COMPUTER AND TECHNOLOGY SECTION

Circuits

e-Journal of the Computer & Technology Section
of the State Bar of Texas
January 2023

Table of Contents

Stay tuned for our FREE CLE each quarter!

Table of Contents

Letter from the Chair

By Pierre Grosdidier

Dear Section members,

I would like to use this issue of *Circuits* to thank all the dedicated attorneys and judges who partook in the Section's 2022 Technology and Justice for All CLE at the Texas Law Center on December 2, 2022.

Past Section Chair Michael Curran, Council member Grecia Martinez, and Section Administrator Erica Anderson organized the CLE for the Section, along with the dedicated and superb support of the Bar's Tracy Nuckols, Lyndsay Smith Jackson, Paul Burks, Jake Stoffle, and supporting staff.

Judges Xavier Rodriguez and Karin Crump, Past Section Chairs Grant Scheiner, Shawn Tuma, Mark Unger, and Shannon Warren, Current Treasurer William Smith, Council members Grecia Martinez and Mitch Zoll, and guest speaker Natalia Santiago all gave captivating talks on a broad range of topics. Judge Rodriguez also gave us an illuminating opening address.

I can assure all the speakers that we received excellent feedback from the audience.

On behalf of the Section, thank you for your time and commitment to the Section. We all know how much time is required to prepare and deliver such a successful CLE. It sets a high bar for the 2023, but the Section will not disappoint.

We also thank all the attendees, including current and new Section Members. Make plans now to attend in early December 2023!

But it is not over! Please also plan to attend the Section's next two free virtual CLEs. Quentin Brogdon, Partner at Crain Brogdon, will talk about Autonomous vehicles and their litigation risks on February 24, 2023. Charles Mudd of Mudd Law, will talk about Space law: the next legal frontier on April 28, 2023. Digital invitations will follow.

In the meantime, I wish you all a Happy New Year 2023!

Respectfully,

Pierre Grosdidier
2022-23 Section Chair,
Computer & Technology Section
State Bar of Texas

COMPUTER AND TECHNOLOGY SECTION

Letter from the Editor

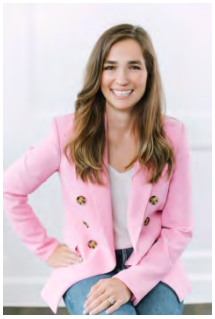
By Sally Pretorius

Cheers to the New Year and welcome 2023! January is always a time for fresh starts and the ability to refocus. The Chinese Zodiac says that we are beginning the Year of the Rabbit, which brings about fluidity and contemplation, which fits right in with this quarters *Circuits*. Many of the topics that are covered this month bring great thought to what has occurred and how it impacts us in the future: the new iOS 16 for Lawyers; how the Capital rioters motion to suppress Facebook action was denied, how drone regulations are being treated; service of process via non-fungible tokens; and a re-print of a wonderful article on e-discovery. Our contributing authors are experts in their areas and hail from some of the most prestigious legal positions and we are so thankful to have their insight and knowledge.

Please take some time to read, contemplate and share these articles. One of the great things of this section is the ability to offer in-depth insight into novel topics.

Kind Regards,

Sally Pretorius,
Co-Editor



Examining Heslin and Lewis v. Infowars and Alex Jones

By Judge Xavier Rodriguez

A. Introduction

On December 14, 2012, Adam Lanza fatally shot 20 children and 6 adults at the Sandy Hook Elementary School in Newtown, Connecticut. It was one of the deadliest school shootings in U.S. history. Alex Jones, founder of InfoWars.com ("Infowars") and host of a news-talk radio program, later aired multiple broadcasts stating that the tragedy was a "giant hoax" created by "crisis actors" on behalf of individuals opposed to the Second Amendment. Implied in these broadcasts was that the family members were lying. Companies and websites associated with Alex Jones have also promoted theories that the United States government either concealed information about – or outright falsified – the 1969 Moon landing, the 1995 Oklahoma City bombing, the September 11 attacks, and the result of the 2020 presidential election. Critics of Alex Jones contend that he has made millions of dollars marketing and advertising products on his websites and that he intentionally promotes his theories to generate revenues.

Below provides a brief background on a lawsuit filed against Jones, Infowars, and related companies and individuals by victims of the Sandy Hook tragedy. This article focuses on the various discovery disputes that arose and what lessons Texas practitioners may learn from this case.

B. Procedural History

On April 11, 2018, counsel for Neil Heslin, the father of one of the Sandy Hook victims[1], sent a letter to Defendants' counsel notifying Infowars and Jones that plaintiffs intended to sue Defendants for defamation. The letter also requested that the Defendants preserve documents regarding Infowars' broadcastings of statements related to the Sandy Hook school shooting. This letter put Defendants on notice that they had a duty to preserve materials related to the shooting. The original petition in this case was then filed in Travis County days later.[2] It did not take long for disputes to arise.

---

1 Other family members also joined this lawsuit.

2 Case No. D-1-GN-18-001835, April 16, 2018.

On July 13, 2018, the Defendants moved to dismiss under the Texas Citizens Participation Act ("TCPA").[3] Before a hearing was held on this motion, the Plaintiffs filed a motion for sanctions, alleging that Defendants intentionally destroyed social media evidence.[4] In this motion, Plaintiffs' counsel stated that a CNN journalist reported that Jones had instructed that several hours of video be deleted from various social media accounts. It was not made clear in the motion whether the video feeds were only no longer publicly available or, indeed, completely deleted. Nor did the motion mention whether the deletions took place before or after the duty to preserve had been triggered in this specific case. In Texas, a party must preserve evidence when a party knows or reasonably should know that a claim might be filed and that evidence in its possession, custody, or control will be material and relevant to that claim.[5] In this case the date that the April 11, 2018, letter was received was the likely trigger date for the duty to preserve.

Plaintiffs also moved to allow discovery, both in response to the TCPA motion and to investigate the allegation that Defendants spoliated certain evidence. The Court granted the motion to conduct discovery[6] and, pursuant to Tex. Civ. Prac. & Rem. Code § 27.004, extended the date for a hearing on the TCPA motion to November 1, 2018.

The Defendants responded by filing

(1) over 100 pages of objections to exhibits relied on by the Plaintiffs in their previous filings,
(2) requests that the Court rule on those objections,
(3) a motion for protective order, and
(4) a notice of appeal.

---

[3] "The purpose of this chapter is to encourage and safeguard the constitutional rights of persons to petition, speak freely, associate freely, and otherwise participate in government to the maximum extent permitted by law and, at the same time, protect the rights of a person to file meritorious lawsuits for demonstrable injury." Tex. Civ. Prac. and Rem. Code § 27.002. "If a legal action is based on or is in response to a party's exercise of the right of free speech, right to petition, or right of association or arises from any act of that party in furtherance of the party's communication or conduct described by Section 27.010(b), that party may file a motion to dismiss the legal action." Tex. Civ. Prac. and Rem. Code § 27.003. This statute, also known as the Texas Anti-SLAPP statute, has been the subject of considerable debate and revised at least once.

[4] August 17, 2018.

[5] Brookshire Bros. v. Aldridge, 438 S.W.3d 9, 20 (Tex. 2014).

[6] August 31, 2018.

In turn, Plaintiffs filed a motion for contempt, arguing that the Defendants openly defied the Court's previous order allowing for discovery by refusing to answer interrogatories and serving lengthy boilerplate objections to all requests for production.

The Texas court of appeals agreed with plaintiffs that the district court had not yet ruled on the motion to dismiss, nor had the motion to dismiss been overruled by operation of law. Accordingly, the court of appeals dismissed Defendants' appeal for lack of jurisdiction.[7] After remand, the trial court heard the TCPA motion to dismiss and denied the motion.[8] Again, Defendants appealed; the court of appeals affirmed the district court's denial of the TCPA motion to dismiss and sanctioned Defendants, awarding plaintiffs $22,250 for attorney's fees.[9]

C. Discovery Disputes & Default Judgment Sanctions

Plaintiffs filed another motion for contempt on July 6, 2021, under the Texas rule of civil procedure addressing discovery sanctions, Tex. R. Civ. P. 215, arguing that the Defendants had still not provided discovery responses. In response, Defendants argued that they "have been working diligently to ensure Defendants' compliance with their discovery obligations," that they had already produced 7,000 pages of documents, and were "continuing to review additional documents to determine if further responsive documents exist necessitating further supplementation."[10] Defendants also argued even though the lawsuit was three years old, "that procedurally, this case is just now in the throes of discovery…"[11] At a hearing, Defendants' counsel allegedly stated that Defendants would supplement their disclosures within 14 days. When no supplementation took place, Plaintiffs moved to compel Responses to Second Set of Discovery Requests and Motion for Sanctions as well as moved for leave to serve discovery on the issue of the Defendants' net worth.[12]

The Court found that the Defendants had

(1) disregarded the Court's previous Order requiring discovery disclosures,

(2) provided no discovery after the June 2021 remand,

---

7 Jones v. Heslin, 587 S.W.3d 134, 137 (Tex. App. – Austin 2019).

8 October 18, 2019.

9 *Jones v. Heslin*, No. 03-19-00811-CV, 2020 WL 1452025, at *6 (Tex. App. – Austin Mar. 25, 2020, review denied Jan. 22, 2021), cert. denied sub nom. *Infowars, LLC v. Marcel Fontaine*, 142 S. Ct. 762, 211 L. Ed. 2d 477 (2022).

10 August 30, 2021.

11 *Id.*

12 The Court granted discovery on net worth on November 5, 2021. *Heslin v. Jones*, No. D-1-GN-18-001835, 2021 WL 6200972, at *1 (Tex. Dist. Nov. 05, 2021).

(3) inadequately produced some documents on August 26, 2021,
(4) failed to make a corporate representative available for deposition, and
(5) failed to fully comply with its discovery obligations.

The Court further found that Defendants had "shown flagrant bad faith and callous disregard" for their discovery obligations and had shown a pattern of discovery abuses across the multiple school shooting cases being actively litigated against the Defendants. The Court concluded that a default judgment was appropriate regarding liability, finding that the discovery misconduct was attributable to the client and not counsel, with the Court noting that the Defendants had been represented by seven attorneys[13] throughout the litigation. The Court also noted that the imposition of lesser sanctions would be inadequate given Defendants' conduct throughout the case.[14]

D. Analysis

A whole set of questions arise concerning the above, particularly whether the trial court's entrance of default judgment was appropriate. "[C]ase-determinative sanctions may only be imposed in 'exceptional cases' where 'clearly justified' and it is 'fully apparent that no lesser sanctions would promote compliance with the rules.'" *Cire v. Cummings*, 134 S.W.3d 835, 840-41 (Tex. 2004). At the time the default judgment was ordered against *all* the Defendants, it is unclear whether the record establishes *all* the necessary elements as to *all* the Defendants.

For example, it is unclear whether the Plaintiffs were prejudiced by the loss of any broadcast videos. The videos were posted on YouTube and other social media platforms, and it is uncertain whether the Plaintiffs already possessed these videos before they were taken down or whether they could have been secured from YouTube and the other platforms.

It was later discovered that Jones possessed text messages in which he discussed the Sandy Hook massacre, but he later, improperly, stated no such text messages existed. Yet it is uncertain at what point Jones' cell phone contents were downloaded, which attorney represented Jones at that time, whether the download was examined for responsive content, and if so, whether any such attorney was also complicit in the attempted spoliation of the text messages.

---

[13] The number of attorneys later escalated to eleven.

[14] An Amended Order was filed with only slight changes made.

Jones filed a motion for reconsideration, arguing that the alleged discovery failures were being asserted against Free Speech Systems LLC and Infowars LLC, but that the Plaintiffs had established no discovery deficiencies attributable to Mr. Jones, individually.[15]

Free Speech Systems and Infowars also filed a multi-prong motion for reconsideration. First, they argued that the Court needed to first determine whether they had any duty to preserve any of the social media associated with the various broadcasts which were the subject of to the litigation. Second, Free Speech Systems and Infowars argued that no evidence showed that these Defendants deleted any relevant data.[16] Alternatively, Free Speech Systems and Infowars appeared to argue that, even if they violated a duty to preserve social media evidence, the appropriate remedy for a violation was to provide a negative-inference instruction to the jury at time of trial instead of a finding of liability.

Fourth, regarding discovery production, these Defendants also argued that they were not in possession, custody, or control of some of the evidence that Plaintiffs requested because the video broadcasts were on YouTube servers. And Defendants argued that even if they possessed the requested data, they already adequately responded to Plaintiffs' requests by producing 85 video broadcasts and 90,000 pages of documents.[17]

Assuming requests for production were made to produce text messages from either Jones, Free Speech Systems or Infowars, it is uncertain which of Defendants' many attorneys were responsible for that discovery production, and why the relevant text messages were not produced. Model Rules of Professional Conduct 3.3 and 3.4 are implicated in the filing of the motions for reconsideration and counsel's responses to requests for production.[18]

The Court ordered Defendants to fully answer certain interrogatories and requests for production (it is uncertain what these discovery requests sought) and ordered that the Defendants pay reasonable costs incurred because of the deficiencies in production.[19]

---

15 December 30, 2021. A similar motion on behalf of Owen Shroyer was filed on this same date. Shroyer was host of the Infowars show "The War Room."

16 December 31, 2021.

17 It is unclear from the court docket sheet at what time Defendants produced these videos and documents.

18 See also Tex. Disciplinary R. Prof. Conduct 3.02 (Minimizing the Burdens and Delays of Litigation), 3.03 (candor toward tribunal), and 3.04 (Fairness in Adjudicatory Proceedings).

19 *Heslin v. Jones*, No. D-1-GN-18-001835, 2022 WL 731748, at *1 (Tex. Dist. Feb. 10, 2022).

Plaintiffs filed another motion for sanctions on March 4, 2022, arguing that the corporate representative designated by Defendants was not adequately prepared to answer questions posed to her. Apparently, the individual designated was not an employee of the corporation but was an attorney retained specifically to serve as the corporate representative. On April 1, the Court granted the motion for sanctions noting that this was the fifth occasion where Defendants failed to adequately prepare an individual for the corporate representative deposition. The Court assessed costs and attorneys' fees as sanctions[20] and ordered that several factual disputes be established in favor of the Plaintiffs and would be reflected in the eventual jury instructions. These jury instructions were later requested to be withdrawn by the Plaintiffs and the Court modified its Order.[21]

Plaintiffs again moved for sanctions, notifying the Court that other lawyers suing the Defendants in other jurisdictions provided them text messages sent by the Defendants related to this matter that had never been disclosed by the Defendants.

As the parties prepared for trial, the Plaintiffs filed a Notice of Nonsuit as to Infowars, LLC, apparently believing that Infowars had no assets. Yet on April 18, 2022, Infowars (but no other active defendant) filed for bankruptcy and Defendants' counsel filed a Suggestion of Bankruptcy in the state case. The Bankruptcy Court remanded the case to the state court on May 24, 2022. Consequently, on May 31, Plaintiffs filed yet another Motion for Sanctions arguing that Infowars represented to Plaintiffs that it had no assets but stated to the bankruptcy court it owned intellectual property rights with an unknown current value.

During trial, Jones was on the witness stand and being subjected to cross-examination by the Plaintiffs' lawyer, Mark Bankston. After testifying that he had searched his cell phone for any text messages about the Sandy Hooks shooting, Jones claimed he found none. Bankston then informed Jones that "12 days ago" Jones attorneys "messed up" and sent the Plaintiffs' lawyers "an entire digital copy of your entire cellphone with every text message you've sent for the past two years." [22] Apparently, text messages about Sandy Hook were found within that production,

---

[20] *Heslin v. Jones*, No. D-1-GN-18-001835, 2022 WL 2463552, at *1 (Tex. Dist. Apr. 15, 2022).

[21] April 18, 2022.

[22] It has been reported that Jones's attorney, Andino Reynal, or his legal assistant sent Plaintiffs' counsel a Dropbox link containing a supplemental production that included the cell phone contents about two weeks before trial. See Hilary Gerzhoy, et al., Ethics Lessons from the Alex Jones Discovery Debacle.

impeaching Jones's testimony that he had no text messages on the topic.[23] Defendants' attorneys did not object to this line of cross-examination at trial.

This revelation raises other questions. First, why did Defendants' counsel provided these documents on the eve of trial when default judgment already been granted against all the Defendants on the liability issue? At that stage in the trial, the trial evidence could only speak to damages; was there evidence of Defendants' net worth or Plaintiffs' damages present on the cell phone? Second, why did Defendants' counsel produce the entire cell phone's contents, rather than producing only what may have been relevant to damages?[24] Third, what, if any, privileged information was contained in that production? Finally, did Texas law as stated in *Brookshire Bros.*[25] prohibit Bankston from raising spoliation issues before the jury, and did Reynal waive any error by not objecting?

Before trial, Bankston apparently informed Jones's lawyer of the inadvertent production after Bankston received the documents. When Bankston informed Reynal of the cell phone production, Reynal replied "please disregard" and that he would work on preparing a new link, but he never did. But under Texas law, did Bankston have any obligation to inform Reynal of the mistake?

After the jury awarded $4.1 million in compensatory damages and $45.2 million in punitive damages, Reynal filed a motion for mistrial, citing the cell phone mishap. The Court denied the motion.[26] In an emergency motion, Reynal argued that Bankston's use of the text messages violated "various privileges," a court protective order,[27] and a Texas "snap back" provision.

---

[23] Besides cell phone data, apparently Defendants' counsel also sent medical records associated with plaintiffs in a Connecticut lawsuit to Heslin's attorneys via the same Dropbox. Reynal has now been ordered to appear in that court to show cause why he should not be referred to disciplinary authorities for that breach of confidential medical records.

[24] This conduct implicates Tex. Disciplinary R. Prof. Conduct 1.01, cmt. 8 (Competent and Diligent Representation and competence in the practice of law, including the benefits and risks associated with relevant technology), 1.05 (Confidentiality of Information).

[25] "[T]here is no basis on which to allow the jury to hear evidence that is unrelated to the merits of the case, but serves only to highlight the spoliating party's breach and culpability. While such evidence may be central to the trial court's spoliation findings, it has no bearing on the issues to be resolved by the jury." Brookshire Bros., 438 S.W.3d at 26-27.

[26] As an aside, the trial court also authorized Bankston to release Jones' text messages to the U.S. House of Representatives Committee investigating the January 6, 2021, attack on the Capitol.

[27] This order merely stated that a party could mark a document as confidential, and if a party disputes that classification the matter could be brought to the Court's attention for resolution.

Reynal argued that a paralegal in his firm intended to send a link containing text messages and documents filed in another related lawsuit (the Lafferty matter), but mistakenly sent a link pointing to Jones' cell phone.[28] Reynal further argued that the material was clearly confidential and should be returned. Reynal did not adequately explain why all the documents in this inadvertent production should be returned as confidential. Indeed, the text messages sent by Jones about the Sandy Hook matter do not appear to fall within any privilege.

In many jurisdictions outside Texas, a version of ABA Model Rule 4.4(b)[29] applies to accidental or mistaken disclosures. In those jurisdictions, attorneys who receive documents or data that was inadvertently produced must notify the sender of the inadvertent production. Texas Ethics Opinion No. 664, however, has stated that failure to notify an opponent does not violate the Texas Disciplinary Rules of Professional Conduct. Outside the ethical rules, Texas Rule of Civil Procedure 193.3 addresses the issue of what a producing party should do when discovering it has inadvertently produced privileged information. Under Rule 193.3, a party that inadvertently produces privileged information does not waive privilege if within ten days of discovering the mishap the producing party then asserts the privilege. The rule implies that the privilege assertion is completed by filing amended discovery responses, but it remains to be seen whether informal methods suffice.[30]

Again, because the production was not disclosed the public and the record itself is unclear, it is unknown whether any privileged – rather than merely incriminating – information was contained within the cell phone production. It also remains to be seen whether Reynal's "please disregard" reply to Bankston's notification satisfied Rule 193.3, or whether Reynal will be found to have waived the issue by failing to object to the cross-examination about the cell phone content. If there was no privileged information contained on the cell phone, this whole issue is

---

28 Defendants' Emergency Motion filed August 4, 2022.

29 "A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender."

30 "A party who produces material or information without intending to waive a claim of privilege does not waive that claim under these rules or the Rules of Evidence if – within ten days or a shorter time ordered by the court, after the producing party actually discovers that such production was made – the producing party amends the response, identifying the material or information produced and stating the privilege asserted. If the producing party thus amends the response to assert a privilege, any party who has obtained the specific material or information must promptly return the specified material or information and any copies pending any ruling by the court denying the privilege."

a red herring. Likewise, any reference to a breach of any protective order is moot if any of its contents were not "confidential information" subject to the agreed upon order.

"[E]vidence bearing directly upon whether a party has spoliated evidence is not to be presented to the jury except insofar as it relates to the substance of the lawsuit." *Brookshire Bros.,* 438 S.W.3d at 14. Nonetheless, pundits debate whether Bankston should have discussed spoliation of text messages before the Texas jury.[31] Depending on the specific cross-examination questions, the exchange could be construed as impeachment evidence. Statements, however, about how Jones' attorneys erred were likely improper. Again, however, any objections to these statements may have been waived.

E. Conclusion

This case highlights the necessity for attorneys to understand technology or to associate with individuals or vendors who can assist in the identification, preservation, review, redaction for privilege, and production of relevant documents and data. This case also demonstrates that once a duty to preserve relevant evidence has been triggered, severe consequences may result from the failure to take reasonable steps to ensure that relevant documents and data are preserved and then produced.

This case also underscores the need to marshal arguments and evidence in support of any spoliation-related motions to compel, motions for protective orders, or motions for sanctions. The bar to establish spoliation in the Texas state courts is high. The Texas Supreme Court requires a close fit between the misconduct and the error and has clearly stated that "the remedy crafted by the trial court must be proportionate when weighing the culpability of the spoliating party and the prejudice to the nonspoliating party." *Brookshire Bros.*, 438 S.W.3d at 21. To avoid reversals on appeal, parties must explain to the trial court when the duty to preserve was triggered, the scope of the relevant data that should have been preserved, how any discovery productions were deficient, the resulting prejudice from the destruction of evidence, and whether any failure to produce relevant data resulted from negligent acts or intentional spoliation. Although it may be clear that improper behavior took place, the prudent practitioner will ensure that any future appellate record will be clear in establishing that spoliation occurred, and that the relief awarded by the trial court was proper.

Until litigants and their attorneys comply with all applicable ethics rules and moral principles, inadvertent productions, however, are sometimes the only means to prove spoliation

---

[31] *See* Craig Ball, More Questions re: Alex Jones Defamation Case, August 5, 2022.

occurred.[32] Parties suspecting spoliation or inadequate productions should be prepared to collect sufficient evidence through deposition testimony or affidavits that show relevant, unique documents or data once existed, has not been produced, and that a duty to preserve existed that has been breached. This challenge must be balanced with proportionality arguments and a judicial disinclination for "discovery on discovery." Parties hoping to avoid reversal cannot make conclusory spoliation accusations.

About the Author

Judge Xavier Rodriguez is a United States District Judge for the Western District of Texas and a Judicial Liaison to the Computer and Technology Section.

[32] See *Bellamy v. Wal-Mart Stores, Texas, LLC*, No. SA-18-CV-60-XR, 2019 WL 3936992, at *1 (W.D. Tex. Aug. 19, 2019) (inadvertent production by paralegal established the concealment of discovery by defense counsel).

Service of Process Via NFT: A Novelty or a Natural Next Step?

By Hon. John G. Browning

So you just had the opposing party served with process using a real, flesh and blood human being—how very quaint and 20th century of you. For more than ten years now, courts all over the world have permitted, under the right circumstances, substituted or alternative service to be accomplished using social media platforms. Courts in eight countries, including the United Kingdom and multiple jurisdictions within the United States, have permitted such service. Some American states, like Texas, have even passed statutes specifically addressing this form of service and setting forth rules governing the practice. As one federal judge in New York observed nearly ten years ago in blessing the "relatively novel concept" of service by Facebook, "history teaches that, as technology advances and modes of communication progress, courts must be open to considering requests to authorize service via technological means of then-recent vintage, rather than dismissing them out of hand as novel."[1]

Judge Engelmayer's words have proven prophetic, since 2022 may have ushered in the next step in technology-assisted service of process: perfecting service via the transfer of non-fungible token (NFT) on the blockchain. On June 2, 2022, the Supreme Court of the State of New York granted an order permitting service of court documents via the airdropping of a token on the Ethereum blockchain in the case of *LCX AG v. John Does Nos. 1-25*. This "service token" was to be served on the anonymous person(s) controlling an Ethereum address via airdropping, with the token containing a hyperlink to a website on which the court papers were published.

The case itself features the plaintiff LCX, a Lichtenstein-based virtual currency exchange, bringing an action for unauthorized access to and theft of nearly $8 million worth of virtual assets from its digital wallets by 25 anonymous "John Doe" defendants. LCX's attorneys at Holland & Knight had traced a $1.3 million portion of the cryptocurrency to a single wallet address on the Ethereum blockchain, but were unable to identify who controlled that address. Ethereum blockchain employs smart contracts that hold the terms of agreements between buyer and seller directly written into lines of code, allowing participants to transact with each other without a central authority like the Federal Reserve System. Even though the defendants

[1] Fed. Trade Comm'n v. PCCare247, Inc., 2013 WL 841037 (S.D.N.Y. Mar. 7, 2013).

had taken various steps to obscure the transaction trail, LCX's lawyers were able to trace at least that portion of the stolen crypto assets.

Concerned that the defendants could sell or transfer the remaining virtual currency at any time, LCX's attorneys sought a preliminary injunction prohibiting such a transfer. They then had to convince a judge of the difficulty in serving the anonymous defendants, after demonstrating that the blockchain showed that the defendants had recently conducted transactions while holding the virtual currency. Fortunately, New York Supreme Court Justice Andrea Masley had educated herself on blockchain issues, and realized that LCX's counsel had provided the court with a mechanism by which the defendants would have notice of the proceedings. Justice Masley issued an Order to Show Cause, noting that the service token's hyperlink would take the defendants to a site with all court documents (including the Order itself), and that this service hyperlink included a means to track when a person clicks on the hyperlink. The court's order stated that "Such service shall constitute good and sufficient service for the purposes of jurisdiction under NY law on the person or persons controlling the Address."

Airdropping tokens from one wallet on the blockchain to another party's wallet is hardly new—it is a method used to transfer cryptoassets to existing holders of NFTs, often as a goodwill gesture (as when holders of the notorious "Bored Ape Yacht Club" NFTs were airdropped a proprietary "Ape Coin" token in March 2022). But transmission of tokens on the blockchain was rarely, if ever, used for communication purposes. Yet as LCX's lawyers reasoned, there is no reason it cannot be done—after all, NFTs are simply digital packets of information, which may include links to media files hosted elsewhere online. This new method of service bypasses the weaknesses inherent in serving an anonymous defendant through in-person contact or even in a text message, since the location of the defendants and the smartphones they operate remains unknown.

As LCX's counsel explained afterward, their proactive and innovative use of "Web 3.0" was a necessity due to the nature of the crypto space. Frequently, in cases involving theft or fraudulent transfer of virtual assets, anonymity poses a challenge: the only identifier is the wallet address of the receiving entity. "We enacted a mechanism provided by the court that presumes that he will have notice of this, even if he does not ever access the address," they stated. "If he just sticks his head into the sand and never accesses it again, that's the equivalent of him saying 'I'm not going to open that email and that will prevent me from being served.'" As a result of the court's order, the defendants must appear and present evidence to contest the freezing of their assets stashed in the Ethereum blockchain address.

As novel as this approach is, the question remains—would other courts, including those in the United Kingdom, be similarly receptive? As it turns out, the answer is yes. After all, as far back as October 2009, in an unreported case (*Blaney v. Persons Unknown*), Lewison J. permitted service of an injunction via Twitter. Alternative service via Facebook, Instagram, and the "contact" section of a defendant's website has been authorized as well under CPR 6.15.[2] And in recent cases involving cryptocurrency fraud, a British court has ordered alternative service by email.[3] While this form of service might be viable in cases where the claim is against a cryptocurrency exchange or against a wallet for whom the exchange holds personal information like the user's email address, it will not work in situations where the wallet address itself is the only form of identifier.

In July 2022, in the case of *D'Aloia v. Binance Holdings and Others*, the High Court of England and Wales addressed the anonymous defendant issue, and granted an order permitting service of court proceedings via the transfer of an NFT on the blockchain. Fabrizio D'Aloia, an Italian engineer and the founder of Microgame (an online gambling joint stock company) asserted claims against four cryptocurrency exchanges holding virtual funds of his—Binance, Polo Digital Assets, Aux Cayes Fintech, and Bitkub Online—along with software company Gate Technology. The order issued by the Court granted permission for D'Aloia to serve the five cryptocurrency exchanges by means of an NFT airdropped to the two wallets into which he had initially deposited his cryptocurrency (in addition to service by email).

Both the U.S. and U.K. cases are significant for a number of reasons. First, much like earlier cases in which alternative service via email and, later, social media was permitted, service via NFT on the blockchain breaks down one of the key barriers in bringing a claim—being able to locate the anonymous defendant. Such cases also open the door to potentially wider applications of such technology, with digital service over the blockchain being used for safe, tamper-free disclosure of documents, digital signatures (private key signatures could eliminate arguments of fraud or false signatures), and even dispute resolution on smart contract platforms. Finally, the use of NFTs under the right circumstances removes the need for third-party verification, just as blockchain itself has helped transform the definition of "ownership" as we know it today. In the future, parties might even contractually agree to be served in this manner; conceivably, such a clause could be embedded as code with smart contracts, in which the parties authorize service of court papers on a specific wallet address. In the United

---

2 *See, e.g.*, Pirtek (UK) Ltd. v. Jackson (2017) EWHC2834 (QB).

3 Danisz v. Persons Unknown and Huobi Global Ltd. (T/A Huobi) (2022).

Kingdom, for example, CPR 6.11(1) allows service "by a method or at a place specified in the contract."

But perhaps the greatest significance of both of these 2022 cases is that they reflect a continued willingness on the part of courts to tackle the challenges that emerging technologies can present to the legal system, at least in the sense of adapting our means of service to match technology. While the law can never hope to keep pace with technological innovation, it has to at least try. Indeed, in cases with fact scenarios like the *LCX* and *D'Aloia*, the fact that the defendants could not be identified and all the complaining party had was a number left very few options but to proceed with alternative service.

There are still questions to be raised regarding service of process via NFT. For example, when is service deemed effective—upon transmission of the token into the defendant's wallet, or not until the recipient clicks on the service hyperlink? According to the approach taken by both the U.S. and U.K. courts, transmission is the necessary step for service to be perfected, but other courts may be more insistent on evidence of the defendant's interaction with the token. This may present a problem, since it is becoming increasingly common for blockchain wallet owners to see malicious tokens being airdropped into their wallets in a Web 3.0 version of phishing. Wary wallet owners can hardly be faulted for their hesitance in interacting with airdropped NFTs or in clicking on hyperlinks from unfamiliar sources. Under such circumstances, how effective will a airdropped token be at providing actual notice of the proceedings or the court documents being served?

Traditional forms of service are not going away anytime soon. Yet as we have already seen with service of process via social media, it is important for lawyers and judges to remain open-minded about technology's benefits and clear-eyed about its risks.

About the Author

Hon. John G. Browning is a partner in the Plano office of Spencer Fane, and a former Justice on Texas' Fifth District Court of Appeals. He also serves as the Distinguished Jurist in Residence at Faulkner University's Thomas Goode Jones School of Law, and as the Chair of the Institute for Law & Technology at the Center for American and International Law. The author of 5 books and more than 50 law review articles, Justice Browning is a graduate of Rutgers University and the University of Texas School of Law.

FAA Drone Regulation Survives Constitutional Challenge

By Pierre Grosdidier

Drones are fun toys and increasingly useful work tools, but that does not mean that they are safe and that they cannot be nuisances or even threats to society. With that in mind, Congress enacted legislation in 2016 and 2018 requiring the FAA to develop drone regulations. In response, the FAA promulgated a Remote Identification (Remote ID) Rule that requires drones to broadcast the digital equivalent of a vehicle license plate. The Rule applies to drones weighing over 0.55 pounds (250 grams) and takes effect on September 16, 2023.

Tyler Brennan, a drone user and retailer, facially challenged the Rule's constitutionality under the Fourth Amendment.[1] He argued, *inter alia*, that the Rule interfered with his reasonable expectation of privacy without requiring a warrant, and that it allowed the government to easily and inexpensively track drone operators without judicial oversight. The D.C. Circuit Court of Appeals rejected all his arguments.

The Remote ID rule requires drones in flight to publicly broadcast their serial number, their location and velocity, the location of their control station, a time stamp, and any applicable "emergency status" flag like low fuel or battery. The location data consist of the device's latitude, longitude, and geometric altitude.[2] The rule does not apply to drones that are flown indoors or within a netted enclosure. The drone's data can be captured and displayed by Apps on smart devices within signal range, so anyone with an App can be made aware of drones' presence around them, and irresponsible operators can be identified and held to account.

Separately, the FAA collects drone owners' personally identifying information when owners register their drones, but this information is confidential and protected by the Privacy Act, 5 U.S.C. § 552a. A drone's flight data can only be matched to these non-public records by authorities "when necessary and relevant to a[n] FAA enforcement activity" and within legal and constitutional bounds.[3] The Rule also does not contemplate public actors recording and storing drone flight data.

---

1 *Brennan v. Dickson*, 45 F.4th 48, 53–54 (D.C. Cir. 2022). This article does not address Brennan's procedural challenges to the Rule, which the Court also rejected.

2 *Id*. at 59.

3 *Id*. at 53–54 (citations omitted) (bracketed term in original).

Under *Katz v. United States*, a Fourth Amendment search occurs when the government intrudes on a person's subjective expectation of privacy that society accepts as reasonable under the circumstances. Here in *Brennan v. Dickson*, the Court reasoned that drones are no exception to the rule that pilots generally have no reasonable expectation of privacy in flight activities that they conduct outdoor in public view.[4]

The Court also noted that the Rule requires the broadcast of drone flight information to the public, not its tracking and storage by the government for later law-enforcement querying. Technology implicates the Fourth Amendment only when it is exploited, not merely because it exists. Moreover, the brevity and local nature of a drone's flight mean that flight data are nowhere as threatening to privacy as the wealth of personal information in a smart device.[5] Drone data broadcasts result in no physical trespass and cannot provide an "intimate window into a person's life" as can cell phone tracking data.[6]

Finally, the personal information that the FAA gathers from drone owners, like name, address, and phone number, remains protected through the Privacy Act. Remote ID does not disclose any of this information to the public. The FAA may only match drone data to owner information when issues arise related to the safety and security of the drone's operation. Even then, use of drone data by the FAA and law enforcement authorities acting with the FAA must comply with all Constitutional and legal safeguards. As things stand, the Rule would have to be changed to allow law enforcement authorities to access the FAA's database to match flight data to owner operation "for uses beyond aviation safety and security." The Court, therefore, rejected Brennan's claim that the Remote ID Rule amounted to a warrantless intrusion into drone owners' "constitutionally cognizable privacy interests."[7]

---

4 *Id*. at 61 (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

5 *Id*. at 62 (citing *United States v. Jones*, 565 U.S. 400, 430 (2012) ("relatively short-term monitoring of a person's movements" in public places recognized as reasonable) (Alito, J., concurring)).

6 *Id*. at 62–63 (citing *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018)).

7 *Id*. at 64–65.

About the Author

Pierre Grosdidier 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 Chair for 2022–23.

iOS 16 for Lawyers

By Lisa Danley

Operating software updates are a headache. They hijack my phone for what feels like an hour (ok, ok, it's probably only about .2 hour) and then change the layout and *feel* of my phone, which is the command center for most of my work.

Fortunately, the iOS 16 update has a lot of useful features for attorneys that will certainly make the pains of adjusting to a new software update very worthwhile. Here are a few that ought to be worth your time:

Unsending Text Messages:

My phone loves to sabotage me by making absurd autocorrects, and I am embarrassed to say that I've sent plenty of typos in text messages to clients. iOS 16 finally provides us with the opportunity to edit texts for up to 15 minutes after sending. You can also unsend a text message within two minutes of sending. As a family law practitioner, I can immediately see the downside to how this might affect evidence between parties, but for the time being, I am enjoying being able to at least correct my flagrant typos.

In order to edit or unsend a sent message, you have to "hard press" on the message bubble just as though you were going to give the bubble a thumbs up, heart, etc. A menu will appear and you will have the option to "edit." Simply, make the changes you want and press the check mark to save the changes.

Reminders for Emails and Unreading Texts:

I admit that I am sometimes better at responding to text messages in my head than on my phone, which is why the new "Remind me Later" feature has been very helpful to me. This feature is available for your email, which will allow you to choose when the email resurfaces at a later date. This feature also allows you to schedule an email delivery, much like you can with Outlook.

Additionally, this new email feature allows you to mark a text message as "unread" to remind yourself to come back to it.

Lock Screens and Focus:

Apple introduced Focus last year, and it's been very helpful to be able to filter the information and notifications I receive while I am in mediation, depositions, or other times when I can only respond to legitimately urgent communications. Apple has improved this technology by adding the option to create a new lock screen and connecting certain focus modes to certain lock screens. Now you can create multiple lock screens each with custom rules for what kind of communications you are notified about. This means you can have a courtroom lock screen, a mediation lock screen, or an afterwork lock screen, which helps me keep my work life balance in check.

Safety Check:

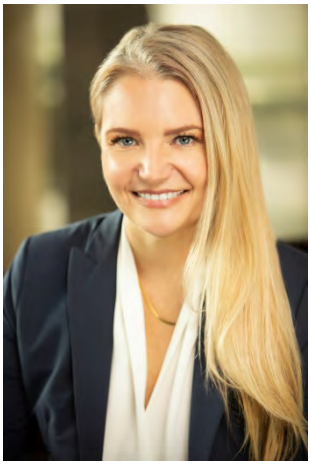
A feature that is helpful to anyone, but in particular family law clients, is the iOS 16's Safety Check. Safety Check allows a user to immediately cut all shared access to your accounts and data in a dangerous situation. This feature also has an "emergency reset" option that will automatically and instantly reset who has access to your messages, location, apps, and other information.

Lockdown Mode:

Another safety-like feature of iOS 16 is a Lockdown Mode. The iPhone's warning describes this feature as an "extreme" measure to prevent against cybercrimes, including types of crimes that happen without any user interaction, also known as "zero-click attacks." Apple was right to address this as these kinds of attacks are invisible to the user and prey on heavily used core features of the iPhone like texts messaging and web browsing. If you find yourself in Lockdown Mode, you will notice that some of your phone's features are not available, like Shared Photos and the link preview in text messages. Lockdown Mode is intricate so I will spare you an article-within-an-article, but I encourage you to research this so that you understand the benefits of it in the unfortunate event you ever need to use it.

iOS 16 update is available for downloading and running on most iPhone 8 (2017) or later models, but some of the features of iOS 16 will work best (or only work) on newer iPhone models that contain the A12 Bionic Chip or newer technology. Apple has announced that they are ending software support for the iPhone 6S Plus, iPhone SE, iPhone 7, and iPhone 7 Plus; so if you own one of these iPhones, it is time to consider an upgrade.

About the Author



Lisa Danley is a partner at Danley Bergia, PLLC (https://danleybergia.com/) where she practices family law. Like most family law attorneys, she sees how technological advances in devices such as phones has a direct impact on the life of clients and their legal matters.

Understanding our Wireless World

By Dawson Lightfoot

What are invisible, manmade, passing through your body while you are awake and asleep, and essential modern components to our daily lives? One good answer is *radio signals*! The reason why the answer was not radio waves is because nature itself also generates radio waves. Although radio signals and radio waves are both *electromagnetic radiation*, *radio waves* may or may not carry useful information, whereas radio signals are radio waves that are *modulated* or otherwise controlled in a manner intended to carry useful information. Some may, nonetheless, argue that nature's radio waves are signals that we happen to not yet understand, and they are probably not wrong.

The term, radiation, raises red flags for most people, and rightfully so. However, it is helpful to differentiate ionizing radiation (which includes nuclear radiation) from non-ionizing radiation. *Ionizing radiation* consists of subatomic particles or electromagnetic waves that have sufficient energy to ionize atoms or molecules by stripping electrons from them (such as damaging DNA and other cellular structure). This type of radiation is a clear threat to living organisms and is the classical type of bad radiation to protect against. On the other hand, the US Occupational Safety and Health Administration (OSHA) has explained *non-ionizing* radiation, the type that is ubiquitous in our lives, as "waves composed of oscillating electric and magnetic fields traveling at the speed of light…" that "includes the spectrum of ultraviolet (UV), visible light, infrared (IR), microwave (MW), radio frequency (RF), and extremely low frequency (ELF)." OSHA further states that, if not properly controlled, these forms of radiation can pose a considerable health risk. Both types of radiation are utilized by industry, and each carry their own special safety burdens. For example, we wear leaded covers to shield against unwanted x-rays exposure and cell phone manufacturers publish time limit recommendations for use. The CDC even suggests use of hands-free headsets.

It is helpful to understand that radio waves form only a small portion of the entire *electromagnetic spectrum* that additionally includes infrared light, visible light (generally perceptible to humans), ultraviolet light (think sun exposure and solar energy), x-rays, and gamma rays. Electromagnetic waves are differentiated from each other based on how many times per second they, for lack of a simpler explanation, wiggle. The unit of measurement of that wiggling is called hertz, where a single hertz is equivalent to one full cycle per second.

Therefore, a local FM radio station of 90.1 MHz means that the signal is *oscillating* at a *frequency* of 90.1 million cycles per second.

In 1865, considering that many frequencies of radio waves can travel around the world and to promote interoperative use of the radio frequency (RF) portion of the electromagnetic spectrum amongst nation states, the United Nations established the International Telegraph Union that is now the International Telecommunication Union (ITU). The ITU and other bodies generally somewhat arbitrarily divide the RF spectrum into sections for ease of discussion, with each section or *band* being a factor of ten (*order of magnitude*) different from the adjacent band. The bands extend from 3–30 Hz (extremely low frequency or ELF) to 300–3,000 GHz (tremendously high frequency or THF) and are labeled Bands 1–12 by the ITU. The bands traditionally recognizable by consumers have been 3–30 MHz (high frequency or HF), 30–300 MHz (very high frequency or VHF), and 300–3000 MHz (ultra-high frequency or UHF), with cell phones operating at ~900 MHz and original Wi-Fi around 2.4 GHz. More recently, increasingly higher bands are being utilized for consumers and industry, with newer Wi-Fi frequencies used in residential settings falling in the 5–7 GHz range (within the super high frequency or SHF band).

Of course, RF spectrum use within the United States is regulated by the Federal Communications Commission (FCC). In March 2022, the FCC rechartered its World Radiocommunication Conference Advisory Committee under the Federal Advisory Committee Act (FACA) to provide the FCC with advice, technical support, and recommended proposals for international frequency spectrum coordination efforts.

In November 2023, the ITU will assemble in Dubai to hold the next World Radiocommunication Conference (WRC) that is generally held every four years. A light review of the published WRC-2023 agenda reveals that work will be conducted on several matters of general impact. Some interesting topics that will be addressed include unmanned aircraft systems (UAS) control needs, mobile satellite internet (think Starlink service while on the move), International Mobile Telecommunications (IMT) systems for consideration as fixed wireless broadband on a primary basis (think broadband by cell frequency as a primary internet service in developing countries and rural areas), use of high-altitude platform stations as IMT base stations for providing mobile-broadband connectivity (think pseudo-satellites at fixed points 20–50 km above the Earth), RF issues regarding communications for sub-orbital vehicles, and removing restrictions on cell phone use while in flight!

Knowing these basics about radio frequencies and bands can help you better understand and appreciate how wireless communications are managed and put to use for us all. Further, some of this information may bolster your knowledge as a consumer, enabling you to better differentiate how new equipment may differ in performance or compatibility. Undoubtedly, the content here will continue to appear in science and technology news that often rely on breakthroughs in use of RF spectrum.

About the Author

Dawson Lightfoot is an experienced Registered US Patent Attorney practicing through his firm, Lightfoot & Alford PLLC. He is an Associate of $(ISC)^2$ via CISSP exam (a rare cybersecurity credential for an attorney), a Certified Information Privacy Professional (CIPP/US), and he will soon launch a new firm, Red Hat Law, to offer cybersecurity and data privacy legal services. He is a Council Member of the Computer & Technology Law Section of the State Bar of Texas, a board member of the North Texas Chapter of the Information Systems Security Association, and is founder and President of the Park Cities Amateur Radio Club.

The Tactical Ediscovery Data Processing Workflow that Streamlines Document Review

By Brett Burney

Reprinted with permission from the Nextpoint Modern E-Discovery Blog.

This ediscovery processing workflow lays out four steps that will help you reduce the volume of discovery data and streamline document review.

Between *collecting & preserving* electronically stored information (ESI) and *reviewing & producing* it, many people regrettably overlook the **critical steps involved in *processing* the data**. If you're tempted to remain oblivious to the workflow of ediscovery data processing, you will overlook opportunities to gain better insight into the collected files, to minimize the costs involved for review and production, and to streamline the logistics of the project. **Here are the steps you need to keep in mind for a successful ediscovery processing workflow.**

As a legal practitioner, you understandably want to start looking at files and documents as soon as possible so you can start developing your legal strategy. You want to see who was talking to whom, what they were saying, and generally gain a better, high-level understanding about the people, places, and events involved in the matter. This Early Case Assessment (ECA) also involves helping your clients understand the legal risks as well as the costs of the matter.

In today's litigation world, a massive cost component revolves around the amount of data that must be collected, processed, reviewed, and produced. We refer to this as Early Data Assessment (EDA), where the data processing phase gives you the ability to comprehend the amount of data involved in the matter so you can better inform your client about the time, effort, and costs required.

Legal teams may prefer to use specialized ECA software to get the full benefits of the processing stage, especially when dealing with large data volumes. For example, Nextpoint recently launched Data Mining, an Early Case Assessment software that offers all the tools you need to follow this ediscovery processing workflow and dive deep into your data.

Step 1: Normalizing Your Data (There's No Such Thing as Normal Data!)

The first step in an ediscovery processing workflow is to "normalize" all the collected data so that the review is consistent and straightforward. For example, when you're looking at a glob of email, Word documents, PDF files, pictures, sound recordings, spreadsheets, and more, you

need to ensure that you can read and see and hear all those files in an approachable manner. It seems like it shouldn't be complicated, but it's important to accurately identify every file type so they can all be properly formatted for your viewing pleasure.

For email, we also have to ensure all attachments are linked to their proper messages (what we call the parent/child relationship). Even more important, we need to "normalize" the time zones associated with all the messages. If we processed all the emails as per the time zone where you practice law, there's a possibility that you would find emails sent *after* they were received, which is obviously confusing (even more confusion when we factor in Daylight Savings Time or international time zones). For this reason, we usually process everything according to Universal Coordinated Time (UTC), and you'll need to be comfortable with that format.

Additionally, we have to make sure any zipped/compressed files are uncompressed and properly listed. And we have to extract any embedded objects that might have been inserted into Microsoft Word documents or Excel spreadsheets. Another important step is to assign each file a "DocumentID" or control number so we can provide analytics and audit trails in the platform. Note this is NOT a Bates number, since those are typically assigned when you generate a production set.

Step 2: Metadata Extraction and File Culling (De-Mystifying the Content)

While lawyers are understandably focused on reading the *content* of emails and documents, **it's critical that all of the metadata from those files is properly extracted so that it can all be populated into a database**. The processing stage extracts all the information from the From, To, CC, BCC fields, along with the Sent & Received dates/times, the Subject line, and several more properties such as whether the message was opened or replied to, and what conversation thread it belongs in. Having all the metadata extracted into a spreadsheet-like database view means you can easily sort and filter data to focus on just the communications you need to investigate.

But even before you look at the metadata, **there are several critical filters that the data must go through so you're not wasting time looking at files that don't contain any content**. There are hundreds of thousands of computer "system" files that sometimes get swept up in the collection process, and there is typically no reason you need them for the purposes of litigation.

The data processing stage will "De-NIST" and cull out those files. The "NIST" here refers to the National Institute of Standards and Technology, which maintains the National Software

Reference Library (NSRL) that catalogs the digital signatures of files in known software applications. Any software executable file or other system file that would appear as gibberish in a review database is De-NISTed according to that official list.

Your ediscovery processing workflow should also include deduplicating files, and this is where you need to provide some input to your vendor. Let's say you've collected emails from 10 different individuals/custodians, and you realize each of those 10 individuals may have received the same email – do you want to read that same email message 10 times? Or would you rather the duplicates be removed with an indicator to each individual who received that message? These are important decisions you need to discuss with your vendor, who can help you understand your options so you get what works best for your review needs.

Lastly, this is the step where any **non-searchable files are OCR'd so they are readable and searchable** in the platform. There may be some scanned paper documents or pictures that contain text that humans can read, while the computer has to attempt to recognize that text for searchability. A computer can try to OCR handwriting, but just know that it won't be perfect, which means your searches may be incomplete.

Step 3: Indexing and Searching (You Can't Search What You Don't Index)

When attorneys think about "searching" documents, they envision typing in a word and having the computer check for that word in every single file. You can't be blamed for visualizing the task that way, but the reality is that it would take so long for a computer to search every document that it would be a time-wasting disaster.

Instead, when you type in a word and hit the search button, **the computer is actually scanning an "index" or dictionary of words that has been generated based on all the words found in the files during the data processing stage.** That way, it's only searching for words found in the files you collected, and it only has to inquire with that index rather than laboriously explore every document every single time. This is much more efficient and gets you the results you're looking for in fractions of a second. The index knows every file where a word is found, and so it can highlight your search terms in the files during your review.

But there's a flip side to this – in order to be most efficient and avoid human impatience, many search indexes will ignore the most common words such as *and*, *to*, *is*, etc. These "noise" words or "stop" words show up at an astronomically higher rate than all other words. Since we're usually not searching for those conjunctions, determiners, and prepositions, the indexes will just completely ignore them.

This is standard procedure, but you should be aware of these limitations if you ever come across a situation where you might need to search for those specific words. Craig Ball has an excellent example that in most ediscovery document review platforms, you won't be able to find the phrase "to be or not to be" even if you put it in quotations, because those are noise words that would not be indexed in the data processing phase.

At this step, **you should consider proactively giving your provider (like Nextpoint) a list of keywords or search terms that you're interested in** so you can receive a "hit report" after processing. This report can be helpful to show you how many occurrences of certain words are found in the data and allows you to filter chosen keywords before diving directly into a manual review.

Step 4: Data Mining and Analytics (Examine What The Data is Telling You)

Lastly, an ediscovery processing workflow should enable you to take advantage of deep-dive analysis of your data. Computational tools, like Nextpoint's Data Mining, can be used to highlight interesting or significant patterns in your data to provide you with better angles to approach review. There are several advanced tools utilizing artificial intelligence (AI), machine learning (ML), natural language processing (NLP), and a host of other mind-blowing technologies. Just ask your vendor what basic analytical tools they have that can help you.

For example, immediately after data processing, Nextpoint provides you with a set of statistics on how many files and documents you're faced with, how many email messages, how many attachments, and how many email threads or conversations in total. You can also view a visual, interactive timeline of files and email messages so you can focus on a specific date range. There are data widgets that break down the different file types found in your data, as well as the authors and email domains.

In addition to these features, Nextpoint offers Data Mining, the new groundbreaking technology for Early Case Assessment and comprehensive data analysis. The app generates snapshots of key themes in your data and offers advanced search features that can be used to create custom visual reports. As volumes of electronic data explode in the legal field, advanced tools like this are becoming key parts of handling potential evidence in litigation.

All of these tools provide you with a much better place to start your review rather than just blindly diving into a collection of files and clicking the first one, then the next, then the next. These analytics are available in the processing stage, and it would be incredibly beneficial for

you to inquire with your platform provider about what tools they can provide for analyzing your data.

An Ediscovery Processing Workflow To Simplify Your Data Load

As you can see, the "processing" stage of ediscovery has a lot more happening under the hood, and while some of these tasks are standard and run-of-the-mill, it's also important that you become comfortable with all the options and processes so you can make the best decisions for your clients and their data. With these strategies, there's no need to be overwhelmed by discovery data – you can simplify and understand it before diving into document review.

Data Mining: The Processing Tool of the Future

Data Mining is Nextpoint's new technology for ediscovery processing and Early Case Assessment. It can process massive amounts of data at speeds 30 times faster than current technologies. Click here to learn how Data Mining can simplify your ediscovery data.

★ LEARN MORE ABOUT DATA MINING

About the Author

Brett Burney is an E-Discovery Consultant who focuses the bulk of his time on bridging the chasm between the legal and technology frontiers of electronic discovery. Brett is also very active in the Mac-using community, working with lawyers who want to integrate Macs, iPhones and iPads into their practice.

Capitol Rioter's Motion to Suppress Facebook Evidence Denied

By Pierre Grosdidier

Matthew Bledsoe allegedly partook in the bellicose mob that stormed the United States Capitol on January 6, 2021, and temporarily brought mayhem to the normally peaceful electoral college presidential election certification.[1] Like many of his acolytes, Bledsoe apparently livestreamed his participation in the rampage on his private Facebook account. The FBI tracked him (and others) down by first submitting an emergency disclosure request to Facebook for non-content identification information concerning active accounts in the Capitol during the riot, and then submitting a warrant for account content.[2] The trial court denied his motion to suppress 32 incriminating exhibits; thus obtained and sentenced him to 48 months of confinement following his conviction.[3]

As early as that anarchic day, the FBI asked Facebook to identify any users who had livestreamed videos from within the Capitol during the riot. The FBI based its request on § 2702(c)(4) of the Stored Communications Act, which authorizes providers of electronic communications services to provide non-content account information "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency."[4] In response, Facebook provided Object IDs for qualifying videos and User IDs for corresponding Facebook and Instagram accounts. The FBI then used these disclosures to secure broad warrants for the contents of the social media accounts, including user information. Bledsoe owned one of the Facebook accounts and was consequently charged on a slew of federal counts.[5]

Bledsoe argued, *inter alia*, that the FBI's first request for non-content information was a Fourth Amendment search under *Carpenter v. United States* that required a warrant.[6] In *Carpenter*, the

---

1 *United States v. Bledsoe*, No. 21-204 (BAH), --- F. Supp. 3d ---, 2022 WL 3594628, at *1 (D.D.C. Aug. 22, 2022) (mom. op.).

2 *Id.* at **2-3.

3 *Id.* at *2; *see also* ECF No. 237 on pacer.gov (sentencing). Beldsoe filed an appeal.

4 *Bledsoe*, 2022 WL 3594628, at *3 (citing erroneously to 18 U.S.C. 2704(c)(4)).

5 *Id.* at **3-4.

6 *Id.* at *2 (the court also rejected Bledsoe's other argument that the warrant lacked probable cause).

United States Supreme Court held that authorities needed a warrant supported by probable cause to obtain a suspect's cell-site location information (CSLI). The Court reasoned that a person enjoyed a reasonable subjective expectation of privacy in the whole of his or her movements as captured with detailed resolution by CSLI.[7] The government responded in this case that the non-content information it obtained from Facebook fell "squarely within the third-party doctrine," which holds that a person has no reasonable expectation of privacy in information voluntarily surrendered to third parties.[8]

In *Carpenter*, the U.S. Supreme Court declined to extend the third-party doctrine to CSLI. It held that CSLI records stood apart because of their invasiveness into a person's privacy, in contrast to other types of information that had historically justified the doctrine, *e.g.*, checks and telephone call logs. The Court also reasoned that a person did not *voluntarily* convey CSLI records to anyone because cell phones were nowadays indispensable, and their transmissions unavoidable by design.[9]

The trial court held that Bledsoe had failed to extend *Carpenter*'s logic to his situation and had failed to meet his burden of establishing a Fourth Amendment violation. The trial court contrasted unavoidable CSLI records with Facebook transmissions that are initiated by the user when he or she downloads the application, creates an account, and shares pictures, videos, and messages. Moreover, unlike cell phones, social media accounts are not indispensable to contemporary life. The trial court held that Bledsoe could not assert a reasonable expectation of privacy in non-content account information after he had voluntarily livestreamed videos of a "highly public event" using Facebook's services. Bledsoe had also failed to show that the third-party doctrine did not apply.[10]

The court also distinguished this case from *Carpenter* in that the non-content information Facebook disclosed did not reveal the intricacies of Bledsoe's personal life, as CSLI records are wont to do. Instead, the records merely concerned user identification numbers in a 4.5-hour time window while a criminal rampage involving hundreds if not thousands took place in the United States Congress building. Nothing about these circumstances remotely suggested that

---

7 *Id*. at *6 (citing *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018)).

8 *Id*. at *5.

9 *Id*. at **6-7.

10 *Id*. at *9.

Bledsoe could have had a subjective expectation of privacy, let alone one that society would recognize as reasonable.[11]

Finally, the trial court noted that Bledsoe had assumed the risk that Facebook would share his non-content account information with authorities in instances of illegality as Facebook reserved the right to do so in its Data Policy. For all these reasons, the trial court denied Bledsoe's motion to suppress evidence on the basis that the FBI's request for non-content information required a search warrant.[12]

About the Author

Pierre Grosdidier 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 Chair for 2022-23.

[11] *Id.*

[12] *Id.* at *10.

Becoming Well Versed in the Metaverse

By Katrinnah Darden

I. Introduction

In regard to the metaverse, "[t]he legal conundrums are about as diverse as the possibilities of the metaverse itself."[1] Most people do not understand this innovation despite unquestionably having seen mention of it across the internet. Others have opinions on its morality, practicality, or legality and some question whether it will ever actually exist.[2] Whether this innovation is frightening, or exciting, certain aspects of our lives will undoubtedly have to change in order to accommodate it. Due to its novelty and recency, there is very little scholarship on the legal ramifications of the metaverse; and that which has been written tends to focus on the questions it raises concerning one practice area alone.[3] In contrast, this paper will examine issues the metaverse raises across several areas, providing an overview of the potential impact of the metaverse on the law as a whole.

The Metaverse, Explained

Facebook Connect is an annual conference during which Meta, Inc. announces its advancements in virtual and augmented reality technology.[4] During the 2021 keynote, CEO Mark Zuckerberg announced that Facebook would be investing billions of dollars into creating the metaverse.[5] To conclude, Zuckerberg explained, "[t]oday we are seen as a social media company. But in our DNA, we are a company that builds technology to connect people. And the metaverse is the next frontier, just like social media was when we got started."[6] Later,

---

1 Kate Beioley, *Metaverse vs Employment Law: the Reality of the Virtual Workplace*, FINANCIAL TIMES, February 20, 2022, at 1, https://tinyurl.com/3dk3hrn6 (quoting Jonathan Newman).

2 Joel Stein, *The Metaverse Will Never Happen*, Jan. 11, 2022, https://tinyurl.com/mfvxuyzm.

3 *E.g.*, Beioley, *supra* note 1; Victoria Hudgins, *E-Discovery's New Wild West: The Metaverse*, LEGALTECH NEWS, March 02, 2022, https://tinyurl.com/2p98e7yu; Alexis Montano, *Real Estate Law May Soon Play A Role In The Metaverse*, SQUIRE PATTON BOGGS, March 2, 2022, https://tinyurl.com/yckkyub7.

4 Facebook Technologies, LLC, *Facebook Connect*, OCULUS (last visited May 13, 2022), https://tinyurl.com/2c9fyn2b.

5 Meta, *The Metaverse and How We'll Build It Together*, YOUTUBE (Oct. 28, 2021), https://www.youtube.com/watch?v=Uvufun6xer8.

6 *Id.*

seemingly to prove their commitment, he announced that "Facebook" would change its name to "Meta."[7]

The metaverse was pitched as the next step in the natural evolution of technology.[8] Importantly, "the metaverse" does not describe one place (not even one virtual, intangible place, at that). To its creators, the term "Metaverse" describes a combination of augmented reality and virtual reality that will (one day) work with existing technology to further the ultimate goal of all technology, according to Zuckerberg: "the feeling of presence."[9] A feeling of presence will be the "defining feature" of the metaverse.[10]

Zuckerberg also said, "openness, safety and privacy . . . have to be fundamental building blocks."[11] Coming from the founder of Facebook, many rightfully question this statement. This company's ability to achieve transparency has yet to be proven.[12] Transparency on data collection and use, easy to use safety controls, and parental controls were mentioned as example features to promote safety and privacy.[13] One specific example was the "blocking" feature, to be used by one user against another who makes them feel unsafe.[14]

Of course, the metaverse does not actually exist yet. While certain aspects are in various phases of beta testing, Meta, Inc. projects all the requisite technology (augmented reality glasses, peer-designed "home spaces," wrist-based neural interfaces, etc.) to be available for wide use in five to ten years.[15] Horizon Home, available today, is the early vision for "home spaces," which will be the starting point of a typical experience in the metaverse.[16] In the future, anyone will be able to design, sell, and buy these virtual rooms.[17]

---

7 *Id.*
8 *Id.*
9 *Id.*
10 *Id.*
11 *Id.*
12 *See Facebook Data Privacy Scandal: A Cheat Sheet*, TECHREPUBLIC, July 30, 2020, https://tinyurl.com/3tv86rbe.
13 Meta, *supra* note 5.
14 *Id.*
15 *Id.*
16 *Id.*
17 *Id.*

Horizon Worlds, opened to the public in 2021 after two years of beta testing, is already occupied by fast food chains, law firms, and churches.[18] Most socializing will happen in Horizon Worlds. Like "home spaces," anyone will be able to create (and sell) a "world."[19] To encourage this commerce, Meta is developing, in tandem with the metaverse, programs to simplify the coding required to design a virtual reality space.[20] Horizon Marketplace will be where users, or "creators," sell 3D digital items, such as non-fungible tokens (NFTs) to "overall grow the metaverse economy."[21] Finally, Horizon Workrooms is currently available to anyone who wants to take Zoom meetings to the next level.[22]

Of course, "the metaverse could gain little traction and never play a significant role in corporate matters," said one expert on its potential to impact e-discovery, "[b]ut lawyers shouldn't ignore the emerging technology."[23] This is true of every area discussed in this paper.

But, virtual worlds (like Second Life) have already impacted the law. So, the emergence of a much more widely-known platform from a technology giant like Meta warrants inquiry into its potential to change the practice of law.

II. Threshold Issues

It has been observed that, "[g]enerally, developers of virtual worlds do not want real-world laws being applied to their platforms . . .. [u]sers likely feel the same way."[24] Arguably, the main appeal of a "social virtual world"[25] is that real-world laws do not govern therein. Neither

---

18 *E.g.*, Stephen Moore, *The 'Wendyverse' Is a Virtually Tasteless Restaurant*, LEGALTECH NEWS, April 4, 2022, https://tinyurl.com/yef3tb5h; Isha Marathe, *4 Reasons Law Firms Are Entering the Metaverse*, LEGALTECH NEWS, March 28, 2022, https://tinyurl.com/yt2c7h8z; Life.Church, *We Brought Church to the Metaverse*, https://www.life.church/metaverse/; VR Church, *VR Church in the Metaverse*, https://www.vrchurch.org/.

19 Meta, *supra* note 5.

20 *Id.*

21 *Id.*

22 Skarredghost, *Horizon Workrooms Review: Nice, But Not Compelling for Work Yet*, August 21, 2021, https://tinyurl.com/yx6wt4xu.

23 Hudgins, *supra* note 3, (quoting Bryant Isbell).

24 Steven Chung, *The Problems With Trying To Apply Real World Laws In The Virtual Metaverse*, ABOVE THE LAW, February 23, 2022, https://tinyurl.com/mr49hu6a.

25 *See* Katherine B. Forrest, *Need Justice Be Real When Reality Is Not?*, N.Y. L. J., March 28, 2022, https://tinyurl.com/yrc437zy.

the laws of physics, as seen in the metaverse's announcement video that advertised floating around with friends in virtual "space,"[26] nor the law that lawyers practice.

However, the virtual realm Second Life has most certainly been subjected to real-world law.[27] In one case, the court stated that "[w]hile the property and the world where it [was] found [were] virtual, the dispute [was] real."[28] For legal specialists, the initial question is whether real-world law even applies in the metaverse. Then, as one article put it, "[w]ith users in different jurisdictions interacting on one platform, which laws apply?"[29]

As to the first question, "[s]hould virtual offenses lead to legal complaints?", one labor and employment litigator "said he would expect the same laws that apply in the real world would apply to virtual violations."[30] Additionally, an article from the New York Law Journal titled, *Need Justice Be Real When Reality is Not?,* discussed whether the metaverse would have crime and punishment.[31] The answer was "TBD."[32] As previously mentioned, this is a common thread in writings on the metaverse. The following section attempts to resolve the threshold issues in a new way.

A. Second Life

Because the metaverse is not yet upon us, the best way to answer these preliminary questions is to explore how real-world law has been applied to similar virtual environments. Second Life, created by Linden Lab, is probably the most similar platform to the metaverse to date.[33] So similar, in fact, that shortly after Meta's announcement, the founder of Second Life rejoined the project as a strategic advisor, increased its workforce, and invested in several patents relating to their virtual world.

---

26 Meta, *supra* note 5.

27 *See e.g.*, Bragg v. Linden Research Inc., 487 F. Supp. 2d 593 (E.D. Pa., 2007).

28 *Id.* at 595 (internal quotation marks omitted).

29 Cedra Mayfield, *Buckle Up: Lawsuits Over Offenses in Virtual Reality Could Become the Next Litigation Trend*, DAILY REPORT, March 09, 2022, https://tinyurl.com/npw99eyj.

30 *Id.*

31 Forrest, *supra* note 25, at 1.

32 *Id.* at 3.

33 *See* Richard Lawler, *Second life Joins the Metaverse Discussion With the Return of its Founder – and Some Key Patents*, THE VERGE, Jan. 13, 2022, https://tinyurl.com/4ama5m5c; Max Vern, *Second Life – A New Dimension for Trademark Infringement*, J. PAT. & TRADEMARK OFF. SOC'Y, March 1, 2008, https://tinyurl.com/3afwwr2y.

Two key features of Second Life differentiate it from other multiplayer interactive online games and make it more like the up and coming metaverse:

First, the users do not just play the game but actively build the game and its content and create their own rules of interaction, modeled on the [real-life] society. In particular, and very notably, the users have the right to own the property they create, including Intellectual Property (§3.2 of Terms of Service).

Second, the users not only pay fees for "living" in the [Second Life], but they also build a real market economy by creating, buying or selling virtual tangible (seemingly, an oxymoron) and intangible property.[34]

Although it is an older creation, as of February 2022, Second Life still had one million active users.[35] Notably, Second Life has always had an arbitration agreement embedded in their Terms of Service.[36] This added layer of complexity in applying the law to Second Life will likely occur with the metaverse because Meta, Inc. also employs an arbitration clause against its consumers.[37]

Another issue with Second Life precedent is that the abundant litigation against Linden Lab did not involve any conduct in the virtual world. For example, Linden Lab was sued for "retaliat[ing] against [a former information security director] for flagging cybersecurity risks and potential violations of anti-money-laundering laws, child exploitation, and data misuse."[38] While these cases may not be helpful in answering our threshold questions or understanding the law as applied in virtual worlds, they do illustrate some challenges Meta, Inc. may face, such as keeping their trade practices fair.

---

34 Vern, *supra* note 33, at 2.

35 Samuel Gush, *4 Reasons People Still Play Second Life*, MAKEUSEOF, Dec. 02, 2021, https://tinyurl.com/y64xrzzm.

36 Second Life Terms and Conditions, (effective July 31, 2017) https://secondlife.com/app/tos/tos.php.

37 Meta Commercial Terms, (effective January 4, 2022) https://www.facebook.com/legal/commercial_terms.

38 Paris Martineau, *Second Life is Plagued by Security Flaws, Ex-Employee Says*, WIRED, Aug. 16, 2019, https://tinyurl.com/4dszd33v.

Jurisdiction

One of the first and most significant cases involving Second Life "provide[d] an indicator of how courts may deal with the complex issue of jurisdiction and disputes over virtual activities."[39] This case was *Bragg v. Linden Research, Inc.*, in which the plaintiff, a lawyer, alleged that Linden (and the other named Defendant, Linden CEO Phillip Rosendale) had unlawfully denied him access to the platform and his virtual belongings.[40] He sought $8,000 in restitution.[41] The overarching issue was "what rights and obligations grow out of the relationship between the owner and creator of a virtual world and its resident-customers."[42] The plaintiff had "purchased numerous parcels of land, created and sold virtual fireworks, and acquired other virtual items."[43] All of this was confiscated by Linden when they froze his account on suspicion of one of his purchases (a $300 parcel of virtual land) being completed through "'exploit,' a software trick used to buy virtual property on the cheap."[44]

The U.S. District Court of the Eastern District of Pennsylvania held that it had specific personal jurisdiction over the CEO as a result of his personal involvement in the national advertisement of virtual land in Second Life (through a real-life press release and TV interview, and a virtual town meeting that the plaintiff attended).[45] He had also stated that "you can really make money" and that the idea of owning virtual land "is intoxicating."[46] According to the court, he had "personally hype[d] the ownership of virtual property on Second Life."[47] And the plaintiff claimed that he and the 50,000 other class members were induced by this publicity to purchase the "land" later confiscated, the price totaling $100 million.[48]

Therefore, the court held "that Rosedale's representations—which were made as part of a national campaign to induce persons, including Bragg, to visit Second Life and purchase virtual property—constitute[d] sufficient contacts to exercise specific personal jurisdiction over

---

39 Roxanne E. Christ & Curtis A. Peele, *Virtual Worlds: Personal Jurisdiction and Click-Wrap Licenses*, 20 INTELL. PROP. & TECH. L. J. 1, 1 (Jan. 2008).

40 *Bragg*, 487 F. Supp. 2d at 595.

41 Courtney Rubin, *A Virtual World Spawns a Very Real Lawsuit*, INC., May 3, 2010, https://tinyurl.com/3a87jtrf.

42 *Bragg*, 487 F. Supp. 2d at 595.

43 Christ & Peele, *supra* note 39, at 1.

44 *Id.*

45 *Bragg*, 487 F. Supp. 2d at 596, 601-02.

46 *Id.* at 596.

47 *Id.*

48 *Id.*; Rubin, *supra* note 41.

Rosedale."[49] It also cited a rule from *Toys "R" Us, Inc. v. Step Two, S.A.*: if a defendant website operator knowingly conducts business with forum state residents via the site, then the "purposeful availment" requirement is satisfied."[50]

This case illustrates how an issue of personal jurisdiction might be handled in a future dispute arising out of the metaverse. When Meta, Inc. sells people augmented reality glass shipped directly to their home, or other physical products purchased inside the metaverse, the purposeful availment requirement would likely be satisfied as to Meta, Inc. in that state. Additionally, Mark Zuckerberg's statements about the wonders of the metaverse (in, for one example, his keynote at Facebook Connect 2021) could easily satisfy the personal jurisdiction requirement of a federal court if a plaintiff could show that their circumstances were induced by these statements.

For example, Zuckerberg stated that he was "genuinely optimistic about work in the metaverse," which was an area that he discussed at length.[51] If a dispute arose regarding a Horizon Workroom, this "personal hyping" could help establish personal jurisdiction over Zuckerberg. More likely, a user will have bought a "home space" specially designed and have certain digital goods (clothing for their avatar, etc.) and, similarly to Bragg in the Second Life case, they will sue for this property. In that case, Zuckerberg's announcement video was clearly intended to induce users to buy and sell these types of goods from each other.

For these reasons, personal jurisdiction will likely not be a barrier to the liability of Meta, Inc. for disputes regarding the metaverse. Considering how significant its contacts will be in every U.S. state at the stage when a suit is likely to arise (*i.e.*, after they have sold augmented reality glasses and oculus headsets and shipped them to the plaintiffs' homes).

This precedent effectively answers our first question: whether residents of the metaverse will have legal recourse for virtual versions of real-life wrongs?[52] At least, it tells us that they probably will against Meta, Inc. However, whether a user may sue another for conduct that took place in the metaverse and what law would apply in that case remains uncertain. So, in each potential type of user versus user litigation, the validity of each claim and choice of law will be examined below.

---

49 *Bragg*, 487 F. Supp. 2d at 598.

50 *Id.* at 599 (citing Toys "R" Us, Inc. v. Step Two, S.A., 318 F.3d 446 (2003)).

51 Meta, *supra* note 5.

52 Mayfield, *supra* note 29.

III. Legal Disputes Between Users

A. Crime

Before Horizon Worlds was released in December 2021 to anyone eighteen years or older in the U.S. and Canada, it was called Horizon Venues, and underwent two years of invite-only beta testing.[53] One beta-tester, Nina Jane Patel, was the vice-president of metaverse research for an IT consulting company dedicated to "creat[ing] [a] safer metaverse to explore."[54] Only a few seconds after appearing on the platform, she was "virtually gang raped," as she described it.[55]

Three or four male-looking avatars with male voices "attacked" her avatar and made obscene statements.[56] Her attackers also photographed her avatar during this incident.[57] She explained, "[i]t was surreal," "[i]t was a nightmare," and she "froze."[58]

In response to this incident, Meta created the Personal Boundary feature to be implemented in all future versions of the metaverse.[59] According to the President of Horizon Worlds, "Personal Boundary creates more personal space for people, and makes it easier to avoid unwanted interactions."[60] Essentially, this feature keeps all other users (a virtual approximation of) four feet away from anyone who has it enabled.[61] Notwithstanding this effort to prevent virtual "crime," one key question remains: are users exclusively reliant upon Meta, Inc. for security in the metaverse?

According to one author, crime in virtual reality can be categorized in three ways: violations of a platform's Community Guidelines, End User License Agreements (EULA), etc.; crimes carried over from the real world (like harassment and unwanted touching); and crimes defined by users' own governments. First, violations of Meta's EULA will likely be the simplest to prosecute, but the real-world justice system would not do the prosecuting and the powers that be at Meta, Inc. would not have much accountability. Virtual crimes often do not meet the legal

---

53 *Id.*

54 Kubani, LinkedIn Profile.

55 Mayfield, *supra* note 29 (quoting Nina Jane Patel, *Reality or Fiction?*, Dec. 21, 2021, https://tinyurl.com/2jyxjwej).

56 Patel, *supra* note 55.

57 Mayfield, *supra* note 29 (quoting Patel, *supra* note 55).

58 Patel, *supra* note 55.

59 Mayfield, *supra* note 29.

60 Vivek Sharma, *Introducing a Personal Boundary for Horizon Worlds and Venues*, OCULUS BLOG, February 4, 2022, https://tinyurl.com/3t49cjfc.

61 *Id.*

elements to be prosecuted in the real world (like the virtual sexual assault perpetrated against Nina Jane Patel). For example, unwanted touching in the metaverse cannot be punished under common law battery, even though one's avatar, and one's psyche as a result, may truly be violated. Therefore, Meta will provide the only protection from these crimes.

Additionally, if Meta only punishes violations under their EULA, the metaverse would become a very unsafe place. This would make one tech company wholly responsible for writing, enforcing, and upkeeping an entire legal system for an effectively infinite virtual world.

The second category of virtual crime, those carried over from the real world, can be seen in Meta's various conduct policies. For example, prohibited conduct under Meta's VR policy includes harassment, stalking, intimidation, sexual "touching," and impersonating a Facebook employee or any other real person.[62] Similar conduct is prohibited in more detail and more broadly under the Community Standards, likely because those also govern users of Facebook.[63] If Meta finds that a user has violated any of the above-mentioned policies, it "may take action on your account, including temporarily restricting or suspending your account. For repeated or egregious offenses, we may permanently disable your account."[64]

It is important that these real-world crimes are carried over into the virtual realm because, as was made clear by Nina Jane Patel's testimony, anxiety and trauma linger after one's avatar is victimized, even if one's physical body is unharmed. Therefore, virtual crimes against persons (or avatars) deserve punishment just as much as real-world crimes.

The third category of virtual crime, those defined by users' own governments, is not relevant to the metaverse (yet). But, there are plenty of examples from Second Life, where users "actively build the game and its content and create their own rules of interaction, modeled on [real-life] society."[65] Furthermore:

> [In Second Life] all avatars subject themselves to Terms of Service, [but] Linden Lab specifically disclaims regulation of content and interaction between avatars (§1.2 Terms of Service), nor does it function or wish to function as an arbiter in case of conflicts

---

62 Meta Quest, *Conduct in VR Policy*, https://tinyurl.com/yc7s2vc2.

63 Meta Transparency Center, *Facebook Community Standards*, https://tinyurl.com/2nf8u8e9.

64 Meta Quest, *supra* note 62.

65 Vern, *supra* note 33.

beyond the cases clearly defined as "harmful practices," *e.g.*, dissemination of obscene or hateful data, spamming, etc.[66]

This is where the virtual worlds differ. Meta attempts to create structure in the metaverse by outlawing and committing to punish virtual crimes committed therein. In contrast, Second Life promotes a primitive, tribal society, in which users are responsible for writing and adhering to their own social contracts. From a consumer's standpoint, it is preferable that Meta has not disclaimed responsibility for user misconduct in the metaverse.

The success of a criminal charge for conduct taking place in the metaverse depends on the crime committed. For a crime like stalking, the real-world legal elements (a course of conduct or behavior, the presence of threats, and the criminal intent to cause fear in the victim[67]) could be satisfied by conduct in the metaverse. In this case, a standard criminal prosecution in the jurisdiction of the user's real-word residence would likely take place. In contrast, crimes like unwanted touching and criminal harassment will be solely the responsibility of Meta to deter, prevent, and punish, since it could never satisfy the traditional legal elements. In this way, crime in the metaverse reflects the common occurrence of the law being behind the times.

B. Torts

Conduct in the metaverse could satisfy the elements currently existing at law for certain torts (like defamation, libel, or conspiracy). Therefore, the prosecution of those torts would likely not be very different if they were committed in the metaverse. In contrast, trespass, assault, battery, and intentional infliction of emotional distress, for example, would be much more interesting than usual if they were committed in the metaverse. First of all, trespass in the metaverse would require proof of ownership of the "land" trespassed upon, which raises significant questions to be discussed below. Assault and battery in the metaverse, as previously mentioned with regard to Nina Jane Patel's story, cannot satisfy the criminal or tortious elements because there would never be any physical "touching." Therefore, intentional infliction of emotional distress will likely be common for conduct in the metaverse as a substitute for assault, battery, and the like.

---

66 *Id.*

67 *Domestic Violence, Stalking, and Antistalking Legislation: An Annual Report to Congress under the Violence Against Women Act*, NATIONAL INSTITUTE OF JUSTICE, April 1996, at 5, https://www.ojp.gov/pdffiles/stlkbook.pdf.

Notably, there would likely not be a choice of law issue at play in a tort case by an individual plaintiff against an individual defendant, even for conduct in the metaverse, since the suit could simply be brought wherever the defendant lives.[68]

C. Working in the Metaverse

The choice of law issue will be especially important in the area of employment law. A "decentralized digital workspace in which workers may be itinerant and geographically disconnected from each other and the company they work for,"[69] like the metaverse, will raise jurisdictional questions, no doubt. The key question being: "Where is the jurisdiction with the greater connection to the work?"[70] Gary Howard, a partner at Fox Rothschild in Atlanta and labor and employment litigator, believes that "legal offenses occurring in immersive mixed-reality realms [of the workplace] aren't off limits," but that the main issue would be jurisdictional.[71] He analogized future meetings in the metaverse to the current practice of meeting on Zoom.[72] As much as Mark Zuckerberg appears to try to revolutionize living, working, and playing by creating the metaverse,[73] according to Howard, there is not "any difference from a legal perspective" from working remotely today and working in the metaverse tomorrow.[74]

D. Property

The most important point to make relevant to property issues in the metaverse is that the metaverse will consist of "persistent state worlds," meaning that any changes a user makes to a home space, work room, or the like, will remain, regardless of how many times the user leaves and returns to it.[75] Additionally, Mark Zuckerberg has discussed the progress Meta is making towards "interoperability" for user's digital possessions.[76] Interoperability will allow a user to adorn their avatar with a virtual t-shirt, for example, in their home space and wear it to their work room and into their favorite Horizon World.[77]

---

68 Chung, *supra* note 24.
69 Beioley, *supra* note 1.
70 *Id.*
71 Mayfield, *supra* note 29.
72 *Id.*
73 *See* Meta, *supra* note 5.
74 Mayfield, *supra* note 29.
75 Meta, *supra* note 5.
76 *Id.*
77 *Id.*

The "Commerce" section of Mark Zuckerberg's announcement video explains that work going on today with NFTs and crypto-currencies will be required for users to "know that [they] own their items."[78] NFTs are "cryptographic tool[s] using a suitable blockchain to create a unique, non-fungible digital asset."[79] NFTs are also intellectual property.[80] Therefore, though most possessions in the metaverse will represent items of personal property that exist in the real world, the clothing for one's avatar, furniture for their home space, etc., will actually be NFTs governed by intellectual property law.

i. Intellectual Property

"Generally, virtual-world platforms . . . give users limited-use licenses to use in-world items,"[81] except in one case: "users [of Second Life] have the right to own the property they create, including Intellectual Property (§3.2 of Terms of Service)." The significance of this choice was discussed in a 2003 press release, *Linden Lab Preserves Real World Intellectual Property Rights of Users of its Second Life Online Services*:

> We believe our new policy recognizes the fact that persistent world users are making significant contributions to building these worlds and should be able to both own the content they create and share in the value that is created. The preservation of users' property rights is a necessary step toward the emergence of genuinely real online worlds.[82]

Similarly, Meta's goal is "to provide a way for as many creators as possible to build a business in the Metaverse."[83] In this early stage of development, Meta is "exploring new types of ownership models and entitlements, to ensure people feel confident they actually own something."[84] It is not yet certain whether Meta will go as far as Second Life or, more likely, just grant intellectual property rights to users that design and sell digital goods in the metaverse to thwart copy cats. For example, Mark Zuckerberg has emphasized, "preventing others from using your avatar will be critical. That's why . . . we're already thinking about how we could

---

78 *Id.*

79 Marcus Hoh & Melvin Pang, *Non-Fungible Tokens (NFT) and Intellectual Property Law*, AMICA LAW LLC, 12 January 2022, https://www.amicalaw.com/non-fungibletokens.

80 *Id.*

81 Chung, *supra* note 24.

82 Press Releases, *Linden Lab Preserves Real World Intellectual Property Rights of Users of its Second Life Online Services*, LINDEN LAB (Jan. 14, 2003), https://tinyurl.com/mr3ym8fz.

83 Meta, *supra* note 5.

84 *Id.*

secure your avatar, whether by tying it to an authenticated account or by verifying identity in some other way."[85]

Zuckerberg believes that "[t]he Metaverse is well-positioned to be a strong digital economy for creators from all walks of life."[86] In Second Life, "[a]ssets on the platform are bought and sold using the platform's native digital currency dubbed Linden Dollars. Linden Dollars are convertible into real-world currency via the platform's Tilia gateway. Tilia is a licensed money transfer solution that supports virtual gaming communities as well as NFT ecosystems."[87] All of this should be quite inspiring to Meta, Inc. But, so far, it has only been stated that a more secure version of existing crypto will be the main form of currency in the metaverse.[88]

ii. Real Estate

In Second Life, "avatars may purchase virtual land, make improvements to that land, exclude other avatars from entering onto the land, rent the land, or sell the land to other avatars for a profit."[89] Meanwhile, in the metaverse, *Wendy's* has branded an entire town square.[90] There is a virtual soda stream and basketball court where users can "shoot hoops with a virtual 'Baconator.'"[91] Disturbingly, this is the "first phase" of *Wendy's* "metaverse strategy."[92]

McDonald's, seemingly also executing a metaverse marketing strategy, "has applied for 10 Metaverse-related patents, including exploring the possibility of delivering food online and in-person and selling more NFTs."[93] *Chipotle* also advertises in the metaverse.[94] But, this omnipresence of large fast-food chains is to be expected. More interesting is the concept of international businesses and individual metaverse users alike, owning "real estate" in the metaverse.

Bragg v. Linden Research was a case against Second Life for confiscating a user's virtual land.[95] Unfortunately, after the district court's remand, the case was confidentially settled before a

---

85 *Id.*
86 *Id.*
87 Gush, *supra* note 35.
88 Meta, *supra* note 5.
89 *Bragg*, 487 F. Supp. 2d at 595-96 (internal citations omitted).
90 *See* Moore, *supra* note 18.
91 *Id.*
92 *Id.*
93 *Id.*
94 *Id.*
95 *Bragg*, 487 F. Supp. 2d at 593.

final decision was reached.[96] "The parties agree[d] that there were unfortunate disagreements and miscommunications regarding the conduct and behavior by both sides and are pleased to report that Mr. Bragg's 'Marc Woebegone' account, privileges and responsibilities to the Second Life community have been restored."[97]

However, in 2010, a very similar 57,000 member class action arose against Linden Research for taking away the plaintiffs' ownership rights to virtual "land" without reasonable compensation.[98]

> "What you have in Second Life is real and it's yours," the suit quote[d] Rosedale as saying. "It doesn't belong to us. We have no claim to it." (The complaint is peppered with Rosedale quotes, painting the founder and former CEO as the driving force behind the property rights concept)."[99]

Second Life had even charged monthly fees to these users and likened it to property taxes.[100] The plaintiffs alleged that the Terms of Service, at some point, had been changed to omit the ownership concept, and that they were not notified or compensated for their loss of property rights.[101] "For example, a question on the FAQ page that read 'Why would I want to own land?' morphed into 'Why would I want to have land?'"[102] The case ultimately settled for 43 million Linden Dollars, or, $172,000 USD.[103]

The metaverse implicates a quintessential principle of property law and raises this question: whether "land" in the metaverse is unique for purposes of real property law. It may have been designed by a user, or Meta, only once, but it may be repeatable. It seems that the same virtual trees, hills, or buildings could be designed identically a second time, especially if the creator used one of Meta's coding simplifiers. This would mean that in a dispute over property in the metaverse, the plaintiff could not be awarded specific performance. Marc Bragg might have

---

96 Benjamin Duranske, *Bragg v. Linden Lab – Confidential Settlement Reached; 'Marc Woebegone' Back in Second Life*, VIRTUALLY BLIND, October 4, 2007, https://tinyurl.com/3e3f5wnk (quoting Linden Lab, Official Second Life Blog, Resolution of Lawsuit).

97 *Id.*

98 Rubin, *supra* note 41.

99 *Id.*

100 *Id.*

101 *Id.*

102 *Id.*

103 Peter Vogel, *Second Life Avatars Class Action Settles*, INTERNET, IT, AND E-DISCOVERY BLOG, 14 June 2013, https://tinyurl.com/5tnwaa24.

considered this when he sought monetary restitution damages, rather than access to his virtual land, in his suit against Second Life.

To the contrary, one author discussed this from a technical point of view:

> [In virtual worlds,] [a]lthough we broadly categorize these transactions as real estate, the assets being traded are NFTs. NFTs are one-of-a-kind digital assets that are indivisible and not interchangeable. This correlates to owning a piece of real property where no two are the same. NFTs are managed by digital ledgers called blockchains much like ownership of real estate is documented in county public records. While deeds contain the legal description of the property you own, NFTs contain metadata that describe the asset they represent.[104]

It is not yet clear whether a court will consider virtual real estate real property or intellectual property. Again, unfortunately, the court in *Bragg* never reached the merits of the property dispute due to an out-of-court settlement.

E. Contracting in the Metaverse

Metaverse Marriage

In Second Life, a user can pair their profile with another's and even have a wedding, essentially getting married.[105] This is called the "partnering feature."[106] "Partnering broadcasts the relationship to other users in the community and causes the relationship status to appear on the paired profiles. It costs 10 Linden dollars to partner on Second Life."[107] Thankfully, the users' property is not affected by gaining a partner in Second Life.[108] At the moment, there is no equivalent planned for the metaverse.

IV. Liability of Meta, Inc.

A. Data Privacy

Mark Zuckerberg has stated that privacy and safety "need to be built into the metaverse from day one."[109] To that end, he is allegedly "taking a thoughtful approach to privacy as he

---

[104] Montano, *supra* note 3.
[105] Gush, *supra* note 35.
[106] *Id.*
[107] *Id.*
[108] Gush, *supra* note 35.
[109] Meta, *supra* note 5.

attempts to build the immersive, virtual world for users known as the metaverse."[110] However, users of virtual reality give up the most personal data of any technological platform.[111] For example, according to Meta,

> Neural interfaces are going to be an important part of how we interact with AR glasses. More specifically, EMG input from the muscles on your wrist combined with contextualized AI . . . we all have unused neuro-motor pathways and with simple and perhaps with simple, even imperceptible gestures, sensors will one day be able to translate those neuro motor signals into digital commands that enable you to control your devices."[112]

Beyond "wrist-based neural interfaces," Mark Zuckerberg has claimed that even by thinking about moving one's fingers, with metaverse technology, one could send a text message in the real world one day.[113] Clearly, this could become invasive.

As for transparency and data privacy, Meta is "democratizing" the development of the metaverse.[114] To them, this means allowing individuals and other interested corporations to research the technology it will need and eventually, to release and profit off of it. Additionally, individual "creators" will design the virtual spaces and the virtual belongings that every avatar uses in the metaverse.

V. Lawyering in the Metaverse

Law firms have moved into the metaverse.[115] This raises questions of how lawyering within the metaverse will be different from lawyering in the real world.

A. E-Discovery

Experts have discussed the metaverse's potential to impact in the area of e-discovery.[116] One concerned author explained:

---

[110] Jonathon Vanian, Mark Zuckerberg's Metaverse May Be As Privacy Flawed As Facebook, FORTUNE, October 29, 2021, https://tinyurl.com/znr4586e.

[111] *Id.*

[112] Meta, *supra* note 5.

[113] *Id.*

[114] Meta, *supra* note 5.

[115] Marathe, *supra* note 18.

[116] *See* Hudgins, *supra* note 3.

> As more enterprises, including law firms, are venturing onto the metaverse, these virtual worlds, and the potential evidence they host, are likely to be dragged into litigation . . . [T]he Metaverse is a 'Wild West' that introduces new technical challenges, potential data issues and jurisdiction complications.[117]

Another expert, the managing director of global e-discovery and data advisory at Baker Mackenzie stated that data privacy and cybersecurity must be kept as priorities as the metaverse continues to develop.[118] "Discovery considerations [raised by the creation of the metaverse] include preservation and collection protocols, distinguishing who owns the data and if metaverse developers can provide copies of deleted data," said another author.[119] Unfortunately, it is believed that most organizations are likely to be slow to consider these issues and even slower to change.[120]

The conclusion overall is that "traditional discovery processes may need to be reassessed"[121] and this is self-explanatory. Cases that arise out of the metaverse will require discovery of information collected (and potentially stored) by Meta, Inc. This information may range from what digital clothes an avatar was "wearing," to how many times they "entered" a specific world, or even to what their EMG waves were communicating to their wrist-based neural interface at a specific time. The possibilities are vast and concerning. It is at least safe to say that e-discovery processes will have to adapt in order to operate in the metaverse.

B. Well-Being Despite The Metaverse

The Proteus Effect is "the tendency for people to be affected by their digital representations, such as avatars, dating site profiles and social networking personas."[122] And research has shown that people's behavior shifts in accordance with their digital representatives.[123] Technology has proven to have a great impact on attorney well-being. So, the increased immersion required to participate in the metaverse compared to the internet of today is likely to worsen these impacts.

---

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

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] *The Proteus Effect*, WHATIS.COM, https://tinyurl.com/49s7cjxn.

[123] Nick Yee & Jeremy Bailenson, *The Proteus Effect: The Effect of Transformed Self- Representation on Behavior*, DEPARTMENT OF COMMUNICATION, STANFORD UNIVERSITY, https://tinyurl.com/4xmt5cjm.

VI. Conclusion

There are numerous potential effects that the metaverse could have on the law itself, the procedures of practice, and the people who practice it. One can only hope that, as Mark Zuckerberg claimed,[124] the development of the metaverse will be gradual enough to allow these areas to "catch up," preventing harm to the public and the legal field.

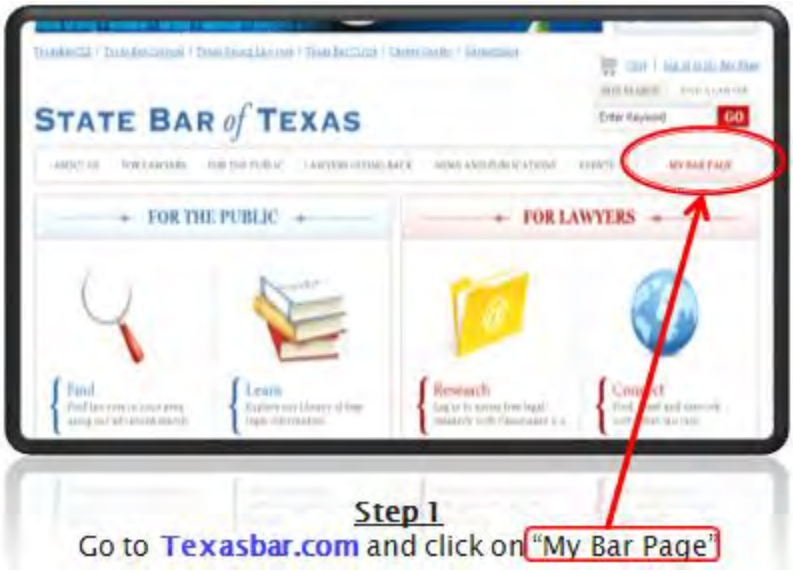
About the Author

Katrinnah Darden is a staff attorney at the Foundation for Moral Law in Montgomery, Alabama. A graduate of Huntingdon College and Faulkner University's Thomas Goode Jones School of Law, Katrinnah became – at age 19 – the youngest lawyer in Alabama history. In law school, she served as Executive Editor of the Faulkner Law Review, and was a Sir Edward Coke Fellow with the Blackstone and Burke Center.

[124] Meta, *supra* note 5.

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:

Pierre Grosdidier – Houston – Chair

Reginald Hirsch – Houston – Chair-Elect

William Smith – Austin – Treasurer

Lavonne Burke Hopkins – Houston – Secretary

Elizabeth Rogers – Austin – Immediate Past Chair

Circuits Editors:

Sanjeev Kumar – Austin

Pierre Grosdidier – Houston (Senior Advisor)

Committee Chairs:

Sally Pretorius – Dallas – Circuits eJournal Co-Chair

Sanjeev Kumar – Austin – Circuits eJournal Co-Chair

Michael Curran – Mc Kinney – CLE Program Coordinator

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 – Justice for All Co-Chair

Alex Shahrestani – Austin – Justice for All Co-Chair

Webmaster:

Ron Chichester – Houston

Appointed Judicial Members:

Judge Xavier Rodriguez – San Antonio

Hon. Roy Ferguson – Alpine

Hon. Emily Miskel – McKinney

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

Term Expiring 2025:

Alan Cooper – Dallas

Mason Fitch – San Francisco

A. Dawson Lightfoot – Mckinney

Sally Pretorius – Dallas

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