Westlaw Today
powered by Reuters

Techno wars and inadvertent productions: an ethics guide to the Alex Jones phone debacle

By Tara Emory, Esq., *Redgrave Data*, Eliza Davis, Esq., and Aviva Surugeon, Esq., *Redgrave LLP*

SEPTEMBER 29, 2022

In a world where enormous amounts of confidential data may be sent inadvertently with a few mouse clicks, do ethical and procedural rules for attorneys adequately protect clients and provide attorney guidance? This article examines how Alex Jones' attorney inadvertently produced an entire forensic copy of his client's phone, the actions by each side's counsel, and how applicable ethical requirements may vary by state.

On August 3, 2022, in the highly publicized Texas trial of *Heslin v. Jones*, plaintiffs' attorney Mark Bankston famously dropped an evidence bombshell on red-faced Alex Jones. After Jones testified he had no text messages or emails about Sandy Hook, Bankston revealed Jones' attorney, F. Andino Reynal:

> messed up and sent me an entire digital copy of your entire cell phone with every text message you've sent for the past two years, and when informed, did not take any steps to identify it as privileged or protected in any way. And as of two days ago, it fell free and clear into my possession. And that is how I know you lied to me when you said you didn't have text messages about Sandy Hook.

Bankston then showed text messages and emails did exist, including financial information about Jones' Infowars website, which was significant for plaintiffs' damages claims. He asked, "You know what perjury is, right? I just want to make sure you know before we go any further."

The Jones phone fiasco raises ethical and procedural issues related to attorney technical competence, inadvertent productions, and privilege waiver.

The inadvertent production bombshell

Sandy Hook Elementary School families filed a defamation lawsuit based on Jones' campaign that the massacre of children was staged. Plaintiffs' counsel dropped its bombshell on the final day of the Texas trial. The next day, Reynal filed an Emergency Motion for Enforcement of Protective Order, arguing plaintiffs should not have used phone evidence, seeking to seal the production as confidential, and requesting a mistrial. Reynal explained:

> [T]he paralegal for Counsel for Defendants emailed Plaintiffs' counsel a link. Defendants' Counsel believed the link contained text messages and other documents that Defendants had previously produced to Plaintiffs in the Lafferty Matter currently pending in Connecticut.[1]

Bankston forwarded that link to his paralegal. While Bankston claimed at a hearing on the motion that the resulting download was complete when he realized the production was inadvertent, his email to Reynal was ambiguous:[2]

> [The paralegal] asked me to take a look because it was a huge amount of material he was downloading, and he wanted me to verify that he needed to download all of it. I looked through the directories and they seem to contain a lot of confidential information, such as depositions and records relating to the Lafferty plaintiffs, and material which appears to be work product or confidential. My assumption is now that you did not intend to send us this? Let me know if I am not correct.

Sandy Hook Elementary School families filed a defamation lawsuit based on Jones' campaign that the massacre of children was staged.

Reynal responded by email:

> [T]here appears to have been a mistake in the file transfer. I'm trying to get you the Lafferty production. Please disregard the link and I will work on resending.

Reynal never sent a new link or production.

On August 4, Judge Gamble heard arguments on the motion. Reynal argued:

> We have a situation here, which is akin to me mistakenly giving him the key to a room and, you know, he opens the door to the room, and instead of finding what he expected to find, he sees other doors ... And he recognized that, and told me, I don't think you meant to give me this key. And I said please throw it away ... And so he took that key and he went back in, and he unlocked and went into each one of those doors.

Bankston countered that Reynal's failures cleared him to use the produced materials under Texas Rule of Civil Procedure 193.3.

The rule provides privilege is not waived, if within ten days of a producing party's discovery of an inadvertent production, it "amends the response, identifying the material or information produced and stating the privilege asserted."

Bankston further argued the materials should not be protected by the confidentiality order because they were not labelled:

> What [a party] must do is specifically identify those documents, provide new copies of those documents with the confidential mark that is required under the Protective Order. To date, Mr. Reynal has still not done that, not at all. And it would be impossible for him to do so, because the vast overwhelming majority of the things contained on Mr. Jones' cell phone are not confidential.

While Reynal argued he had confirmed the materials were confidential by responding to Bankston's email, Bankston responded, "Please disregard creates no legal duty on me whatsoever. None."

Jones' attorney clearly raised ethical issues by inadvertently producing a copy of his client's phone via an unencrypted cloud-based link.

Judge Gamble disregarded the mistrial motion as a "throwaway" argument but provided Reynal an opportunity to identify specific files to seal. Bankston then informed the court that the phone copy had been requested by the Select Committee to Investigate the January 6th Attack on the United States Capitol.

Despite Reynal's request that plaintiffs be prohibited from sharing them without a subpoena, Judge Gamble refused to intervene. "I don't know that you get to stop that anyway... I think [the Committee] is going there [getting a copy] either way."

Shortly thereafter, the jury returned a verdict for plaintiffs for $4.1 million in compensatory damages and $45.2 million in punitive damages.

Ethical duties of the producing party

Jones' attorney clearly raised ethical issues by inadvertently producing a copy of his client's phone via an unencrypted cloud-based link. First, attorneys must provide competent representation to their clients.[3]

Texas Ethics Opinion 680 requires, "a lawyer must take reasonable precautions in the adoption and use of cloud-based technology for client document and data storage..." Similar requirements to protect client information and keep abreast of relevant technology can be found in Model Rule 1.1 comment 8 and Rule 1.6.

Supervising attorneys often enlist the assistance of associate attorneys and non-attorney staff, especially for eDiscovery, as Jones' attorneys did. However, supervising attorneys must ensure junior attorneys and staff follow ethical requirements. Under ABA Model Rule 5.1 and 5.3 and Texas Rules, attorneys are responsible for their own errors as well as the practice and missteps of the junior attorneys and staff they supervise.

There are steps law offices should take to protect confidential information. *First*, they should have controls for site, folder, and document level permissions on their cloud file sharing platform. Information that is confidential, privileged, or otherwise sensitive should be well organized and stored in encrypted folders.

Second, law offices using file transfer platforms should have established procedures for sharing links, including use of passwords and expiration dates, and human quality control checks of transmitted folders and links. Quality checks should determine if files appear to be a standard document production; in the Jones case, someone may have noticed the files may have contained natives and no Bates labels.

Finally, all employees should receive technological training regarding cloud use and eDiscovery processes to protect sensitive information.

Ethical duties of the receiving party

Attorneys who receive inadvertently-produced information are in a sticky position — with potential ethical duties to respect confidentiality or privilege on one hand, and to zealously advocate for their clients, as per ABA Model Rule 1.3, on the other. States maintain different approaches on these issues.

ABA Model Rule 4.4(b) requires the "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."

While Judge Gamble allowed Jones' attorney to identify records to seal after the trial, the case reflects a danger for inadvertently produced client personal information to become unprotected and public.

This rule applies whether the document received was produced in discovery or in a different context and is not limited to privileged material. The ABA has not provided guidance on what "relating to the representation of the lawyer's client" covers.

While twenty states have adopted ABA Model Rule 4.4, some other states require only notification of inadvertent productions, but with no requirement to refrain from reading the material.

For example, Illinois Rule of Professional Conduct 4.4(b) requires a lawyer who receives inadvertently sent or produced information "relating to the representation of the lawyer's clients" to "promptly

notify the sender." As described in its comments, the recipient should permit the sender to take protective measures. The rule is also not limited to privileged material.

Moreover, in Illinois and the District of Columbia, Ethics Opinions further differentiate ethical responsibilities based on whether or not receiving attorneys review the material *before* knowing it was mistakenly produced. D.C. Ethics Opinion No. 256 states where "the receiving lawyer in good faith reviews the documents before the inadvertence of the disclosure is brought to the lawyer's attention, the receiving lawyer engages in no ethical violation by retaining and using those documents."

Now that vast stores of data can be inadvertently disclosed just by sending a link, perhaps it is worth reflecting on whether additional protections should exist for privileged and confidential information.

However, if the receiving lawyer knows of the inadvertent disclosure *before* examining it, the receiving lawyer must return the material and may not read or use it.

Other states require the receiving attorneys to stop reading inadvertently produced material when they determine the material is privileged. For example, California Rule of Professional Conduct 4.4(b) requires the receiving lawyer to "refrain from examining the writing any more than is necessary to determine that it is privileged or subject to the work product doctrine."[4]

Texas has not adopted Model Rule 4.4(b), and Texas Professional Ethics Opinion No. 664 found lawyers generally have no duty to notify opposing counsel of receipt of inadvertently-sent confidential information.

Civil Procedure rules may include other protections, for privileged material only, disclosed in the course of discovery. As described above, Texas Rule 193.3(d) provides a ten-day window for a producing party to correct inadvertently produced privileged information. It further states that "[i]f 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."

This rule seemingly prevented plaintiff's lawyers from immediately reviewing the contents of Jones' phone, because it potentially contained privileged information intermingled among its other contents.

Reynal failed to take these actions within the requisite ten days, so privilege was arguably waived, at least assuming the notice he received was adequate to do the job under all applicable Rules.

While focus has rightly been on Jones' attorneys' actions and Jones' misrepresentations about his texts and emails, was it appropriate for Bankston to use the phone data at trial with no notice?

Would the disclosure be viewed differently if it were plaintiffs' lawyers who accidentally sent confidential phone copies to Jones' lawyers? What if plaintiffs' counsel had notified Jones' counsel that it sent a link in error, and then Jones' counsel used the contents at trial anyway? What if Jones claimed the right to use the plaintiffs' phone data however he wanted, including on his broadcasts, since it was not labelled confidential when it was inadvertently produced, as the confidentiality order required to apply?

There is also a question as to how far a recipient of inadvertently-sent links to large data stores must go to determine whether and what might be privileged, and what files may or should be reviewed. In this case, would Bankston need to stop downloading when he saw the production link materials were not intended for him, and potentially privileged, based on file names?

For states that would require attorneys to stop review of privileged materials, it is unclear whether they may download the material, and whether they might then review any files not clearly reflecting potential privilege based on folders and names.

For inadvertently-sent files where privilege is not apparent, counsel may be permitted or even required, as zealous advocates, to review them. To the extent duties may arise from ethical rules, which ones generally apply to any third-party confidential information, or civil procedure rules related to privilege waiver in discovery? Is it desirable and logical for attorneys' duties to avoid using inadvertent disclosures to depend on whether the disclosure was related to an intended discovery production or not?

Additionally, erroneous links sent as productions, which may contain native files not intended to be part of discovery at all, are unlikely to carry confidential designations. While Judge Gamble allowed Jones' attorney to identify records to seal after the trial, the case reflects a danger for inadvertently produced client personal information to become unprotected and public.

Key takeaways

Ethical rules require attorneys to have technical knowledge and competently protect client confidential information. But when they receive information that was inadvertently sent or produced, ethical duties will vary by applicable state ethics and procedural rules, and at times by whether it was part of a discovery production or not.

Now that vast stores of data can be inadvertently disclosed just by sending a link, perhaps it is worth reflecting on whether additional protections should exist for privileged and confidential information.

The Jones discovery debacle highlights eDiscovery ethical obligations on requesting and responding parties, and raises questions of whether ethical and procedural rules may need updating to keep up with technological advances.

Ethics Committees may consider providing further guidance on inadvertently sent information as the nature of inadvertent disclosures changes with technology. Cloud storage and file sharing

platforms have made it easier than ever to share, and inadvertently send, large stores of files to others, creating new challenges and dangers for attorneys.

Notes

[1] In related Connecticut litigation, the judge held a hearing to determine how confidential medical information produced in that proceeding found its way to Jones' lawyers in the Texas matter. Jones' attorneys stated Jones' Connecticut attorneys provided the data to one of Jones' financial attorneys, who, without reviewing it, provided it to Reynal, who was not admitted in the Connecticut proceeding. Reynal also did not review the data but copied it to his firm's cloud storage. The Connecticut attorney, facing disciplinary proceedings, pled the Fifth. E. Cousins, 'The Worst Day of My Legal Career': As One of Alex Jones's Lawyers Takes the Stand, the Other Pleads the 5th, Law.com, available at https://bit.ly/3xY60QB.

[2] At the hearing, he said the paralegal contacted him because, "this file that we now have on our server has clogged up our entire server. It's like 300 gigs. What's going on?"

[3] *See* Tex. R. Disc. P. 1.01 comment 6; ABA Model Rule 1.1.

[4] *See also*, New Jersey Rule 4.4(b) ("A lawyer who receives a document or electronic information and has reasonable cause to believe that the document or information was inadvertently sent shall not read the document or information or, if he or she has begun to do so, shall stop reading it."); New Hampshire Rule 4.4(b) (requiring the receiving attorney to "promptly notify the sender and shall not examine the materials ... [and] shall abide by the sender's instructions or seek determination by a tribunal").

About the authors



Tara Emory (L), senior vice president of strategic operations and consulting at **Redgrave Data**, helps clients identify and leverage technology to improve their eDiscovery processes and information governance programs. She is based in northern Virginia and can be reached at tara.emory@redgravedata.com. **Eliza Davis** (C), counsel at **Redgrave LLP**, has extensive experience in information law matters and advises clients on eDiscovery, information governance, and data privacy issues and strategies. She is based out of Chicago and can be reached at edavis@redgravellp.com. **Aviva Surugeon** (R), an attorney also based in the firm's Chicago office, advises and counsels clients on the eDiscovery process and assists with implementing strategic information law solutions. She can be reached at asurugeon@redgravellp.com.

This article was first published on Westlaw Today on September 29, 2022.