COMPUTER AND TECHNOLOGY SECTION

Circuits

e-Journal of the Computer & Technology Section
of the State Bar of Texas
May 2022

Table of Contents

Featured Articles

Short Circuits

Table of Contents

Feature Articles:-

Short Circuits:-

Letter from the Chair

By Elizabeth C. Rogers

On behalf of the Council of the Computer and Technology Law Section of the State Bar of Texas, I hope this issue of *Circuits* finds you and your families healthy and thriving. We are now entering the 2nd quarter of the Chinese "Year of the Tiger". The 'Tiger', as a spirit animal is said to be a symbol of courage and personal strength. In the first quarter of this year, we have continued to draw on these skills, like we have since the beginning of the Bar year, to re-connect, renew and invigorate our business and social relationships. For the first time December of 2019, we have had 4 in-person meetings as a Council. In 2021, we met in August and December. And, since my last Chair's letter, we met for our Annual "*And Justice for All,*" with several in-person speakers and council members, in the State Bar Building on February 11, 2022 and at the San Antonio JW Marriott Hotel & Conference Center for our Annual Spring Retreat on April 7, 2022.

This year's *And Justice for All* CLE focused on the real notion that because remote lawyering and hybrid client meetings are here to stay, there is a critical need to become competent in our knowledge of the risks and benefits of the of technology. (Comment 8, Rule 1.01, Texas Disciplinary Rules of Professional Conduct). So, our subject matter experts provided the audience with a breadth and depth of technical and legal awareness that transposed to practical takeaways about applicable standards of security and how to establish and maintain them. Thanks to everyone on the staff of the State Bar, including Tracy Nuckols, William Korn and many others who were onsite with us in the building and who helped us to deliver the State Bar's first ever high quality hybrid CLE!

Our annual retreat is usually built around a theme that will enlighten and educate all council members about a trending issue involving legal technology or legal technology resources that we can, in turn, pass on to our members and the greater Bar membership. In 2020 and in 2021 we had hoped to have a retreat in and around Cupertino, CA to visit the headquarter campuses of some of the tech giants and a university technology scholars. Alas, we defaulted to the JW Marriott San Antonio Hill Country Resort and Spa and for the first time in three years, had an *in person* gathering of 17 of our Council's members!!! Our agenda included some focused discussion on the format of our annual And, Justice for All CLE, going forward as well as a robust conversation of the future of this publication. Stay tuned for some practical tweaks to these classic traditions of our section over the next bar year. As we have done in the last 3 hybrid meetings, we hosted a guest but this time, it was a surprise. Rod Ponton, Presidio

County Attorney, a/k/a, “the Cat Lawyer” showed up for a stirring discussion that gave us pause about being filter savvy before a hearing!

We are excited to participate in the *in*-person State Bar Annual Meeting that will be in Houston, this year. When you register to attend, please be sure to register for our 60 Apps in 60 minutes presentations on Thursday afternoon and Friday morning. We are arranging for members to renew and new section members to join on site!

By the time the next issue of the Circuits, we will have four new members of the Council and a new slate of officers to lead you in the next bar year of 2022-2023. It has been a professional and a personal pleasure to serve you and to work with all of the brilliant and friendly members of the Council who have treated me like family.

In closing, please know how much we value your membership in the Computer & Technology Section of the State Bar of Texas. The time to renew your membership is rapidly approaching. We welcome you back with open arms and invite you to encourage your colleagues to join as well!

As always, we welcome your feedback about what are your expectations and what we can do to improve your benefits at any point in time. We also welcome your participation on any of our working groups or committees without needing to be a member of the Council. Please reach out to me if you have any interest or thoughts. Until our next issue, I hope to see you at the annual meeting!!

Respectfully,

Elizabeth C. Rogers
2021-2022 Chair
Computer & Technology Section
State Bar of Texas

COMPUTER AND TECHNOLOGY SECTION

Letter from the Editor

By Sanjeev Kumar

Welcome to the first issue of *Circuits* for the 2022-23 Bar year! After a brief hiatus as Editor of *Circuits*, it is good to be back with you all.

Getting right to business, in our Feature Articles, we start with a contribution from the Honorable Xavier Rodriguez and Antony P. Ng highlighting a few recent cases where parties and/or counsel were sanctioned for improper conduct during discovery, reminding us all of the very real duties we owe to our clients, opposing counsel, and the court to comply with the Federal Rules and ethical code in eDiscovery.

The next Feature Article is penned by Amy C. Falcon, who discusses the capabilities — and limits — of artificial intelligence as an adjudicator. While we may be seeing an uptick in "AI judges" used for small claims with repetitive facts and issues, Falcon describes why we are still a far cry from seeing AI judges ruling in complex civil litigation.

Guest writer Chris Castle next walks us through one of the things that have been all the rage lately: Non-Fungible Tokens. What are they, are they considered "securities" per the SEC, and what does that mean for the legal practitioner or layperson looking to get in the NFT game? Chris lays out the basics for us.

In the final Feature Article, Grant M. Scheiner provides us with a comprehensive summary on *United States v. Cheng*, a recent 2022 opinion from the Southern District of Texas that invoked the "inevitable discovery doctrine" to hold that cell phone evidence obtained from an illegal FBI interrogation was, in fact, admissible. Scheiner's article walks us through an interesting thought experiment in the scope of 4th and 5th Amendment protection of rights and poses the question: may application of those rights with respect to cell phone data hinge on whether the accused uses a numerical passcode versus a fingerprint or face scan?

Our Short Circuits kick off with a contribution from longtime *Circuits* contributor Pierre Grosdidier providing a further discussion on 4th Amendment rights, this time with respect to evidence obtained from camera surveillance. Grosdidier explains that the Seventh Circuit's recent opinion in *United States v. Tuggle* may make some individuals give more thought to just how much privacy they have behind the four walls of their home.

In the next Short Circuit, we have a familiar face adding to Judge Rodriguez's and Ng's articles on eDiscovery sanctions. Craig Ball provides a detailed explanation of the effects of the 2015

amendment to Fed. R. Civ. P. 37(e) through the lens of *Kristin Fast v. Godady.com LLC et al.*, a February 2022 case from the District of Arizona. Indeed, there is still much room for learning about the pitfalls of eDiscovery wrongdoing across the legal industry.

In Grosdidier's second Short Circuit for this issue of *Circuits*, he discusses a recent Texas Supreme Court case upholding the validity of plaintiff's digital signatures on an arbitration agreement they claimed they had never seen before and the broader trend we have been seeing toward the acceptance of digital signatures. Think before you click, folks.

When is a website simply a publisher of third-party content, and when is it a content-provider? In our final Short Circuit, Shelby Menard provides an overview of the presiding test and highlights a recent ruling in an Alabama district court that Pornhub is a content-provider within the meaning of the Communications Decency Act and is therefore not shielded from liability for acts related to the trafficking of persons.

Many thanks to all the contributors, new and old, to this issue. Thanks to Kirsten Kumar for her review of and assistance with this issue's articles.

We hope that you enjoy this new issue of *Circuits* and as always, we welcome any comments that you may have. The accomplished members of the Computer & Technology Section Council are always willing to help in any way possible. Please do not hesitate to contact us, be it a comment or a request for assistance, through our section administrator at admin@sbot.org.

Kind Regards,
Sanjeev Kumar, Editor

Electronic Discovery Related Sanctions in Federal Courts

By Xavier Rodriguez and Antony P. Ng

There are many sanction options at a court's disposal to address various electronic discovery related mischiefs.

I. Sanctions under Fed. R. Civ. P. Rule 16(f)

A court may issue sanctions against a party (or its attorney) if the party fails to appear at a scheduling or other pretrial conference. A court may issue sanctions even if the party is substantially unprepared to participate in the pretrial conference.

II. Sanctions under Fed. R. Civ. P. Rule 26(g)

By signing a discovery request or response, an attorney certifies that the discovery request or response is complete and correct as of the time it is made, and that the discovery request or response is consistent with the various requirements under Rule 26(g). Thus, if a certification violates Rule 26(g) without substantial justification, the court must impose an appropriate sanction on the signer, the party on whose behalf the signer was acting, or both.

In some cases, the court may just impose Rule 26(g)(3) sanctions on the party only, and not the party's counsel.

III. Sanctions under Fed. R. Civ. P. Rule 37(a)

If a party fails to make a disclosure required by Rule 26(a), any other party may move for appropriate sanctions. A party seeking discovery may move for an order compelling production. This motion may be made if a party fails to produce documents as requested under Rule 34.

Thus, in addition to sanctions under Rule 26(g), as mentioned above, a court may also issue sanctions under Rule 37(a) when the document productions were incomplete.

IV. Sanctions under Fed. R. Civ. P. Rule 37(b)

When a court orders the production of certain documents, and representations are made to the court that no additional documents existed, but additional documents are later found, the court may issue sanctions under Rule 37(b).

V. Sanctions under Fed. R. Civ. P. 37(e)

Precatory introduction

In order for Rule 37(e) sanctions to apply, all the elements of the precatory introduction (*i.e.*, ESI that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and the lost ESI cannot be restored or replaced through additional discovery) must be established initially.

Two modes of culpability

Rule 37(e) explicitly enumerates two separate modes of culpability, *i.e.*, party prejudiced and intent to deprive. After all elements of the precatory introduction have been satisfied, at least one of the two modes of culpability has to be found by a court in order for the court to impose Rule 37(e) sanctions. With two modes of culpability, there are four possible scenarios, as follows:

– Scenario 1 –

If no party is prejudiced, and there is no intent to deprive, then no sanction will be applied.

– Scenario 2 –

If a party is prejudiced, but there is no intent to deprive the party, then Rule 37(e)(1) is applicable.

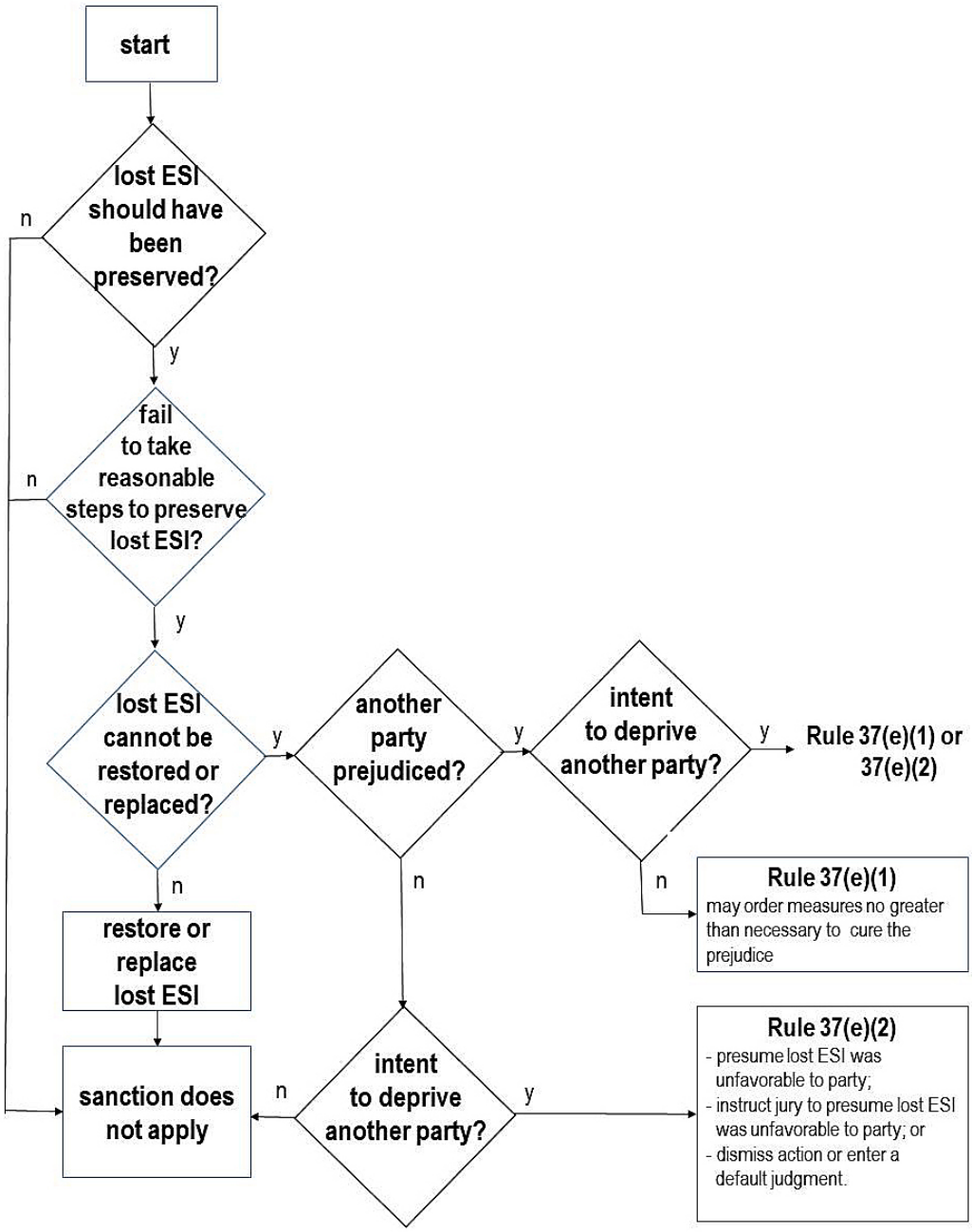
– Scenario 3 –

If there is an intent to deprive a party, but the party is not prejudiced, then Rule 37(e)(2) is applicable.

– Scenario 4 –

If there is an intent to deprive the party, and the party is prejudiced, then either Rule 37(e)(1) or Rule 37(e)(2) is applicable.

The above-mentioned precatory introduction and four scenarios can be better illustrated in the following flowchart.



Basically, a court may impose sanctions under Rule 37(e)(1) if the court has found that a party has been prejudiced, but there is no intent to deprive the party. Alternatively, a court may impose sanctions under Rule 37(e)(2) if the court has found that there is an intent to deprive a party even though the party has not been prejudiced. However, if a court has found that there is an intent to deprive the party and the party has been prejudiced, then the court may impose sanctions under Rule 37(e)(1) or Rule 37(e)(2), but not both.

Rule 37(e)(1)

When electronically stored information (ESI) is lost due to the negligence or gross negligence of a party, Rule 37(e)(1) permits only the imposition of sanctions that are "no greater than necessary to cure the prejudice." According to the Advisory Committee's note to the 2015 amendment, the choice of which measures to employ takes into account the "importance of the information of the lost information to claims and defenses in the litigation." The prejudice to plaintiff includes (but is not limited to) engaging in "months of fact discovery trying to recover" documents that defendants failed to preserve, preparing for depositions without electronically stored documents, and loss of goodwill with plaintiff's "current and potential customers who are being pulled into this litigation."

Courts appear to be limiting severe sanctions, but nevertheless are still issuing some form of adverse jury instructions in cases involving negligent spoliation.

Rule 37(e)(2)

Although some courts have required explicit evidence of willful spoliation before issuing sanctions under Rule 37(e)(2), other courts have reasoned that "intent to deprive" can be established through circumstantial evidence.

VI. Sanction under 28 U.S.C. § 1927

Any attorney admitted to conduct cases in any court of the United States who so multiplies the proceedings in any case unreasonably and vexatiously may be required by the court to satisfy personally the excess costs, expenses, and attorneys' fees reasonably incurred because of such conduct.

In *Rossbach v. Montefiore Med. Ctr.*[1], the evidence at an evidentiary hearing conclusively demonstrated that the alleged sexually harassing image was not of text messages received on an iPhone 5, that it was not a photograph taken by an iPhone X, that the image is not an authentic representation of how text messages received on an iPhone would be displayed, and that the image was not even a photograph. There were also clear and convincing evidence indicating that Rossbach had fabricated the image and engaged in perjury and spoliation to prevent discovery of that fabrication. With regard to counsel, the court stated that attorney Altaras had failed to take reasonable steps to preserve critical evidence and failed to recognize the gravity of his client's misconduct and its implications for his own duties, and that he had

[1] No. 19-CV-5758 (DLC), 2021 WL 3421569, at *10 (S.D.N.Y. Aug. 5, 2021).

burdened the defendants and the court by suborning his client's perjury and making frivolous and procedurally improper legal and factual arguments. Thus, the court issued a monetary sanction against Altaras and Rossbach under 28 U.S.C. § 1927 and its inherent power.

VII. Sanctions based on Court's Inherent Authority

Some courts take the view that the issuance of sanctions can only be based on a specific statutory rule. For example, in *Alsadi v. Intel Corp.*[2], the court stated that Rule 37(e) was the exclusive authority for sanctions that can be imposed for the loss of ESI. However, other courts maintain that they possess inherent authority to sanction a party or counsel independent of any rule. *See Estate of Moreno v. Corr. Healthcare Co.*[3]

By taking a middle-ground approach, some courts only employ inherent authority as a "gap filler" for circumstances not contemplated by statutes.

Courts have also issued harsh sanctions apart from Rule 37(e) when there is a finding of persistent non-compliance with discovery rules and/or failure to comply with court orders. For example, in *State Farm Mut., Auto. Ins. Co. v. Max Rehab Physical Therapy, LLC*[4], the court found that defendants' approach to their discovery obligations to be "dismissive and cavalier, and likely intentionally obstructive." The court also found that defendants' persistent non-compliance with discovery rules and the orders to enforce them as "willful bad faith." Thus, the court adopted the magistrate judge's recommendation of default judgment to be entered against the defendants.

Role of the Jury

Although Rule 37(e)(2) contemplates that adverse jury instructions are only proper when intent to deprive has been established, the Advisory Committee Note addressing Rule 37(e)(1) states:

> "In an appropriate case, it may be that serious measures are necessary to cure prejudice found by the court, such as forbidding the party that failed to preserve information from putting on certain evidence, permitting the parties to present evidence and argument to the jury regarding the loss of information, or giving the jury instructions to assist in its evaluation of such evidence or argument, other than instructions to which subdivision (e)(2) applies. Care must be taken,

---

2 No. CV-16-03738-PHX-DGC, 2020 WL 4035169 (D. Ariz. July 17, 2020).

3 No: 4:18-CV-5171, 2020 WL 5740265 (E.D. Wash. June 1, 2020).

4 No. CV 18-13257, 2021 WL 2843832, at *4 (E.D. Mich. June 28, 2021), *report and recommendation adopted*, No. CV 18-13257, 2021 WL 3930133 (E.D. Mich. Sep. 2, 2021).

> however, to ensure that curative measures under subdivision (e)(1) do not have the effect of measures that are permitted under subdivision (e)(2) only on a finding of intent to deprive another party of the lost information's use in the litigation."

Some courts have issued adverse inference instructions in Rule 37(e)(1) settings. This is likely to be the case as courts consider which evidentiary matters can be properly placed before the jury.

Under federal law there are two sources of authority under which a district court can sanction a party who has despoiled evidence: the inherent power of federal courts to levy sanctions in response to abusive litigation practices, and the availability of sanctions under Rule 37. "In the Court's view, this underscores why judges, not juries, should be the ones deciding whether to impose spoliation sanctions. It seems fairly self-evident that questions pertaining to how judges should exercise their inherent authority are not jury issues. Similarly, when a party seeks sanctions or other types of relief under Rule 37, the judge acts as the factfinder concerning any underlying factual disputes." "Admittedly, '[t]here is inconsistency in how courts deal with the division of fact-finding labor in spoliation cases.' Specifically, although the court 'makes the findings of fact necessary to reach a conclusion on the spoliation issue, 'because [t]hat practice follows the usual rule that the court, rather than a jury, is responsible for finding facts on a motion for sanctions, 'some courts go further and permit the jurors to re-assess the evidence and determine whether, in their judgment, spoliation has occurred at all.' The Court is not convinced that such reassessment by the jury is ever necessary or appropriate. Judges are fully capable of making discovery-related factual findings. Moreover, presenting spoliation-related factual disputes to juries creates a high risk of confusion and prejudice." *Mannion v. Ameri-Can Freight Sys. Inc.*[5].

About the Authors

Judge Xavier Rodriguez serves as a United States District Judge in the Western District of Texas and is a judicial appointee of the Computer and Technology Section.

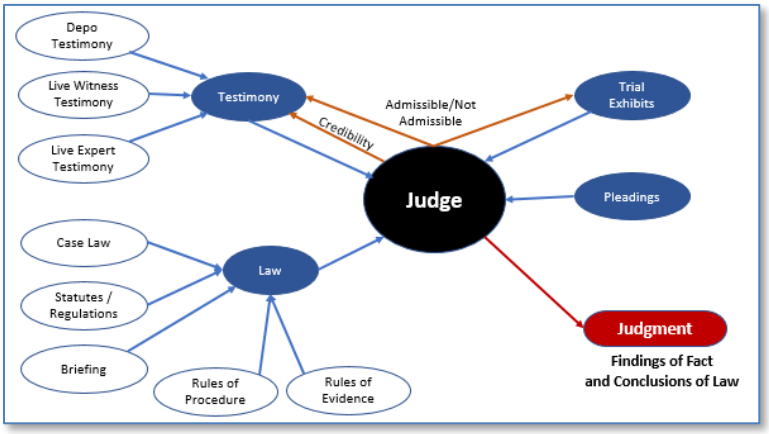
Antony P. Ng is a patent attorney and adjunct professor. He practices in various areas of intellectual property law in Austin, Texas.

[5] No. CV-17-03262-PHX-DWL, 2020 WL 417492, at *45 (D. Ariz. Jan. 27, 2020).

The AI Judge Will Hear Your Case Now

By Amy C. Falcon

Artificial Intelligence. Bill Gates, billionaire founder of Microsoft, has said the power of artificial intelligence—that is, "the capability of a machine to imitate intelligent human behavior"[1] or to replicate human thinking[2]—is "so incredible, it will change society in some very deep ways."[3] Could that include civil litigation? In civil litigation, the human judge takes the parties' arguments and proffered evidence, makes evidentiary rulings, and considers case law "peer pressure" (i.e., stare decisis) to make rulings and issue judgments.[4]



Can AI's power be harnessed to duplicate these cognitive processes and create an AI Judge who decides a case? In brief, yes AI can, but only to a limited extent.

In Hangzhou, China, an AI Judge presides over the Internet Court, which is the forum for disputes arising from online transactions, copyright and trademark, ownership and

---

1 *Artificial Intelligence*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/artificial%20intelligence (last visited May 26, 2021).

2 Dan Sincavage, *How Artificial Intelligence Will Change Decision-Making for Business*, BUSINESS2COMMUNITY (Aug. 24, 2017), https://www.business2community.com/business-innovation/artificial-intelligence-will-change-decision-making-businesses-01901048.

3 Catherine Clifford, *Bill Gates: A.I. is Like Nuclear Energy – 'Both Promising and Dangerous'*, CNBC (Mar. 26, 2019, 8:45 AM), https://www.cnbc.com/2019/03/26/bill-gates-artificial-intelligence-both-promising-and-dangerous.html.

4 Because an AI jury is unlikely, as an AI cannot be the peer of a human, this article is limited to considering the AI Judge ruling on motions or acting as the arbiter of the facts and law in a bench trial.

infringement of domains, trade disputes, and e-commerce product liability claims.[5] The cases rely primarily on blockchain evidence, which makes the facts and legal issues fairly consistent from case to case.[6] The parties upload documents. The AI Judge then leads them through various questions to decide the case.[7] Chinese litigants seem happy with the AI Judge; it resolved more than 3.1 million cases from March to October 2019.[8] Estonia plans to implement an AI Judge to adjudicate small claims.[9] Similar to China's AI Judge, the parties will upload documents and other information. The AI Judge will issue a decision—that is reviewable by a human judge.[10] These cases are a far cry from a complex civil case involving multiple witnesses and thousands of exhibits.

These AI Judges use weak AI, which is not advanced sufficiently to duplicate the human judge's cognitive processes in deciding a complex case and explaining the decision.[11] Weak AI (like Siri, Alexa, and Google) [12] uses algorithms that enable the AI to act, process, data, and make decisions to accomplish a specific task, rather than cognitive reasoning.[13] Weak AI is driven by mountains of data that is used to "train" the AI to do a particular task. Thousands of photographs can train an AI to distinguish pandas from koalas.[14] However, once an AI learns a particular task, unlike a human, it cannot adapt how it learned to do that task to doing even a similar task that involves something it does not "know" about. "Machine-learning systems can

---

5 Santosh Paul, *Will Artificial Intelligence replace Judging?*, BAR AND BENCH (May 28, 2020), https://www.barandbench.com/columns/is-artificial-intelligence-replacing-judging.

6 *Id.*

7 *Id.*; Julie Celestial, *China Unveils Digital Courts with AI Judges and Verdicts Via Apps*, THE WATCHERS (Dec. 25, 2019), https://watchers.news/2019/12/25/china-unveils-digital-courts-with-ai-judges-and-verdicts-via-apps/ (see video of AI judge in action).

8 Paul, *supra* note 5.

9 Stephen Hoffman, *AI Judges: Can A Good Judge Be Artificially Intelligent?*, LAW OFFICE OF STEPHEN L. HOFFMAN LLC (April 11, 2019), https://www.hofflawyer.com/general/2019/04/11/ai-judges/.

10 *Id.*

11 Bernard Marr, *What Is the Difference Between Weak (Narrow) and Strong (General) Artificial Intelligence (AI)?,* BERNARD MARR & CO., https://bernardmarr.com/default.asp?contentID=2194 (last visited June 27, 2021) [hereinafter Marr *Weak-Strong* Post].

12 Bernard Marr, *What is Weak (Narrow) AI? Here Are 8 Practical Examples*, BERNARD MARR & CO., https://bernardmarr.com/default.asp?contentID=2198 (last visited June 27, 2021) [hereinafter Marr *Weak* Post]; Andrew Davies, *Artificial Intelligence and the Legal Industry*, LEGALFUTURES (May 2, 2019), https://www.legalfutures.co.uk/blog/artificial-intelligence-and-the-legal-industry.

13 Marr *Weak* Post, *supra* note 12.

14 *See, e.g.,* Lauri Donahue, *A Primer on Using Artificial Intelligence in the Legal Profession*, HARV. J. OF L. & TECH. (2018), https://jolt.law.harvard.edu/digest/a-primer-on-using-artificial-intelligence-in-the-legal-profession.

be duped or confounded by situations they haven't seen before. A self-driving car gets flummoxed by a scenario that a human driver could handle easily."[15] These types of tasks are child's play for a human, but not the current weak AIs. In contrast, strong AI, or "general AI," thinks like a human and sets out to perform any task it envisions.[16] True strong AI doesn't exist yet.[17]

The China Internet Court and the planned Estonia Small Claims AI Judge have two things in common that allow their weak AI to operate: they focus on a narrow slice of cases and the facts and issues are straightforward and repeated. Together, these characteristics continually yield additional relevant data for the AI Judge to learn from for each new case brought before it. This is the kind of "big data" AI needs to operate and learn. And because the AIs that decide the cases—and the cases themselves—are not that complex, it also means "explainability"—"machine learning techniques that make it possible for the human users to understand, appropriately trust, and effectively manage AI"[18]—and therefore trust the AI judge, is likely possible.

In contrast, explainability in a complex civil case is far more challenging. The AI Judge there must make many more and more complex decisions than China's Internet Court AI Judge that affect the outcome of a case. For example, the AI Judge would need to assess witness credibility. In theory, thousands of videos of people telling the truth and being deceptive could hone the AI Judge's deception detection skills. The University of Maryland's Deception Analysis and Reasoning Engine ("DARE") AI is being used just that way: to "autonomously detect deception in courtroom trial videos" by looking for "micro-expressions" and "vocal patterns"

---

[15] Brian Bergstein, *What AI Still Can't Do*, MIT Technology Review (2020), https://www.technologyreview.com/2020/02/19/868178/what-ai-still-cant-do/.

[16] Marr *Weak-Strong* Post, *supra* note 11; Brian Haney, *The Perils and Promises of Artificial General Intelligence*, 45 Notre Dame J. Legis. 150, 152 (2018), https://scholarship.law.nd.edu/jleg/vol45/iss2/1/.

[17] Marr *Weak-Strong* Post, *supra* note 11; Davies, *supra* note 12; *A LawTech Glossary*, Radiant L. Blog, https://radiantlaw.com/blog/a-lawtech-glossary (last visited June 27, 2021) ("'General' artificial intelligence refers to thinking computers, a concept that for the foreseeable future exists only in science fiction and lawtech talks. 'Narrow' artificial intelligence refers to a limited capability (albeit one that may be very useful) such as classifying text or pictures, or expert systems. Discussions of AI that blur general and narrow AI are a good indication that you are dealing with bullshit.").

[18] Jessica Newman, *Explainability Won't Save AI*, Brookings (May 19, 2021), https://www.brookings.edu/techstream/explainability-wont-save-ai/ (citing Kevin Casey, *What is Explainable AI?*, The Enterprisers Project (May 22, 2019), https://enterprisersproject.com/article/2019/5/what-explainable-ai).

that indicate "truthfulness or deception."[19] But how would a DARE-based AI Judge explain its witness credibility assessments to the parties in a way that they can understand? Referencing micro-expressions and vocal patterns is too complex. Maybe the AI Judge could use a system like the Theranos trial jurors—assign a credibility rating to each witness.[20]

The point is explainability is key for litigants to accept an AI Judge's decision. Who would trust an AI Judge that simply pronounces: "I find for the plaintiff on its breach of contract claim. I find for the defendant on plaintiff's fraud claim"?[21] It's "not a matter of calling balls and strikes. Laws are made by humans, they affect humans and their application is unavoidably a human endeavor."[22]

The need for "explainability" results from AI's "black box problem"—its inability to explain how it arrives at its decision. The black box problem arises because we can know the inputs that go into an AI algorithm and the output that it spits out, but we quite often don't know what happens in between—inside the algorithm itself.[23] The black box problem also means that AI can be infected with the biases and mistaken assumptions of its human creators or be influenced by datasets that don't reflect a broad and representative data sample.[24] For example, what if the DARE AI's human designers trained it that a particular microexpression shows deception but the human designers were incorrect in their assessment? The DARE AI would reflect that same mistake.

---

[19] Dom Galeon, *A New AI that Detects "Deception" May Bring an End to Lying as We Know It*, FUTURISM (Jan. 9, 2018), https://futurism.com/new-ai-detects-deception-bring-end-lying-know-it; *see also* Zhe Wu et al., *Deception Detection Videos*, ARXIV (Dec. 12, 2017), https://arxiv.org/pdf/1712.04415.pdf; *see also BORDERS' Avatar on Duty in Bucharest Airport*, UNIV. OF ARIZ. (Dec. 13, 2013), https://eller.arizona.edu/news/2013/12/borders-avatar-duty-bucharest-airport (discussing the AVATAR deception detecting AI used at border crossings).

[20] Sara Randazzo and Meghan Bobrowsky, *Jury in Elizabeth Holmes Trial Seized on Two 'Smoking Guns' to Convict Theranos Founder, Juror Says*, THE WALL STREET JOURNAL (Jan. 6, 2022), https://www.wsj.com/articles/jury-in-elizabeth-holmes-trial-seized-on-two-smoking-guns-to-convict-theranos-founder-juror-says-11641503502.

[21] Ironically, we allow human arbitrators to do this when issuing standard awards versus reasoned awards.

[22] Sean Braswell, *All Rise for Chief Justice Robot!*, OZY (June 6, 2015), https://www.ozy.com/the-new-and-the-next/all-rise-for-chief-justice-robot/41131/.

[23] Newman, *supra* note 18.

[24] *Id.* (citing as an example, JOY BUOLAMWINI & TIMNIT GEBRU, GENDER SHADES: INTERSECTIONAL ACCURACY DISPARITIES IN COMMERCIAL GENDER CLASSIFICATION (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf).

"Explainable AI" targets the black box problem. But "explainability" is different for different audiences. To AI developers, it helps debug systems. To AI users, it makes the system understandable. [25] The latter is more difficult. It requires "understanding the context of an explanation, communicating uncertainty associated with model predictions, and enabling user interaction with the explanation."[26] And while explainability may highlight a problem in an AI model's "reasoning," it won't mitigate it. *Humans* must still implement such changes. Thus, "[e]xplainability will only result in trust alongside testing, evaluation, and accountability measures that go the extra step to not only uncover, but also mitigate exposed problems."[27]

In the context of civil litigation, to make the AI Judge's decision understandable to the litigants would likely require the AI Judge to announce its findings of fact and conclusions of law. Weak AI just can't do this. Certainly, many AIs augment the civil litigation process—including AIs that assist with investigation,[28] case assessment[29] and discovery,[30] legal research,[31] responsive pleadings,[32] and motions.[33] Perhaps capabilities of these AIs and the DARE deception detecting AI could be integrated to output a list of findings of fact and conclusions of law from inputs of pleadings, briefing, exhibits, testimony, statutes, rules, and case law and the AI Judge's intermediate rulings on motions and objections. Litigants might still not consider that sufficient. They might require the AI Judge to explain *how* it determined the facts and legal conclusions—even though human judges are not required to explain their decisions at this granular level. That level of "explainability" would allow humans to judge how well the AI Judge approximates its human counterpart. That level of explainability must wait for strong AI. Until then, the Internet Court AI Judge sits alone on its bench.

---

[25] *Id.* (citing UMANG BHATT, ET. AL., EXPLAINABLE MACHINE LEARNING IN DEPLOYMENT (Jan. 27, 2020), https://dl.acm.org/doi/pdf/10.1145/3351095.3375624).

[26] Newman, *supra* note 18.

[27] *Id.*

[28] *See, e.g.,* TrialDrone and Intraspexion.

[29] *See, e.g.,* Solomonic, Gavelytics, LexMachina.

[30] *See, e.g.,* Casepoint CaseAssist, Luminance, Reveal NexLP, Everlaw, Disco.

[31] *See, e.g.,* Casetext Parallel Search, Westlaw Edge, LexisNexis.

[32] *See, e.g.,* LegalMation, Casetext Compose, Casemine.

[33] *See, e.g.,* LegalMation.

About the Author

Amy Falcon (J.D. South Texas College of Law 2008; LL.M. Litigation Management, Baylor College of Law 2022) is an unabashed technology and legal nerd. A first career in technology combined with her second career in law causes her frequently to ponder the influence of rapidly advancing technology on the practice of law and lawyers. Amy views litigation as a repeated set of common activities that, much like technology projects, can benefit from project management processes and tools. As a partner in the Litigation Section of Porter Hedges LLP, Amy looks for ways to leverage technology to help her manage cases and deliver value to her commercial litigation clients.

Entertainment NFTs are All the Rage: Basics, the Basic Agreement and a Checklist

By Chris Castle

NFTs are all the rage—which is almost a guarantee that something is up. The market for NFTs does seem to have erupted faster than you can say "dot bomb" or "tulip" or even "bubble." But like so many other things, it's good to understand what an NFT is and how to analyze it because it may be coming soon to a client near you.

The regulatory environment for NFTs is evolving as is the litigation over the tokens.[1]

What Is An NFT?

The acronym stands for Non Fungible Token, which is not particularly descriptive. Let's compare a few different definitions in the reporting.

Forbes: "An NFT is a digital asset that represents real-world objects like art, music, in-game items and videos. They are bought and sold online, frequently with cryptocurrency, and they are generally encoded with the same underlying software as many cryptos."

Investopedia: "Non-fungible tokens or NFTs are cryptographic assets on a blockchain with unique identification codes and metadata that distinguish them from each other. Unlike cryptocurrencies, they cannot be traded or exchanged at equivalency. This differs from fungible tokens like cryptocurrencies, which are identical to each other and, therefore, can be used as a medium for commercial transactions."

CNET: "An NFT is a unique digital token, with most using the ethereum blockchain to digitally record transactions. It's not a cryptocurrency like bitcoin or ether, because those are fungible -- exchangeable for another bitcoin or cash. NFTs are recorded in a digital ledger in the same way as cryptocurrency, so there's a listing of who owns each one. What makes an NFT unique is

---

[1] See e.g., *Robert Armijo vs. Ozone Networks, Inc. d/b/a OpenSea, Yuga Labs, LLC D/B/A Bored Ape Yacht Club*, (Case No. 3:22-cv-00112-LRH-CLB U.S. D.C. Nev., Feb. 28, 2022); *Nike, Inc. v. StockX LLC* (Case No. 1:22-cv-00983 U.S. D.C. S.D.N.Y., Feb. 3, 2022); *Free Holdings, Inc. v. Kevin McCoy, Sotheby's Inc., Nameless Corporation and Alex Amsel* (Case No. 1:2022cv00881 U.S. D.C. S.D.N.Y., Feb. 1, 2022); *Miles Parks McCollum pka Lil Yachty v. Opulous, Ditto Ltd. dba Ditto Music, James Lee Parsons* (Case No. 2:22-cv-00587 U.S. D.C. C. Dist. Calif., Jan. 27 , 2022); *Hermes International v. Rothschild* (Case No. 1:22-cv-00384 U.S. D.C. S.D.N.Y., Jan. 14, 2022); *Miramax LLC v. Quentin Tarantino* (Case No. 2:21-cv-08979 U.S. D.C. C. Dist. Calif., Nov. 16, 2021).

the digital asset tied to the token. This can be an image, video, tweet or piece of music that's uploaded to a marketplace, which creates the NFT to be sold."

You will also see the term "smart contract" used with NFTs.[2] A smart contract is not really a contract in the conventional sense but is rather self-executing computer code representing the terms of an agreement between parties which may be a separate document. The code of the smart contract exists on a distributed and decentralized blockchain sometimes called a ledger.

In a simple form, a smart contract allows a customer to transfer cryptocurrency into the ledger something like a vending machine and goods are transferred to your account (often a digital wallet). Some terms of a smart contract can also be enforced depending on the nature of the good concerned and the degree of enforcement that can be connected to the blockchain. It is important to note that smart contracts and the blockchain are highly resistant to modification and are sometimes called "immutable." This makes fixing mistakes or correct downstream rights transfers difficult or impossible.

Generally speaking, in order to build a smart contract the program must be able to lock and unlock access to goods or services automatically; the terms must be able to be expressed in an exact sequence of concrete terms agreed to by all the participants expressed by a trusted digital signature; and the contract must be capable of being deployed to the blockchain of a particular platform (which must be maintained by someone essentially forever) and distributed to the platform's nodes.

Realize that because smart contracts are, or give effect to, contracts between parties, they will be interpreted in accordance with state law including UCC and statute of frauds where applicable. JAMS has developed rules and clauses for dispute resolution involving smart contracts which are evolving.[3]

So if we summarize, an NFT is a "token", only used in the way "token" has meaning in computer programming and not on buses. A "token" is essentially a piece of code assigned to a computer on a network that can perform certain tasks and can be trusted by other computers on that

---

[2] See generally, Stuart D. Levi and Alex B . Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE (May 26, 2018) available at https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/

[3] *JAMS Smart Contract Clause and Rules (DRAFT)*, JAMS MEDIATION, ARBITRATION AND ADR SERVICES available at https://www.jamsadr.com/rules-smart-contracts

network as authentic. However, depending on the terms associated with a particular NFT, other regulatory issues may apply such as state or federal securities laws.

NFTs and Securities

There's a serious issue of whether an NFT is itself a "security" bringing it within the authority of the U.S. Securities and Exchange Commission.[4] This is a deeper subject, but I will try to get you started.

The SEC enforces U.S. securities regulations designed to protect investors through disclosures by "issuers" and other market-making rules. To my knowledge, the SEC has not ruled on NFTs as an asset class, and likely will review each on a case-by-case until a practice develops regarding categories of these financial products. But there are comparable financial products that may indicate how the SEC will move in the future. Recent SEC guidance on celebrity endorsement of Initial Coin Offerings for crypto currencies (that monetize NFTs) and the SEC's prosecution of Ripple Labs may shed some light by analogy for issuers of NFTs.

"Anti-Touting" Rules Implicated in Celebrity Endorsement of Crypto

The SEC has issued some guidance about entertainers endorsing cryptocurrency initial coin offerings that may be analogous to some NFTs:

> Celebrities and others are using social media networks to encourage the public to purchase stocks and other investments. These endorsements may be unlawful if they do not disclose the nature, source, and amount of any compensation paid, directly or indirectly, by the company in exchange for the endorsement….Celebrities and others have recently promoted investments in Initial Coin Offerings (ICOs). In the SEC's Report of Investigation concerning the DAO, the Commission warned that virtual tokens or coins sold in ICOs may be securities, and those who offer and sell securities in the United States must comply with the federal securities laws. Any celebrity or other individual who promotes a virtual token or coin that is a security must disclose the nature, scope, and amount of compensation received in exchange for the promotion. A failure to disclose this information is a violation of the anti-touting provisions of the federal securities laws. Persons making these endorsements may also be liable for potential violations of the anti-fraud provisions of the federal securities laws, for

[4] See, e.g., *In re Tomahawk Exploration LLC and David Thompson Laurance, Securities* (SEC Admin. Proceeding 3-18641 (Aug. 14, 2018)) available at https://www.sec.gov/litigation/admin/2018/33-10530.pdf (Virtual tokens offered by Tomahawk were securities under *Howey* test and can be treated like penny stock).

participating in an unregistered offer and sale of securities, and for acting as unregistered brokers. The SEC will continue to focus on these types of promotions to protect investors and to ensure compliance with the securities laws.

The Big Enchilada: Is any NFT a "Security"?

Determining whether an NFT is a "security" is a key step in evaluating the sale of NFTs and whether a seller of NFTs needs to comply with securities laws, disclosure requirements and limitations on investors. This seems more likely to apply if the NFT uses the "smart contracts" we hear so much about in the cryptocurrency discussion. One way—and it's just *one* way—that an NFT might be regulated as a security is if it is determined to be an "investment contract" under the test in *S.E.C. v. W.J. Howey Co.*[5]

The *Howey* test asks if:

1. there is an investment of money or some other consideration,
2. in a common enterprise,
3. with a reasonable expectation of profits,
4. to be derived from the efforts of others.[6]

So that's pretty inclusive criteria. Before anyone brushes aside the possibility that the SEC could determine an NFT to be a security, take a close look at those criteria because how the basic question is answered is one to discuss thoroughly with your securities litigation lawyer (or engage one). That advice may be a good idea whether you are either an issuer or an endorser of an NFT.

One might say that a one-off sale of a unique product—which is truly "nonfungible" in the sense that there is only one of the product in existence—may be less likely to be determined a "security" under the *Howey* test.

But—if the asset being sold is or is part of a "smart contract" (similar to *Howey*'s investment contract) which it almost inevitably will be, or an NFT representing shares of a small interest in a royalty stream start looking like shares of stock, the SEC may rule that the NFT is a security.

Your NFT is a "security"--now what? *SEC v. Ripple Labs, Inc.*

Let's say that your NFT is a security under *Howey*. Then what happens? The rule of thumb is that if you issue securities in the United States, it must either be pursuant to the IPO rules

---

[5] 328 U.S. 293, 66 S. Ct. 1100 (1946).

[6] *Id.* at 1103.

(under Form S-1 for those reading along at home) unless the issuer can rely on a securities law exemption (of which there are many). Also realize that there very well may be somewhat or entirely duplicative state securities laws you must also comply with as well as potentially foreign securities laws if your purchaser or transaction is or is deemed to be subject to the jurisdiction of securities regulators outside the United States.

Consider the pending case of *SEC v. Ripple Labs, Inc.*[7] concerning the Ripple cryptocurrency. According to the SEC's press release:

> According to the SEC's complaint, Ripple; Christian Larsen, the company's co-founder, executive chairman of its board, and former CEO; and Bradley Garlinghouse, the company's current CEO, raised capital to finance the company's business. The complaint alleges that Ripple raised funds, beginning in 2013, through the sale of digital assets known as XRP in an unregistered securities offering to investors in the U.S. and worldwide. Ripple also allegedly distributed billions of XRP in exchange for non-cash consideration, such as labor and market-making services. According to the complaint, in addition to structuring and promoting the XRP sales used to finance the company's business, Larsen and Garlinghouse also effected personal unregistered sales of XRP totaling approximately $600 million. The complaint alleges that the defendants failed to register their offers and sales of XRP or satisfy any exemption from registration, in violation of the registration provisions of the federal securities laws.
>
> "Issuers seeking the benefits of a public offering, including access to retail investors, broad distribution and a secondary trading market, must comply with the federal securities laws that require registration of offerings unless an exemption from registration applies," said Stephanie Avakian, Director of the SEC's Enforcement Division. "We allege that Ripple, Larsen, and Garlinghouse failed to register their ongoing offer and sale of billions of XRP to retail investors, which deprived potential purchasers of adequate disclosures about XRP and Ripple's business and other important long-standing protections that are fundamental to our robust public market system."

That last sentence is important and tells the defendants what they have to prove—essentially that they were not selling securities so did not have to comply with the registration and disclosure requirements of federal securities law. (But see controversial speech of former SEC

---

[7] Complaint, C.A. No. 1:20-cv-10832 (Dec. 22, 2020), *available at:* https://www.sec.gov/litigation/complaints/2020/comp-pr2020-338.pdf.

director William Hinman on applicability of Howey to digital asset transactions.) Combined with the anti-touting rules applicable to the crypto currency guidance, celebrities in all fields, including songwriters, artists, record companies, sports figures, and beyond have to be careful.

While it's beyond the scope of this post, it must also be asked whether an NFT platform that is determined to be selling unregistered securities has exposure as an unregistered broker dealer or other violations. Entertainment properties produced under union agreements may have additional wrinkles yet to be adjudicated.

Performer Payments and NFTs

You've all heard about them: NFTs are going to save the music business or at least artists. You do have to ask yourself how much would we have to pay them to leave us alone. But NFTs are definitely all the rage.

If the copyright being licensed for minting happens to be a motion picture or television program or sound recording created by a union signatory under a collective bargaining agreement such as the Screen Actors Guild-AFTRA Basic Agreement, it may—*may*—qualify as a "reuse" which requires direct negotiation with any performer whose performance appears in the material being licensed. If it does and if you don't clear the use, this is the kind of thing that can ruin your whole day. (See SAG-AFTRA Basic Agreement paragraph 22.) Paragraph 22A of the 2014 Basic Agreement states:

> *No part of the photography or sound track of a performer shall be used other than in the picture for which he was employed,* ***without separately bargaining with the performer and reaching an agreement regarding such use****. The foregoing requirement of separate bargaining hereafter applies to reuse of photography or sound track in other pictures, television, theatrical or other, or the use in any other field or medium.* ***Bargaining shall occur prior to the time such reuse is made, but performer may not agree to such reuse at the time of original employment.*** *The foregoing shall apply only if the performer is recognizable and, as to stunts, only if the stunt is identifiable.*[8]

The higher the prices go in the NFT bubble, the more likely it is that someone will be in this situation and that a performer—or their estate—may well ask for the payment to which they are entitled under the union agreement. But here's the kicker: the union obligation applies to

---

[8] Screen Actors Guild-AFTRA Basic Agreement (2014), *available at:* https://www.sagaftra.org/files/2014_sag-aftra_cba_1.pdf (emphasis added).

signatories to the collective bargaining agreement. That's likely to be the studio or record company, which is why those licenses almost always include language about the buyer's (or licensee's) responsibility to make all third-party payments, including union payments.

The more the NFT transaction trades on the name of the actors or musicians involved, the more convincing the case. This is very fact specific, but it's not all that fact specific. It's going to come up (*but see Brown v. 20th Century Fox Film Corp.*[9]). If you are hearing about reuse negotiations for the first time, don't feel bad, it's often overlooked even by the smart people.

Even so, I fully expect that we are going to suffer through another round of loophole seeking behavior regarding copyright that we saw in the 1990s and 2000s when there was just too much money to be made on the Internet (reminiscent of the "49ers" who came to California in the 1849 Gold Rush). The greed factor of 99ers gave us very long and protracted excuses for theft, such as the trilogy by the very well-funded Lessig, as well as seemingly endless litigation that goes on to the present day over loophole seeking behavior that distorts the DMCA and fair use, as well as the controversial Section 230 of the Communications Decency Act. There's just too much money being made with NFTs, cryptocurrency and blockchain to think otherwise.

It must also be said that the same kind of willfully blind hucksters are at work in the NFT market that were and still are engaged in massive copyright infringement online. NFTs can easily be tokenized without the owner of the underlying copyright having any idea that their work is being infringed, much less consented. The same could be said of right of publicity claims, palming off, and trademark infringement.

Even though NFTs are an evolving area of the law, they are a hot area of business. So what should we think about right now today if an artist or celebrity client is approached to lend their brand to an NFT?

An artist's checklist for an NFT pitch

If you or your client have been pitched to lend your name to an NFT platform or promotion, or if you are an NFT promoter who wants to attract artists to your program, the following are some issues that should get addressed before you commit to anything.

1. What artist rights are being granted and to whom? How are future copyright reversions or statutory terminations handled? Is the smart contract so immutable that it cannot permit such transfers?

---

9 799 F. Supp. 166 (D.D.C. 1992).

2. Does grant of rights match the project summary and are the license agreement, smart contract, marketplace/auction TOS and cryptocurrency rules all consistent? Has a subject matter expert been engaged to produce a report stating and certifying that the smart contract code implements the actual deal or needs to be revised? Does any lawyer in the transaction have a duty to confirm that the smart contract code actually implements the license agreement terms?
3. What royalty is paid and to whom and when? Does artist, previous owner or charity participate in resale revenue after initial sale? Are any state or federal relevant tax rules implicated?
4. Are there exploitation or marketing restrictions on the NFT that would prevent the NFT and artist name being used in ways that are offensive to the artist, at least during the artist's lifetime? Could heirs enforce these rights?
5. Are there any third-party payments involved like producer payments, production company overrides, or any third-party rights involved, such as re-recording restrictions? Will any letter of direction be required, e.g., for producers?
6. Are you being asked to clear song rights (often called "publishing")? If someone is telling you that they have cleared publishing, has the publisher confirmed the license and are individual songwriters actually receiving a share of revenue? The tendency is that the major publishers "settle" these kinds of cases for a lump sum and prospective royalty, which may or may not be received by individual songwriters after multiple commissions being siphoned off the top.
7. When does NFT terminate? (On resale, transfer by owner, term of years)). Consider smart contract immutability issues on termination.
8. What is the governing law and venue? (And how to enforce)
9. Who maintains the blockchain and who is responsible for policing it? What happens if they fail to do so? (See my post with Alan Graham on this subject.)
10. Is the artist asked to make representations, warranties and indemnity? Can the artist make such representations and warranties?
11. Is indemnity capped?
12. Are there any active disputes among anyone in the chain on the NFT promoters' side? ("Disputes" includes any disagreement, including, but not limited to, litigation or threatened litigation.) Who will cover artist's costs of defense?
13. Is there insurance on chain of title, failure to enforce the smart contract, nonpayment, and business risk?
14. Can the license agreement or smart contract be revised unilaterally?

15. Is the NFT or NFT collection comprised of "generative art" or artwork created by machines, algorithms, artificial intelligence, and related technologies (i.e., potentially not capable of copyright protection)? What are the implications for name and likeness rights?
16. What assurances have been given to identify purchasers of NFTs to enforce terms or prosecute breaches for first or subsequent sales?
17. Are any union rules implicated (e.g., SAG-AFTRA Basic Agreement Par. 22A, discussed above)?
18. Is NFT or any NFT cash flow implicated in any sanctions placed on persons related to the Russian Federation?
19. Has the NFT seller or marketplace obtained legal opinion regarding whether the NFT constitutes a "security" that would require sale by a registered securities broker-dealer or other regulatory oversight?
20. Are any state securities laws, tax laws or regulations, or "doing business" laws implicated or reporting obligations triggered?

Each NFT raises its own questions, so this checklist is just a starting point.

About the Author

Chris Castle is a music lawyer in Austin and director of the State Bar of Texas Entertainment Law Institute. He practices at the nexus of music, music-tech and public policy.

Case Summary: *United States v. Cheng*, No. 4:20-CR-455, 2022 WL 112025 (S.D. Tex. Jan. 12, 2022) (slip copy)

By Grant M. Scheiner

Judge Andrew Hanen of the United States District Court for the Southern District of Texas (Houston Division) applied the "inevitable discovery doctrine" in ruling that cell phone evidence obtained as a result of an illegal FBI interrogation should not be suppressed at trial. Despite that FBI agents violated a Texas A&M professor's rights under *Miranda v. Arizona*, 384 U.S. 436 (1966) and related authority by cajoling the professor into revealing his mobile device passwords — during a custodial interview and after the professor had unequivocally requested a lawyer — the Court held the Government would have inevitably discovered the password information through use of a court order or search warrant. As such, evidence obtained by the Government was not ruled inadmissible as "fruit of the poisonous tree."[1]

This opinion adds to a growing body of case law attempting to strike a balance between an accused's 4th Amendment right against unreasonable search and seizure, as well as the 5th Amendment right against self-incrimination, versus the Government's desire to secure private data it believes may be evidence of a crime. Whether the Government may compel an accused to reveal a mobile device password is an issue that seems destined for repeated trial and appellate court litigation, until the United States Supreme Court articulates a rule(s) that Government agents, legal practitioners, and trial judges can easily understand and apply.

Factual Summary

On August 20, 2020, Texas A&M Professor Zhengdong Cheng ("Professor Cheng") was returning from a work trip in Qatar when, at Easterwood Airport in College Station, two Federal Bureau of Investigation ("FBI") agents approached Professor Cheng and requested that he follow them to a room in the airport for questioning.[2] Shortly after detaining Professor Cheng in the

---

1 *United States v. Cheng*, No. 4:20-CR-455, 2022 WL 112025 at *1 (S.D. Tex. Jan. 12, 2022) (slip copy) (citing *United States v. Hernandez*, 570 F3d 616, 620 (5th Cir. 2012)).

2 *Cheng*, Slip Copy at *1.

room, the agents read him his *Miranda* warnings.[3] Professor Cheng asked whether the agents could tell him why he was being questioned, but the agents suggested they could not do so until Professor Cheng waived his *Miranda* rights and abandoned his right to remain silent.[4] Professor Cheng then requested a lawyer, to which one of the agents replied, "You are absolutely [entitled to have a lawyer] – but we just can't talk to you if you do that right now. We can't answer any of your questions right now."[5] Professor Cheng then asked whether he was free to go to his hotel, and an agent informed him that Professor Cheng could not leave because he was being detained, but also claimed he was not under arrest.[6] At the time of his detention, Professor Cheng was carrying electronic devices and those were segregated by the agents.[7]

Professor Cheng continually sought an explanation as to why he was being detained, and the agents repeatedly asserted they could provide him more information only if he waived his *Miranda* rights.[8] The agents stressed that Professor Cheng was not free to leave and revealed only that the matter was "very serious."[9] The agents claimed an arrest warrant had been issued for him.[10] As the Trial Court's written opinion aptly noted, when a detained suspect makes "some statement that can reasonably be construed to be an expression of a desire for the assistance of an attorney," the "interrogation must cease until an attorney is present."[11] The Trial Court noted that "[w]hen a suspect makes an ambiguous or equivocal statement, officers may seek to ask clarifying questions to ensure that the suspect has actually invoked his or her

---

3 *Id*. As the trial court noted, "one of the rights included under *Miranda's* umbrella is the accused's right to counsel." *Id.* at *2 (citing *Miranda*, 384 U.S. at 470). Another is the right to remain silent and not make any statement at all. Although the purpose of this case summary is to educate and not dispense legal advice, I can tell you as a criminal defense lawyer I typically advise clients who are confronted by police or government agents to exercise their right to remain silent. If taken into custody and interrogated, I normally advise clients to give the following response to questions (repeatedly, if necessary): **"I want a lawyer."** There are numerous reasons why a person, whether in formal custody or merely having been read *Miranda* warnings, should repeatedly and unambiguously request a lawyer.

4 *Id*.

5 *Id*. at *1.

6 *Id*.

7 *Id*.

8 *Id*. at *2.

9 *Id*.

10 *Id*.

11 *Id*. (citations omitted).

right to an attorney."[12] An officer or government agent may not, however, use "clarification" as a guise for convincing a suspect to waive his or her rights.[13]

As it turned out, Professor Cheng was under investigation for and eventually charged with wire fraud, false statements, and conspiracy, stemming from allegedly intentionally failing to disclose that Professor Cheng was employed by the Chinese University, Guangdong University of Technology, in order to obtain a grant from the National Aeronautics and Space Administration (NASA).[14] After convincing Professor Cheng to waive his *Miranda* rights, the accused interviewed with FBI agents, answered their questions, and verbally provided FBI agents with passwords to his mobile devices.

The Trial Court ruled that due to FBI agents violating Professor Cheng's *Miranda* rights, all statements made in response to custodial interrogation would be inadmissible at trial. However, Professor Cheng's attorneys argued that evidence obtained on the devices should likewise be ruled inadmissible, since the FBI obtained passwords only as a result of the *Miranda* violation – i.e., they were fruit of the poisonous tree. While the Trial Court's opinion recognized the 4th Amendment's exclusionary rule generally "prohibits the introduction at trial of all evidence that is derivative of an illegal search,"[15] the Court nonetheless ruled the evidence obtained from the mobile devices was admissible, because the Government would have inevitably discovered it.

The inevitable discovery doctrine "renders the exclusionary rule inapplicable to otherwise suppressible evidence if that evidence would inevitably have been discovered by lawful means."[16]. In this case, the Trial Court concluded that because it was a "foregone conclusion" that Professor Cheng knew the passwords to the seized devices (which itself is not a crime), his acts in producing the devices and the passwords would not qualify as "incriminating testimony" in violation of his 5th Amendment privilege against self-incrimination.[17] Moreover, possession of the devices and/or the passwords that facilitated access was not testimonial.[18] As such, the Government would have been able to obtain a court order to compel Professor Cheng to decrypt the devices. The Trial Court concluded that because the Government would have been

---

[12] *Id.* at *3 (citations omitted).
[13] *Id.*
[14] *Id.* at *1.
[15] *Id.* at *4.
[16] *Id.* at *5 (citing *United States v. Jackson*, 596 F.3d 236, 241 (5th Cir. 2010)).
[17] *Id.* at *7.
[18] *Id.*

able to obtain a court order to compel Professor Cheng to provide passwords, the contents of the devices would have been "inevitably discovered."[19]

While it certainly seems like compelling an accused to speak (that is, verbally tell the Government his mobile-device passwords) would violate the 5th Amendment, the Trial Court appeared piqued by the thought of allowing a criminal defendant to claim privilege as a means of avoiding disclosure of a password. "A rule prohibiting the government from ever compelling decryption of a password-protected device would certainly lead to absurd, untenable results," the Trial Court wrote.[20] Quoting an opinion from the Northern District of California, the Trial Court offered: "Whether a defendant would be required to produce a decrypted drive would hinge on whether he protected that drive using a fingerprint key or a password composed of symbols … [or] whether he kept the documents at issue in a combination safe or key safe."[21] "The application of the Fifth Amendment should not be dependent on the manner in which an individual locks or secures material, whether physically or electronically."[22]

Conclusion

While there does not appear to be any controlling case law for this type of fact pattern or the application of the 5th Amendment as it relates to the manner in which an individual locks or secures an object, there is plenty of general case law on the application of the 4th Amendment. Sometimes the *actions* of the accused can make all the difference in determining whether the Government may search an object. For example, whether and how a person closes or locks a container or suitcase are directly relevant to whether the police may conduct a lawful search. *See, e.g., U.S. v. Basinski*, 226 F.3d 829, 834-35 (7th Cir. 2000) (Inasmuch as a reasonable person would be less likely to believe that defendant granted free access to contents of locked containers, precautions taken to ensure privacy, such as locks or government's knowledge of defendant's orders not to open the container, are relevant considerations in determining a third party's authority to consent to search of a container.) It might be feasible and logical to apply a similar analysis of privacy interests under the 4th Amendment as to the 5th Amendment. Different results aren't necessarily absurd or even a bad thing. If a person specifically chooses to use a password(s) instead of a fingerprint or face scan, then forcing him to utter that password may indeed violate his rights under the 5th Amendment. In any event, it is clear that

---

[19] *Id.*

[20] *Id.* at *6.

[21] *Id.* (citations omitted).

[22] *Id.*

Government agents, legal practitioners, and trial and appellate courts could all benefit from some better guidance in this developing area of the law.

About the Author

Grant Scheiner is Managing Attorney of Scheiner Law Group, P.C., a criminal defense firm in Houston. He is a Former Chair of the Computer and Technology Section, Immediate Past President of the Texas Criminal Defense Lawyers Association, Board Member of the Texas Board of Legal Specialization, and a Life Member of the Texas Bar Foundation.

SHORT CIRCUITS:-

Ubiquitous cameras make it ever harder to hide.

By Pierre Grosdidier

In *United States v. Tuggle*, the Seventh Circuit Court of Appeals held that the government did not need a search warrant to monitor the home of a suspected methamphetamine dealer with three cameras mounted on public utility poles located on public property.[1] The cameras remained in place for 18 months, surveilled the home around the clock from several vantage points, and monitored the ins and outs of suspected mules. The surveillance yielded evidence that supported a search warrant that led to Tuggle's indictment on drug charges. The trial court denied his Fourth Amendment challenges of the camera evidence. Tuggle eventually pleaded guilty, reserving his right to appeal the trial court's denials of his motions to suppress. The Circuit Court affirmed.[2]

Because the government had not physically intruded into Tuggle's home, the Circuit Court analyzed his Fourth Amendment challenge under *Katz*'s reasonable expectation of privacy test.[3] The Court easily rejected Tuggle's first argument that the use of cameras, rather than police observers, changed the nature of the surveillance into an unconstitutional invasion of privacy. The camera looked at places visible from the public thoroughfare and Tuggle had not exhibited an expectation of privacy by fencing his property or otherwise shielding it from public view.[4] It is black letter law that the Fourth Amendment's protection does not apply to things visible from public thoroughfares and authorities have no obligation to avert their eyes from criminal activities.[5] The Court added that even though some advanced surveillance technologies are impermissible without a warrant (*e.g.*, thermal imaging of a home),[6] the United States Supreme Court has long held that the government can use zooming cameras in

---

1 4 F.4th 505, 511 (7th Cir. 2021), *cert denied*, 142 S. Ct. 1107 (2022).

2 *Id.* at 511–12.

3 *Id.* at 512–13 (citing *Katz v. United States*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (Fourth Amendment analysis inquires whether a person has manifested a subjective expectation of privacy that society is willing to recognize as reasonable)).

4 *Compare with United States v. Cuevas-Sanchez*, 821 F.2d 248, 251 (5th Cir. 1987) (surveillance cameras aimed at defendant's backyard qualified as Fourth Amendment search because backyard fences obstructing public view manifested subjective expectation of privacy).

5 *Tuggle*, 4 F.4th at 514.

6 *Id.* at 515 (citing *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (home thermal imaging violates Fourth Amendment)).

their investigations, so long as the surveillance does not "penetrate walls or windows so as to hear and record confidential discussions."[7]

The Court next turned to Tuggle's mosaic theory argument whereby he alleged that the cameras' lengthy surveillance unconstitutionally captured the whole of his movements.[8] Reviewing the mosaic theory's traction among various—but not all—state and federal courts, the Court first noted that the United States Supreme Court has yet to direct lower courts to use it.[9]

In this case, the Court held that even if it accepted the theory—which it did not—Supreme Court precedent did not support Tuggle's argument. The cameras recorded the time Tuggle spent at his home but provided little other information about his public movements that, in the aggregate, would provide intimate details of his "familial, political, professional, religious, and sexual associations."[10] The fact that the cameras provided prospective and not historical information further distinguished this case from *Carpenter v. United States* and *United States v. Jones*. In these cases, the Supreme Court invoked the power of CSLI and GPS data, respectively, to reconstruct a person's past peregrinations to justify the necessity of search warrants. Because the pole-mounted cameras provided no historical location data, they did not offend the Fourth Amendment.[11]

In closing, the Court stressed that its holding did not depend on the theoretical possibility of stationing government agents atop poles as camera substitutes. Such an assumption would contravene the "Fourth Amendment and *Katz*'s command to assess reasonableness."[12] Advanced forms of surveillance, the Court concluded, are not constitutional simply because they can be accomplished conventionally. In *dicta*, the Court also expressed its unease with the growing capabilities of surveillance cameras but nonetheless declined to draw a line that demarcated when the duration of the surveillance offended the Fourth Amendment. It also

---

7 *Id*. (citing *Dow Chemical Co. v. United States*, 476 U.S. 227, 238–39 (1986) (warrantless aerial photographic surveillance of chemical plant from navigable airspace does not violate the Fourth Amendment)).

8 *Id*. at 524.

9 *Id*. at 517.

10 *Id*. at 524 (citing *Carpenter v. United States*, --- U.S. ---, 138 S. Ct. 2206, 2217 (2018) (accessing CSLI requires a warrant); *United States v. Jones*, 565 U.S. 400, 415 (2012) (GPS tracking device attached to a car requires a warrant)).

11 *Id*. at 525.

12 *Id*. at 526.

expressed concern that advancing technological capabilities might weaken the Fourth Amendment's protections as individuals increasingly come to expect and rely on these capabilities, which in turn diminishes their expectations of privacy.

About the Author

Pierre Grosdider is an attorney in Houston. He belongs to the first group of attorneys board certified in construction law by the Texas Board of Legal Specialization in 2017. Pierre's practice also includes data privacy and unauthorized computer access issues and litigation. 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, an AAA Panelist, a registered P.E. in Texas (inactive), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Treasurer for 2020–21.

Case Commentary: *Kristin Fast v Godaddy.com LLC et al.*

By Craig Ball

United States District Judge David Campbell of Arizona issued an order on February 3, 2022 imposing serious sanctions for discovery abuse against a plaintiff in a case styled, *Kristin Fast v Godaddy.com LLC et al.*, No. CV-20-01448-PHX-DGC, 340 F.R.D. 326 (D. Ariz. Feb. 3, 2022).

Plaintiff Kristin Fast sought damages on theories built around an injury she claimed was aggravated by her work at Godaddy.com. A skiing accident and surgery led Fast to be diagnosed with a syndrome called Complex Regional Pain (CRP). Detailing Ms. Fast's actions to creatively curate facts and jettison and recast unfavorable evidence, Judge Campbell found Ms. Fast acted with that rare species of hubris, the "intent to deprive."

Rule 37(e) of the Federal Rules of Civil Procedure was amended in 2015 to make it well-nigh impossible for a U.S. federal judge to punish a party's failure to preserve electronically stored information (ESI) absent proof that the party acted with an "intent to deprive another party of the information's use in the litigation." By "punish," I mean assessing the most severe sanctions, like dismissing the action or instructing the jury it can infer that whatever the guilty party lost was unfavorable to the party who destroyed it.

Since its inception, there's been uncertainty attendant to whether Rule 37(e) is the sole and exclusive remedy for the loss of ESI that should have been preserved for litigation. Reasonable minds may conclude that, if "lost" ESI is ultimately recovered, sanctions aren't available despite gross malfeasance. That is, if the "lost" ESI wasn't *irreparably* lost, it wasn't "spoliated," and no sanction may issue. Not just no *serious* sanction; no sanction *at all*.

Not so, Judge Campbell makes clear. Rule 37(e) is NOT the exclusive remedy for spoliation of ESI . . . so long as you dress the loss up as something you don't call "spoliation."

For example, plaintiff secretly recorded conversations using her phone, and a few (but not all) of these recordings miraculously surfaced long after they were supposed to have been produced. Addressing a truly "lost" digital recording, Judge Campbell writes, "And Defendants continue to be prejudiced by the failure of Plaintiff to produce the fourth recording she claimed to have made. It is not clear whether that recording is lost or Plaintiff has not produced it. Sanctions under Rule 37(c)(1) are authorized." *Fast* at pp. 33-34.

As Chair of the Advisory Committee on the Federal Rules of Civil Procedure when the 2015 revision of Rule 37(e) was developed and adopted, Judge David Campbell is chief architect of the revision. He knows how the Rule is supposed to work as well as anyone.[1]

If the conventional wisdom is "Rule 37(e) is the exclusive remedy for spoliation sanctions for loss of ESI," then Judge Campbell turns that on its head by adding *in effect,* 'the full range of sanctions available under Rule 37(c)(1) are available for failing to produce ESI.' That Judge Campbell construes the failure to produce ESI for causes *not* tied to spoliation as being a sufficient ground for FRCP 37(c)(1) sanctions is eye-opening; not that he's the first judge to do so, but Judge Campbell is a peculiarly influential voice.

Granted, an aggrieved party is unlikely to secure an order of dismissal or an adverse inference instruction for merely negligent delay or failure to produce because elements of bad faith are sure to be required before the big guns come out. *But see* FRCP Rule 37(b)(2)(A)(i)-(vi) and its sanctions for not obeying a discovery order.[2]

Still, Rule 37(c)(1) packs its own punch for conduct that violates Rule 26(e) (that's the rule requiring parties to timely supplement discovery responses if the party learns that prior responses are materially incomplete or incorrect). As the Court notes at p. 4, "Rule 37(c)(1) provides that a party who violates Rule 26(e) may not use the withheld information at trial unless the failure was substantially justified or harmless. This is "a 'self-executing, automatic sanction to provide a strong inducement for disclosure of material…'" The Court adds, Rule 37(c)(1) also permits a court to order the payment of reasonable expenses caused by the

---

[1] He clearly wishes others understood Rule 37 half so well, *e.g.,* his Footnote 2 states, "It is therefore quite frustrating that, years after the 2015 revision, some lawyers and judges are still unaware of its significant change to the law of ESI spoliation. *See*, *e.g.*, *Holloway v. Cnty. of Orange*, No. SA CV 19-01514-DOC (DFMx), 2021 WL 454239, at *2 (C.D. Cal. Jan. 20, 2021) (granting ESI spoliation sanctions without addressing the requirements of Rule 37(e)); *Mercado Cordova v. Walmart P.R.*, No. 16-2195 (ADC), 2019 WL 3226893, at *4 (D.P.R. July 16, 2019) (same); *Nutrition Distrib. LLC v. PEP Rsch., LLC*, No. 16cv2328-WQH-BLM, 2018 WL 6323082, at *5 (S.D. Cal. Dec. 4, 2018) (ordering adverse inference instructions without addressing the strict requirements of Rule 37(e)(2), and applying the negligence standard that Rule 37(e) specifically rejected)." https://craigball.net/#_ftn1.

[2] One of my many maxims is that "a Court guards its power more scrupulously than a party's rights." That's not a slam on courts, who must scrupulously protect the sanctity of their orders lest chaos ensue. The lesson being that parties should endeavor to convert agreements about discovery obligations into orders whenever possible because a judge is far more likely to punish a transgression of its own order than an offense to a party. At bottom, it's just human nature to do that, right? https://craigball.net/#_ftn2.

failure, to inform the jury of the party's failure, or to "impose other appropriate sanctions, including any of the orders listed in Rule 37(b)(2)(A)(i)-(vi)." Those are big guns, too.

Backup your Phones!

Another positive aspect of the sanctions order in *Fast v Godaddy.com* is that it characterizes mobile devices as sources of ESI that must be routinely preserved in anticipation of litigation. I've been beating that drum for years, so it's delightful to hear it from a Senior District Judge with tons of influence in e-discovery.

Still, there's something about phones in the Order that throws me. The Plaintiff claimed her iPhone was stolen, and the Court took the alleged theft to be true. At p. 20, the Court states, "By failing to back up her iPhone, Plaintiff failed to take reasonable steps to preserve the ESI contained on the phone."

I applaud that conclusion. I've written and spoken quite a lot about how to quickly and cheaply backup phones for ESI preservation and of the need to do so; accordingly, the ruling doesn't offend on grounds of disproportionality. Well done, Judge!

A party needs to foresee the loss of a phone or its contents and, rather than simply preserving the data *in situ* on the phone, a party must affirmatively act to back up the contents of the phone.

That would seem to be the takeaway, *except,* when assessing intent on the next page, Judge Campbell writes, "Assuming the phone was stolen, that act could not have been foreseen or intended by Plaintiff, and neither could its corresponding loss of ESI. The Court therefore cannot find Plaintiff acted with an intent to deprive as required by Rule 37(e)(2)."

So, a party *must* foresee the loss of a phone or its contents as being sufficiently likely to require a copy of its contents be made, but that selfsame loss is *not* sufficiently foreseeable so as to supply the requisite intent to deprive?

I see the distinction, but where do we draw the line in practice? **Why is the phone itself not deemed a sufficient repository for the data to be preserved? If the loss of the phone "could not have been foreseen," why would there be an independent legal duty to back up the ESI contained on the phone?**

It's a fact that any device that stores ESI will fail or may be lost, stolen or destroyed. Phones. Laptops. Electromagnetic drives. Solid state drives. *Anything* that stores ESI lives on borrowed time. Is there a duty to maintain *two* copies of data stored on electronic media because of the

inevitable and omnipresent risk of theft, loss, or failure? Or does that duty *uniquely* attach to phones? If history has taught us anything, it is that dogs have an insatiable hunger for homework. So, parties must act to protect the evidence from reasonably foreseeable loss or failure.

Duties of Counsel

Since the venerable *Zubulake v. UBS Warburg* decisions at the start of this millennium, Courts have warned lawyers over-and-over-again that there's more to initiating a proper legal hold than just telling clients not to delete relevant ESI. Yet, lawyers seem resolutely immune to calls for competence. Judge Campbell raises this in Footnote 18:

> The Court is also concerned about the conduct of Plaintiff's counsel in discovery. He had an affirmative obligation to ensure that his client conducted diligent and thorough searches for discoverable material and that discovery responses were complete and correct when made. See Fed. R. Civ. P. 26(g); *Legault v. Zambarano,* 105 F.3d 24, 28 (1st Cir. 1997) ("The Advisory Committee's Notes to the 1983 amendments to Rule 26 spell out the obvious: a certifying lawyer must make 'a reasonable effort to assure that the client has provided all the information and documents available to him that are responsive to the discovery demand.'"); *Bruner v. City of Phoenix,* No. CV-18-00664-PHX-DJH, 2020 WL 554387, at *8 (D. Ariz. Feb. 4, 2020) ("[I]t is not reasonable for counsel to simply give instructions to his clients and count on them to fulfill their discovery obligations. The Federal Rules of Civil Procedure place an affirmative obligation on an attorney to ensure that their clients' search for responsive documents and information is complete. See Fed. R. Civ. P. 26(g)."); *Stevens*, 2019 WL 6499098, at *4 (criticizing "cavalier attitude toward the preservation requirement" where "counsel failed to immediately preserve obviously crucial evidence at a time when the duty to preserve existed and instead allowed the phone to remain in [his client's] possession").
>
> *Id.* at p. 39, n. 18.

The obligations of counsel to carry out a proper legal hold and collection, and counsels' ability to meet those obligations, remain a river too few can ford. But the lack of lawyer competence is not as reprehensible as the prevailing blasé attitude of the bar respecting rife incompetence. *Hardly anyone seems to care*, at least not enough to prioritize teaching information technology to lawyers and judges. *If we don't teach something to those out of law school, how can anyone be expected to learn it?*

Coming back to *Fast v. Godaddy.com*, perhaps clucking one's tongue at an errant lawyer in a footnote isn't going to change things. In their efforts to dredge a safe harbor in Rule 37(e), Judge Campbell and the distinguished Advisory Committee all-but-immunized the most common instances of spoliation from consequences. Absent proof that spoliation occurred with an intent to deprive, what's really the worst that occurs now? The guilty party is compelled to belatedly do what they were obliged to do all along, or some fraction of same.

The efforts to rein in judicial discretion to punish gross incompetence has been good for business but bad for justice. The fleeting interest in e-discovery education of 15+ years ago was driven by sanctions. By *Zubulake.* By *Coleman (Parent) Holdings v. Morgan Stanley*. By *Qualcomm v. Broadcom.* We never had much of a carrot supporting ESI competence, and 37(e) took away the stick.

Judges must get tougher, and demand more. Your Honors: *Just because you didn't know it when you were practicing doesn't mean lawyers needn't know it now.*

About the Author

Craig Ball teaches Electronic Evidence at the University of Texas and Tulane University Schools of Law. He limits his practice to service as a Special Master in eDiscovery and Computer Forensics.

Read before you click: Electronic signatures are binding.

By Pierre Grosdidier

The authenticity of digital acts by individuals is a recurring courtroom issue. Ten years ago, the Texas Court of Criminal Appeals set the standard for ascribing a text message or a social media posting to a person.[1] Recently, in *Aerotek, Inc. v. Boyd*, the Texas Supreme Court applied the Uniform Electronic Transactions Act ("UETA")[2] to uphold the validity of an arbitration agreement that former employees claimed they never digitally signed.[3]

Aerotek used an online application to recruit employees. Applicants accessed the application via their assigned unique username, password, and security questions. The application led each candidate through a workflow that required consent via digital signatures at certain steps. The first digital signature bound the applicant to "Aerotek's electronic hiring documents 'as though . . . signed . . . in writing.'" Another digital signature bound the applicant to a Mutual Arbitration Agreement ("MAA"). Each action in the workflow created an unalterable record in the application's database, and applicants had to complete all steps to complete their employment application.[4]

Plaintiffs, employees hired and quickly terminated, sued Aerotek and others for racial discrimination and retaliation. Aerotek filed a motion to compel arbitration supported by copies of time-stamped records showing that plaintiffs electronically signed the MAA. Plaintiffs, in response, admitted that they completed the online hiring application but submitted sworn declarations that they had never "seen, signed, or been presented with the MAA." The trial court denied Aerotek's motion to compel arbitration and a divided Dallas Court of Appeals affirmed. Applying the UETA, the Texas Supreme Court reversed and remanded.[5]

The UETA "applies only to transactions between parties each of which has agreed to conduct transactions by electronic means."[6] It states in part that:

---

1 *See Tienda v. State*, 358 S.W.3d 633, 641–42 (Tex. Crim. App. 2012) (requiring something more than device or account ownership to ascribe a text message or a post to a person, even if the bar for this "something more" is low); *see also*, "*Authenticating: can cellphone text messages stand up in court?*" Texas Bar Journal, April 2016, p. 278.

2 Tex. Bus. & Comm. Code §§ 322.001 *et seq*.

3 624 S.W.3d 199, 200 (Tex. 2021).

4 *Id*. at 201.

5 *Id*. at 202–04.

6 Tex. Bus. & Comm. Code § 322.005(b).

> [a]n electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.[7]

The UETA further defines a security procedure as:

> a procedure employed for the purpose of verifying that an electronic signature, record . . . is that of a specific person . . . [and] includes a procedure that requires the use of . . . identifying words or numbers, . . . or other acknowledgment procedures.[8]

The Texas Supreme Court found that Aerotek's security procedures featuring secret credentials qualified under this statutory language. It also found that plaintiffs provided no evidence to support their claims other than their declarations and noted that they sought no discovery from Aerotek to discredit its evidence.[9]

The Court rejected plaintiffs' attempts to impeach the testimony of the Aerotek program manager who defined and helped design and develop the application. She had testified, *inter alia*, that the employees could not have completed their application without signing the MAA and that Aerotek had no ability to alter the employees' submitted records. Importantly, the Court rejected the plaintiffs' argument that the testimony of an IT expert was required "to prove the application's operation and security procedures."[10] The program manager had helped develop the application and had overseen its use by "hundreds of thousands" of applicants. She was, therefore, sufficiently qualified to testify regarding its operation, and her testimony was "sufficiently 'clear, direct, and positive'" to overcome her interested witness status.[11] In light of this evidence, the Court held that "reasonable people could not differ in concluding that the Employees could not have completed their hiring applications without signing the MAAs."[12] Consequently, the trial court's factual finding that the plaintiffs did not sign the MAAs was not supported by the evidence and merited no deference.

---

7 *Id.* § 322.009(a).
8 *Id.* § 322.002(13).
9 *Aerotek*, 624 S.W.3d at 208.
10 *Id.* at 207.
11 *Id.*
12 *Id.* at 209.

About the Author

Pierre Grosdider is an attorney in Houston. He belongs to the first group of attorneys board certified in construction law by the Texas Board of Legal Specialization in 2017. Pierre's practice also includes data privacy and unauthorized computer access issues and litigation. 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, an AAA Panelist, a registered P.E. in Texas (inactive), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Treasurer for 2020–21.

Pornhub: Provider or Publisher?

By Shelby Menard

According to a recent ruling denying defendants' motion to dismiss plaintiffs' complaint by a U.S. District Judge in Alabama,[1] Pornhub is not shielded from liability by Section 230 of the Communications Decency Act ("CDA") for claims brought against it alleging that Pornhub profits off of sexual trafficking and abuse. Section 230 of the CDA states that a provider or user of an interactive computer service shall not be treated as the publisher or speaker of any information provided by another information content provider.[2] However, Section 230 contains a carve-out for liability for sex trafficking acts, specifically indicating that nothing in Section 230 impairs or limits a victim's ability to bring a claim under section 1595 of Title 18 (the civil remedy for the trafficking of persons).[3] Further, the Allow States and Victims to Fight Online Sex Trafficking Act ("FOSTA"), signed into law in 2018, amended the CDA and provided that sex trafficking claims are excluded from the immunity from liability provided by Section 230.[4]

Determining whether liability of a website is precluded under Section 230 involves first analyzing whether the website is a content provider or simply a publisher of third-party content. If it is determined the website is a content provider, the website is not automatically immune from liability under Section 230.

In his Order, the Alabama judge pointed to a test set forth by the Ninth Circuit, which has also been adopted by other Circuits, in determining whether a website is a content provider. This test states that websites are considered content providers if they contribute materially to the illegal conduct.[5] In other words, websites which contribute materially to illegal conduct are considered content providers themselves, rather than just a publisher of third-party content, and are thus not shielded from liability by Section 230. Clearly, the participation level of the website as to the posted content is important in determining whether the website is itself a content provider. In analyzing the website's participation level, courts, in the absence of a

---

1 *Doe #1 v. MG Freesites, LTD*, No. 7:21-CV-00220-LSC, 2022 WL 407147 (N.D. Ala. Feb. 9, 2022).

2 An information content provider is defined as: "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C.A. § 230(f)(3).

3 47 U.S.C.A. § 230(e)(5); 18 U.S.C.A. § 1595.

4 ALLOW STATES AND VICTIMS TO FIGHT ONLINE SEX TRAFFICKING ACT OF 2017, PL 115-164, April 11, 2018, 132 Stat. 1253.

5 *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1168 (9th Cir. 2008).

direct association, determine whether there is a continuous business relationship between the trafficker and the defendant such that it would appear the trafficker and the defendant have established a pattern of conduct or could be said to have a tacit agreement.[6] For example, in this Alabama case, Pornhub actively advertised the child sexual abuse material ("CSAM"), generated tags for increasing views of said CSAM, created thumbnails of the videos, and even created timelines jumping to certain graphically labeled scenes (which the judge indicated "amounts to new creation and possession of child pornography"), thereby contributing materially to the illegal conduct and acting as a content provider rather than simply an interactive computer service. In contrast to the case at hand, rulings in cases with similar fact patterns have differed due to the presiding judge's conclusion that the website owner was not a content provider and did not have an ongoing business relationship with the trafficker.[7] This case against Pornhub is currently ongoing.

About the Author

Shelby Menard is an attorney in Spencer Fane LLP's Data Privacy and Cybersecurity practice group and the Litigation and Dispute Resolution practice group in Plano, Texas. She received her J.D. from Baylor University School of Law in 2017 and holds a bachelor's degree in Political Science from Texas Tech University.

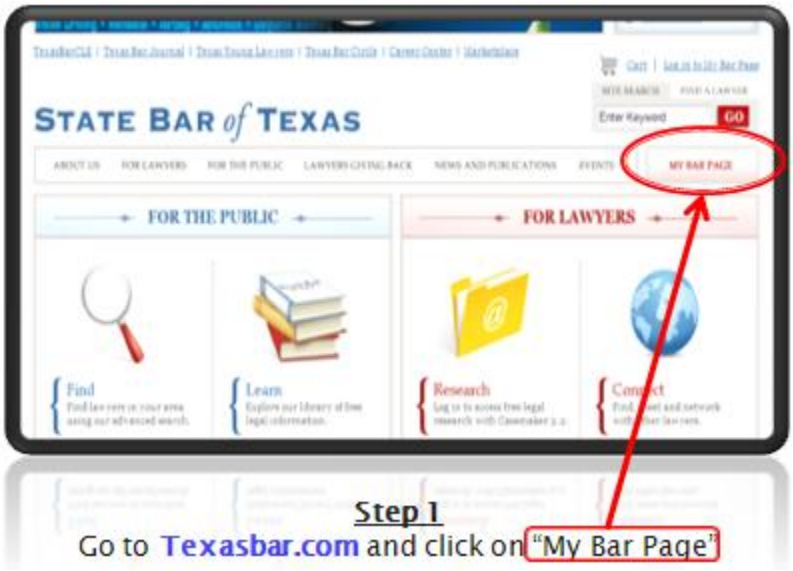
---

6 *J.B. v. G6 Hospitality, LLC*, 2020 WL 4901196, *9 (N.D. Cal. Aug. 20, 2020).

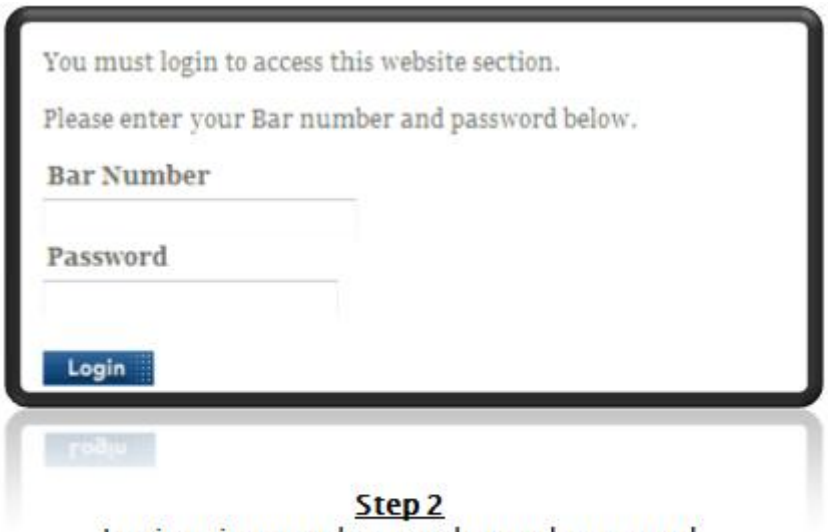
7 In a lawsuit brought against Reddit, Inc., the court determined that the company is not a "content provider," as it is individual users of Reddit submitting content, Plaintiff did not allege that Reddit was responsible at all for the creation or development of CSAM, as is required under the definition of "information content provider," and merely alleged that Reddit *enabled* the posting of CSAM on its website and made it easier for traffickers to view child pornography. *See Doe v. Reddit, Inc.,* No. SACV21768JVSKESX, 2021 WL 4348731, at *1 (C.D. Cal. July 12, 2021) (emphasis added); *See also G6 Hospitality, LLC*, 2020 WL 490119 (where Plaintiff's allegation of participation by Craigslist consisted of Plaintiff's complete creation of the information and Craigslist mere posting of said information.).

How to Join the State Bar of Texas Computer & Technology Section

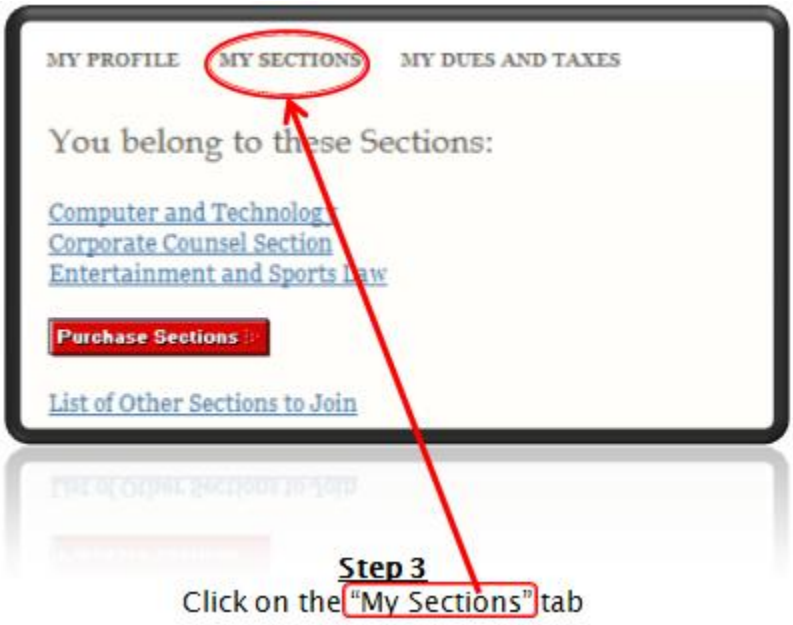
Joining the State Bar of Texas Computer & Technology Section is easy. You can join online by visiting the State Bar of Texas Website at www.Texasbar.com. Please follow these instructions to join the Computer & Technology Section online.



Step 1
Go to Texasbar.com and click on "My Bar Page"



Step 2
Login using your bar number and password
(this will be the same information you'll use to login to the Section website)



If you see "Computer and Technology", congratulations, you're already a member.

If not, click the "Purchase Sections" button and follow the instructions to add the Computer and Technology Section. **Please note: It may take several days for the State Bar to process your section membership and update our system.**

You can also complete this form and mail or fax it in.

State Bar of Texas Computer & Technology Section Council

Officers:

Elizabeth Rogers – Austin – Chair

Pierre Grosdidier – Houston – Chair-Elect

Reginald Hirsch – Houston – Treasurer

William Smith – Austin – Secretary

Shawn Tuma – Plano – Immediate Past Chair

Circuits Editors:

Sanjeev Kumar – Austin

Pierre Grosdidier – Houston (Senior Advisor)

Committee Chairs:

Grecia Martinez – Dallas
– Membership Chair

Chris Krupa Downs – Plano
– App committee Co-Chair

Mark Unger – San Antonio
– App committee Co-Chair

Rick Robertson – Dallas
– Tech in Courts Chair

Seth Jaffe – Houston
– Cybersecurity & Privacy Chair

William Smith – Austin
– CLE Chair

Alex Shahrestani – Austin
– Marketing Chair

Webmaster:

Ron Chichester – Houston

Appointed Judicial Members:

Judge Xavier Rodriguez – San Antonio

Hon. Roy Ferguson – Alpine

Hon. Emily Miskel – McKinney

Term Expiring 2022:

Lavonne Burke Hopkins – Houston

Gwendolyn Seale – Austin

Alex Shahrestani – Austin

Michelle Mellon-Werch – Austin

Term Expiring 2023:

Craig Haston – Houston

Sanjeev Kumar – Austin

Christine Payne – Austin

Mitch Zoll – Austin

Term Expiring 2024:

Justin Freeman – Austin

Zachary Herbert – Dallas

Grecia Martinez – Dallas

Guillermo "Will" Trevino – Brownsville

Chairs of the Computer & Technology Section

2021–2022: Elizabeth Rogers
2020–2021: Shawn Tuma
2019–2020: John Browning
2018–2019: Sammy Ford IV
2017–2018: Michael Curran
2016–2017: Shannon Warren
2015–2016: Craig Ball
2014–2015: Joseph Jacobson
2013–2014: Antony P. Ng
2012–2013: Thomas Jason Smith
2011–2012: Ralph H. Brock
2010–2011: Grant Matthew Scheiner
2009–2010: Josiah Q. Hamilton
2008–2009: Ronald Lyle Chichester
2007–2008: Mark Ilan Unger
2006–2007: Michael David Peck
2005–2006: Robert A. Ray
2004–2005: James E. Hambleton
2003–2004: Jason Scott Coomer
2002–2003: Curt B. Henderson
2001–2002: Clint Foster Sare
2000–2001: Lisa Lynn Meyerhoff
1999–2000: Patrick D. Mahoney
1998–1999: Tamara L. Kurtz
1997–1998: William L. Lafuze
1996–1997: William Bates Roberts
1995–1996: Al Harrison
1994–1995: Herbert J. Hammond
1993–1994: Robert D. Kimball
1992–1993: Raymond T. Nimmer
1991–1992: Peter S. Vogel
1990–1991: Peter S. Vogel