and Middle Eastern Conference on Information Systems, 2022

[6] Council Regulation 2022/2554, art. 30(2)(b), 2022 O.J. (L 333) 1 (EU).

competitive edge:

1. **Enhanced Service Offerings:** By aligning with DORA's standards, ICT Providers can offer enhanced services that meet the regulatory requirements of financial institutions. This can include advanced cybersecurity solutions, comprehensive risk management frameworks, and resilient cloud services.
2. **Developing Specialized Solutions:** ICT Providers can develop specialized risk management and automated reporting solutions that align with DORA mandates, offering tailored services that enhance compliance and operational efficiency.
3. **Leveraging Technology Innovations:** ICT Providers can improve compliance reliability and flexibility by integrating technology innovations such as blockchain to offer cutting-edge solutions that address emerging threats.[7]
4. **Competitive Advantage:** Compliance with DORA can serve as a competitive advantage, positioning ICT Providers as trusted partners for financial institutions. ICT Providers that proactively address DORA's requirements can attract new clients and retain existing ones.[8]
5. **Innovation and Collaboration:** DORA encourages innovation in digital resilience strategies. ICT Providers can collaborate with financial institutions to develop cutting-edge solutions addressing emerging threats and enhancing operational resilience.[9]

Challenges in Adapting to DORA Requirements

There's an old saying: no good deed goes unpunished. While the opportunities are significant, ICT Providers face challenges in adapting to DORA's requirements. These include substantial investments in technology and infrastructure, navigating complex regulatory landscapes, and ensuring continuous compliance. ICT Providers must stay alert to evolving threats and regulatory updates. Failing to comply with DORA can lead to hefty penalties, reputational damage, and operational disruptions, similar to a team losing a game due to avoidable errors.[10] Therefore, understanding and adhering to DORA's requirements is a regulatory obligation and a strategic imperative for ICT Providers.

Three Strategies for ICT Providers

1. **Risk Assessments and Compliance Audits:** Conduct regular risk assessments and compliance audits to identify vulnerabilities and ensure adherence to DORA's standards.[11]
2. **Partnerships with Financial Institutions:** Develop strategic partnerships with financial institutions to enhance operational resilience and address shared risks collaboratively.[12]
3. **Continuous Improvement:** Implement a culture of continuous improvement, leveraging feedback and insights to refine resilience strategies and service offerings.[13]

Conclusion

The Digital Operational Resilience Act presents both

[7] Grima, Simon, et al. "The Perceived Effectiveness of Blockchain for Digital Operational Risk Resilience in the European Union Insurance Market Sector." *Journal of Risk and Financial Management*, vol. 14, no. 8, 2021, p. 363

[8] Mike, P., & James M. "Key Themes of Resiliency, Outsourcing and Third-Party Risk Management Regimes." *Journal of Securities Operations & Custody*, 2025

[9] The E.U.'s Digital Operational Resilience Act: Cloud Services & Financial Companies." *Social Science Research Network*, 2021

[10] Derek, D. "The Impact of the Digital Operational Resilience Act on Financial Market Infrastructures in Europe." *Journal of Securities Operations & Custody*, 2024

[11] Eyup, K. "Challenges in Regulating Cloud Service Providers in E.U. Financial Regulation: From Operational to Systemic Risks, and Examining Challenges of the New Oversight Regime for Critical Cloud Service Providers under the Digital Operational Resilience Act." *Computer Law and Security Review*, 2024

[12] S., G., M. K., K. S., & Mehmet E. "The Perceived Effectiveness of Blockchain for Digital Operational Risk Resilience in the European Union Insurance Market Sector." *Journal of Risk and Financial Management*, 2021

[13] Katarzyna, P. "Do Not Get Lost in the Cloud: How E.U. Financial Institutions Could Avoid Problems with Cloud Services Arising under DORA." *Law, Innovation and Technology*, 2024

challenges and opportunities for ICT Providers. By embracing the indirect obligations imposed by DORA, ICT Providers can transform these challenges into growth and innovation opportunities. With enhanced service offerings, strategic partnerships, and a commitment to compliance, ICT Providers can play a pivotal role in strengthening the digital resilience of the financial sector. As the regulatory landscape evolves, proactive engagement with DORA's requirements will be key to unlocking new opportunities and achieving long-term success. Just like in any game, it's about making the right plays at the right moments.

ABOUT THE AUTHOR:

Zandra is a seasoned legal professional with over 10 years of in-house experience at leading companies such as Dell, PepsiCo, and Oracle. Currently serving as Cybersecurity Counsel for Dell Technologies, she specializes in third-party risk management and global cybersecurity incident response. Zandra has a strong track record of navigating complex legal challenges and fostering collaborative environments that drive business success. She has received multiple accolades, including Dell's "Game-Changer Award," and was nominated for the Dallas Women's Lawyer Association's "Outstanding Corporate Counsel" award in 2024.

Passionate about delivering exceptional legal counsel, Zandra firmly believes that our ability to innovate and cultivate breakthrough thinking serves as an engine for growth, success, and progress—not just for our clients, but for the practice of law as a whole.

The Ethical and Transparent Integration of AI Tools and Systems in Legal Writing and Pedagogy: Balancing Innovation with Integrity



Lea Williams

Senior Technology Commercial Transactional, and Privacy Attorney

Artificial intelligence (AI) has rapidly evolved from a futuristic concept into our everyday reality. Though the tech revolution has long been underway, we are now in its transformative phase. The legal profession must either evolve or risk becoming obsolete. Legal education—especially in legal writing and pedagogy—stands at the intersection of this transformation. This article explores ethical implications, administrative challenges, and best practices for responsibly integrating AI into legal education, guided by the standards of the American Bar Association (ABA).

I recently presented on this topic at the 2025 Lone Star Legal Writing Conference at Baylor University School of Law. The reactions were mixed: some attendees were skeptical of AI's role in legal education, while others embraced the relevance and urgency of the discussion. This response underscores a broader question: Should we preserve traditional methods or embrace AI to enhance student analysis and engagement?

Defining AI and Its Role in Legal Education

AI includes a range of technologies that simulate human

intelligence. Key types include generative AI, Generative Adversarial Networks (GANs), and Large Language Models (LLMs). Generative AI analyzes large datasets to produce new content. GANs, composed of a generator and a discriminator, create realistic outputs through competitive learning. LLMs like GPT are capable of generating and understanding complex text.

AI is not a replacement for legal education; it is a tool—an innovation that can elevate legal education when used responsibly. As these tools become embedded in legal research, drafting, and education, it is crucial that educators and practitioners understand both their potential and their limitations. While AI can improve efficiency, it also poses risks—bias, inaccuracy, and overreliance. Keeping human judgment in the loop is a necessary safeguard.

Ethical Frameworks and Standards

Responsible AI integration is not merely beneficial—it is a professional mandate. The ABA Model Rules and Texas Disciplinary Rules of Professional Conduct implicate several ethical duties, including:

- **Rule 1.1** – Competence (including technological competence)
- **Rule 1.6** – Confidentiality
- **Rule 5.3** – Supervision of Nonlawyers
- **Rule 8.4** – Misconduct

Focusing on Rule 1.1, the ABA in 2012 added Comment 8, requiring lawyers to stay abreast of relevant technology and its implications. Texas followed suit in 2019, amending Comment 8 to Rule 1.01 to include similar language. If technological competence has been a professional standard in Texas for over five years, why does resistance persist?

Implications for Legal Writing Instruction

Introducing AI into legal writing classrooms requires intentionality. Professors must teach students to use AI ethically and effectively for tasks like case synthesis, issue spotting, and drafting. Students should verify AI-generated citations, question content for accuracy, and apply independent analytical skills. Uncritical AI reliance can undermine pedagogical goals and violate ethical expectations tied to professional competence.

Implications for Practicing Attorneys

Practicing lawyers using AI in briefs or client communications must meet similar standards. They must validate AI output, understand tool limitations, and maintain confidentiality—especially with public or cloud-based tools. Competent legal practice now includes discerning when and how to use AI tools, always preserving the attorney's judgment and duty of care.



Administrative and Generational Challenges

Institutional challenges accompany pedagogical ones. Legal educators must incorporate AI literacy into curricula while addressing the risks of bias, factual error, and data misuse. Failing to prepare students for the technological realities of practice jeopardizes the future of legal education.

Further complicating implementation is the generational diversity among faculty and students. While many baby boomers may prefer traditional methods, Gen Z and Gen Alpha are generally tech-native. Administrators and faculty must build bridges across these divides through inclusive design,

communication, and professional development.

Transparency and Integrity in AI Integration

Maintaining academic integrity requires clear rules for AI use. Institutions should adopt policies requiring students to disclose and cite AI tools used in their work. Faculty should model transparent AI usage and engage students in critically evaluating AI outputs.

Additionally, schools must address equity. Not all students have equal access to paid AI tools, creating potential disparities. Institutions should consider access and affordability when designing AI-integrated classrooms.

Encouraging Innovation, Not Stagnation

Innovation in legal education must not come at the expense of analytical rigor. AI literacy is a core legal skill, and institutions must treat it as such. To ensure thoughtful integration, law schools should:

- Include AI use guidelines in course syllabi
- Require students to cite AI tools when used
- Define unauthorized use as academic misconduct
- Encourage AI use for brainstorming and revision—not as a substitute for legal reasoning

Law schools should also expand their course offerings to reflect today's legal landscape. Topics like contract negotiation in tech industries, data privacy, intellectual property in generative systems, and AI-related antitrust litigation are increasingly relevant. A modern curriculum helps law students remain competitive globally.

The Only Constant is Change

As legal educators, our task is not simply to preserve tradition, but to prepare students for a future in which AI is ubiquitous. AI technologies offer extraordinary opportunities for transformation, but require ethical guardrails, critical scrutiny, and a commitment to continuous learning.

Educators must lead this effort with strategic policies, ethical clarity, and collaborative leadership. Innovation should strengthen—not undermine—the foundational integrity of legal education. Ultimately, our responsibility is to elevate the next generation of lawyers, equipping them with the skills and judgment to thrive in a rapidly changing world.

ABOUT THE AUTHOR:

Lea Williams is a Senior Corporate Privacy and Transactional Lead Counsel with over 12 years of experience in sectors such as technology, finance, healthcare, and energy. Currently, she advises companies on privacy compliance and AI-driven contracts. Additionally, she serves as a Visiting Professor at Texas Southern University's Thurgood Marshall School of Law. Williams earned a Bachelor of Arts from the University of North Carolina at Chapel Hill and a Juris Doctor from SMU Dedman School of Law.

Simple AI for Lawyers



Robert Ray

Artificial Intelligence (AI) is useful but can be complicated. It is a tremendous tool for lawyers and others, provided you learn how to use it effectively and design your prompts properly. Crafting effective prompts can be challenging. With the proper prompt, AI can save significant time that lawyers desperately need.

However, AI can also be simple. I want to share with you a recent, simple example of its application, and how it saved me time, not much time, but time, nonetheless.

I don't normally do appeals, but I was involved in one, and we had just prevailed. I was out of the office, waiting for something, and I thought about the case, wondering how long the other side would have to ask for a rehearing. I pulled out my phone and asked ChatGPT, "In the Texas Court of Appeals, once it makes a decision, how long does the party have to ask for a rehearing?"

ChatGPT responded that there is a 15-day time limit for requesting a rehearing and cited TRAP Rule 49.1. I asked it to show me TRAP Rule 49.1, which it did. (I later confirmed that it has cited it correctly.)

While I was reading its response, ChatGPT asked me if I wanted it to prepare a draft motion for rehearing. I had not specified that I was asking for our side or the other side. So, I told it, yes, give me a draft motion for rehearing, and it did.

I did not need a motion for rehearing, but if I did, would I file the draft without confirming it was

correct? No. However, I had a form book outline of a motion, which I could use if I were inclined to do so.

While ChatGPT did not save me a lot of time, it did save me some time and answered a question I had on a case that I would have spent time researching back in my office. It was a simple use of AI, one that encourages you to use AI more and more, and it may transform your practice. So, start simple and gradually add more AI to your practice.

The entire discussion with ChatGPT is copied below, in its original, unformatted form.

In the Texas Court of Appeals, once it makes a decision, how long does the party have to ask for a rehearing?

[ChatGPT]

In the **Texas Court of Appeals**, a party generally has **15 days** from the date of the court's judgment or order to file a **motion for rehearing**. This is governed by **Texas Rule of Appellate Procedure 49.1**.

If a party needs more time, they may file a **motion for extension of time**, but it must be filed **within 15 days of the original deadline** under **Rule 49.8**.

Would you like any details on the requirements for a motion for rehearing?

[Me]

Can you show me Texas Rules of Appellate Procedure 49.1?

[ChatGPT]

Certainly. Here is the text of **Texas Rule of Appellate Procedure 49.1**:

1. Texas Rule of Appellate Procedure 49.1 – Motion for Rehearing

A motion for rehearing may be filed within 15 days after the court of appeals' judgment or order is rendered. The motion must clearly state the points

relied on for the rehearing. No response to a motion for rehearing need be filed unless the court so requests. A motion will not be granted unless a response has been requested or the court is acting on its own initiative.

This rule establishes the 15-day deadline for filing a motion for rehearing, requires that the motion specify the reasons for rehearing, and notes that no response is required unless requested by the court.

Would you like additional details on filing procedures or strategic considerations?

[Me]

Yes.

[ChatGPT]

2. Strategic Considerations and Filing Procedures for a Motion for Rehearing in the Texas Court of Appeals

i. 1. Timing and Deadlines

- The motion for rehearing must be filed **within 15 days** after the appellate court's judgment or order is rendered (**Tex. R. App. P. 49.1**).
- If more time is needed, a **motion for extension of time** can be filed, but it must be submitted **within 15 days of the original deadline** (**Tex. R. App. P. 49.8**).

ii. 2. Key Requirements for the Motion

- The motion must **clearly state the points relied on for rehearing**, explaining why the appellate court's decision was incorrect.
- It should focus on **errors of law or fact**, highlighting issues the court may have overlooked or misapplied.
- No response from the opposing party is required unless the court **requests one**.
- The motion is **rarely granted** unless the court believes it made a significant error.

iii. 3. Strategic Considerations

- **Identify Legal or Factual Errors:** A strong motion should focus on a **material mistake of law or fact**. If the court correctly applied the law to the

undisputed facts, a rehearing is unlikely to succeed.

- **Cite Precedent and Persuasive Authority:** Referencing binding case law or persuasive authority can strengthen your argument.
 - **Avoid Repeating Arguments:** The motion should not simply rehash arguments already made in the appellate briefs. Instead, it should highlight **new aspects** or **misinterpretations** by the court.
 - **Consider En Banc Rehearing:** If the case involves an important legal issue, you may also consider filing a **motion for en banc reconsideration** under **Tex. R. App. P. 49.7**, requesting that the entire panel of appellate judges review the case.
- #### iv.4. Practical Steps for Filing
- **Draft the Motion:** Clearly articulate the specific reasons for rehearing.
 - **File Electronically:** Most Texas courts of appeals require electronic filing through **eFileTexas.gov**.
 - **Monitor for Court Response:** The court may either **deny the motion outright** or request a response from the opposing party.
 - **Prepare for Further Action:** If the motion is denied, consider whether to file a **petition for review with the Texas Supreme Court**.

Would you like assistance in drafting a motion for rehearing or reviewing specific case law that could support one?

[Me] Yes

[ChatGPT]

To draft a strong **Motion for Rehearing** in the Texas Court of Appeals, we should focus on legal and factual errors in the court's opinion. Below is a **template** you can modify based on your case. If you provide specific details about the court's ruling and the grounds for rehearing, I can refine this further.

1. NO. [Case Number]

IN THE [X] COURT OF APPEALS
FOR THE [X] DISTRICT OF TEXAS
AT [CITY]

[Appellant/Petitioner's Name],

Appellant,

v.
 [Appellee/Respondent's Name],
 Appellee.
 On Appeal from the [Trial Court Name]
 [Trial Court Case Number]

1. MOTION FOR REHEARING TO THE HONORABLE JUSTICES OF THE [X] COURT OF APPEALS:

Pursuant to Texas Rule of Appellate Procedure 49.1, [Appellant's Name] files this Motion for Rehearing and respectfully requests that the Court reconsider its [Date] opinion because it contains [legal errors, factual errors, or misapplications of law] that warrant correction.

3. I. INTRODUCTION

This Court's opinion, issued on [Date], affirms/reverses the lower court's judgment. However, in reaching its decision, the Court **overlooked** or **misapplied** key legal principles/factual findings that materially affect the outcome.

The Court's ruling is inconsistent with [relevant Texas Supreme Court precedent, statutory law, or conflicting appellate decisions].

Specifically, the Court:

1. [Error #1 – Misinterpretation of Law] – The Court incorrectly applied [statute or case law], which should be interpreted as [correct interpretation].

2. [Error #2 – Factual Misstatement] – The Court's opinion states that [incorrect fact or finding], but the record demonstrates [correct fact].

3. [Error #3 – Overlooked Argument] – The Court failed to address [important argument or key legal principle], which is crucial because [reason].

Because these errors materially impact the Court's decision, a rehearing is warranted.

4. II. LEGAL ERRORS WARRANTING REHEARING

The Court's ruling conflicts with established precedent and misapplies controlling law. Specifically:

1. **Misapplication of [Statute or Case Law]**
 The Court's interpretation of [statute or case law] is

inconsistent with [Texas Supreme Court decision or binding authority]. In [Case Name, Citation], the Texas Supreme Court held that [relevant holding]. This Court's ruling contradicts that precedent by [explain how the ruling deviates].

2. Misstatement or Mischaracterization of the Record

The Court's opinion [misstates a key fact or misinterprets trial evidence] by concluding that [erroneous statement from the opinion], whereas the record actually reflects [correct fact from trial evidence]. This factual error substantially affects the Court's legal reasoning and ultimate judgment.

3. Failure to Address a Critical Argument

This Court did not consider [an important argument presented in briefing], which, if properly analyzed, would have led to a different conclusion. Under [cite relevant authority], the correct analysis should have been [explanation of proper legal reasoning].

5. III. CONCLUSION AND PRAYER

For the foregoing reasons, [Appellant's Name] respectfully requests that this Court **grant rehearing, reconsider its opinion, and issue a new opinion correcting the identified errors.** Alternatively, Appellant requests that the Court **request a response from Appellee and set the matter for further review.**

Respectfully submitted,

[Your Name]

[Your Law Firm Name]

[Your Address]

[Your Phone Number]

[Your Email]

Attorney for [Appellant's Name]

6. Certificate of Compliance

I certify that this document complies with the word count and formatting requirements of Texas Rule of Appellate Procedure 9.4.

[Your Name]

7. Certificate of Service

I certify that a true and correct copy of this **Motion for Rehearing** was served on all counsel of record via

[e-file, email, or mail] on [Date], in accordance with Texas Rule of Appellate Procedure 9.5.
[Your Name]

8. Next Steps

1. Tailor the Motion: If you provide the specific legal issue and the court's ruling, I can refine this with stronger arguments.
2. Case Law Research: If you need supporting Texas Supreme Court or appellate precedent, I can help find and cite relevant cases.
3. Filing & Deadlines: Ensure you file within 15 days of the appellate opinion and check the court's local rules for any additional requirements.
4. Would you like help drafting case-specific arguments or researching precedent?

ABOUT THE AUTHOR:

Robert Ray practices throughout Texas from his DFW area base and limits his practice to probate and inheritance litigation. A graduate of SMU Law School, Robert has served as past chair of the State Bar of Texas Computer & Technology Section. The Chief Justice appointed him as an ex-officio member of the Texas Supreme Court's Judicial Committee on Information Technology. He is Board Certified in Personal Injury Trial Law.

Genius Act

On February 4, 2025, the Guiding and Establishing National Innovation for U.S. Stablecoins Act, Senate Bill 394, (the “Genius Act”) was introduced in the Senate. Then on May 20, 2025, the Senate voted to advance the bill, which was then advanced by a vote of 66–32. As of this writing, the bill is currently in the 119th Congress (2025–2026) and is still under consideration.

This bipartisan legislation aims to establish a comprehensive federal framework for the regulation of payment stablecoins, which is a type of digital asset that is pegged to a reserve asset. It sets standards for reserve backing, audits, disclosures, and compliance with anti-money laundering laws. The Act also clarifies that payment stablecoins issued by permitted issuers are not considered securities or commodities under existing federal laws, thereby delineating regulatory responsibilities among agencies like the SEC and CFTC. The GENIUS Act is designed to take effect either 18 months after its enactment or 120 days following the issuance of final implementing regulations by federal banking regulators, whichever comes first.

Legally, the GENIUS Act imposes stringent requirements on stablecoin issuers, mandating that only entities meeting specific criteria—such as insured depository institutions or those granted a federal license—can issue payment stablecoins. It also prohibits non-financial publicly traded companies from issuing stablecoins unless they satisfy rigorous standards related to financial risk management, consumer data privacy, and equitable business practices. Additionally, the Act empowers the U.S. Treasury Secretary to grant “safe harbor” exceptions to certain issuers under extraordinary circumstances, provided that such exceptions are justified to the Senate Banking Committee and House Financial Services Committee. These provisions aim to balance innovation in the digital currency space with the need for financial stability and consumer protection.

The GENIUS Act is an important regulatory development because it clarifies a lot of the current legal uncertainty. Such regulatory clarity will bring back the

fintech ecosystem and innovation to US, which were previously driven to other jurisdictions with more accommodating laws. As a result, the GENIUS Act will open markets to US Treasuries while protecting the US Dollar as the world's leading reserve currency.

Texas Cyber Command

On June 2, 2024, Governor Greg Abbott signed Texas House Bill 150 (89th Legislature), the Texas Cyber Command (the “TCC”), into law and it will take effect on September 1, 2025. This bill establishes the Texas Cyber Command and transfers certain powers and duties of the Department of Information Resources to it.

The Texas Cyber Command (TCC) creates the largest state-based cybersecurity department in America and will be a component of the University of Texas System, located at the University of Texas at San Antonio (UTSA). To address the shortage of cybersecurity investment at the state and local levels, the TCC now deploys a \$135M investment from the State of Texas.

The TCC is tasked with preventing and responding to the prevalent cybersecurity attacks from foreign and domestic threat actors that are attempting to disrupt and cripple state agencies, local governments, and critical infrastructure. Its responsibilities include developing cybersecurity best practices and minimum standards, providing training to governmental entities, and administering a cybersecurity threat intelligence center and a digital forensics laboratory.

The TCC mandates that all elected or appointed officials and employees of local governmental entities with access to information resources complete annual state-certified cybersecurity training. Entities must verify and report compliance to the TCC and may deny access to information resources for non-compliant individuals. The TCC also assumes certain powers and duties previously held by the Department of Information Resources, positioning it as the state's primary cybersecurity authority. The command is subject to the Texas Sunset

Act and is scheduled for review and potential abolition on September 1, 2035, unless continued by the legislature.



Aaron Woo

ABOUT THE AUTHOR:

Aaron Woo is a partner at Vanguard Legal, PLLC. Aaron is business and technology attorney in Texas and represents a variety of emerging technology companies and investors throughout the Southwest. As a strong proponent of entrepreneurship, he advises emerging technology companies from startup through acquisition by developing IP strategy, implementing business development objectives, and obtaining the necessary financing to position businesses for growth.