JS|HELD

PERSPECTIVES

Protect What You Produce: Practical eDiscovery Lessons Learned from the Alex Jones Case

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

Making crucial errors in eDiscovery can prove detrimental to both lawyers and their clients. Nowhere is this more apparent than in the case of the Sandy Hook parents who won a $49.3 million judgment, including $45.2 million in punitive damages, against Alex Jones, the InfoWars founder and commentator.

This case – Heslin v. Jones, Tex. Dist. Ct., No. D-1-GN-18-001835 – was brought by Neil Heslin and Scarlett Lewis, whose six-year-old son, Jesse, was among 20 children and six teachers killed in the Sandy Hook Elementary School mass shooting in Connecticut in 2012. They sued Jones for repeatedly calling the shooting a hoax and sought $150 million for defamation and intentional infliction of emotional distress.

Jones' attorneys inadvertently gave the parents' lawyer, Mark Bankston, the entire digital copy of Alex Jones' mobile phone with every text message that had been sent for the past two years. This provided critical information that would help Bankston's clients when Jones testified at trial in his defense. Bankston indicated the text messages made mention of Sandy Hook despite Jones' previous claim in sworn statements that he had no such text messages.

Jones' defense attorneys didn't take any steps to identify any of the information as privileged or protected. Instead, they argued that the plaintiffs' attorneys should have immediately destroyed the inadvertently produced records and requested a mistrial. The judge denied the request. As a result, Jones is facing a multi-million dollar judgment. The inadvertently disclosed text messages may have swayed the jury to hit Jones with a larger amount in punitive damages for the plaintiffs who were seeking $150 million. Jones' media companies filed for bankruptcy during the trial. Furthermore, if charged, indicted, and convicted of criminal perjury charges, he also could serve time in prison.

While many cases will not follow such a dramatic arc, unintentionally handing over the entire digital contents of a mobile phone, without claiming privilege or protection for any of the information, will prove injurious to any client – whether sympathetic victim or wrongdoer – when a legal team makes such a mistake.

This article explains how to effectively implement an eDiscovery process, especially when it comes to gathering and protecting information requested from and found in mobile phones and text messages. It will also outline steps that attorneys and their litigation support teams can take in order to avoid damaging outcomes for their clients.

MOBILE PHONES: A KEY COMPONENT IN eDISCOVERY

For many years mobile phones played a background role in eDiscovery and were examined with less scrutiny than more "essential" data sources such as laptops and email. That has changed drastically in recent years with mobile phones now being a key component in almost all legal matters involving eDiscovery. The shift in focus to mobile data in litigation has been accelerated by increased communication, both in volume and breadth of topics, via text or messaging applications. Business topics once reserved for email are now regularly discussed via phones as the working world has become more mobile.

With mobile phones now being an integral part of eDiscovery calculations, counsel must take great care in how the data residing within a mobile phone is examined and produced. Because mobile devices slip so conveniently into our pockets, we may take for granted all the types of information that reside within. A person's mobile phone now likely contains personal health information (PHI), banking information, personal photos and media, social media information, browsing history, password management, geolocation history, and more.

It would be a mistake to produce all of this information in a legal proceeding sight unseen. While it is recommended during the data collection stage to capture as much data as possible from mobile phones (via "full images" or backup retrievals), it is essential to have this data flow through the normal rigors of the eDiscovery process before being turned over to other parties.

Digital forensic experts have tools to report on types of data captured from mobile phones and can work with counsel to isolate targeted data sources of interest to the matter (e.g., specific chat applications). Non-relevant data sources, while still preserved, can be screened from further review

and production. This not only saves time and cost but also helps safeguard personal data.

When reviewing text or chat messages for potential relevance to the matter, counsel should have the benefit of the context of those messages. Modern data extraction and eDiscovery tools can provide visual representations of text-based discussions that include each party's response, the time of each message, attached or referenced material, and even reactions or emojis in the conversation.

It is important to understand how these conversations are captured and portrayed when starting the review. Communication cadence will vary in different types of conversations and should be considered when "tokenizing," or breaking down how much of a conversation is helpful to review at one time. For example, a busy stock trader may send hundreds of messages in less than an hour, while a group chat tied to a monthly meeting might have sparse activity over the course of a year. Ediscovery experts can provide guidance on how to best handle each type of conversation to provide the best possible context for counsel reviewing the information. With appropriate context, accurately collected metadata, and an informative visual representative of the discussion, attorneys are able to make more accurate decisions on the relevance of a text conversation before producing it to the other side.

Though mobile phone data may seem different than "traditional" data sources, it is important to follow the same procedures and practices for collecting, reviewing, and producing data.

PRACTICAL TIPS TO AVOID eDISCOVERY PROBLEMS AND ERRORS

As technology expands the parameters of what is discoverable, it is important to know how to handle digital documents in their various forms and how to handle eDiscovery requests. The following are steps to consider in such matters:

- First and foremost, engage eDiscovery / litigation support professionals (either within or external to the firm) who regularly guide the technical process of collecting, reviewing, and producing data relevant to a litigation. This tech-savvy group can help the legal team navigate the complex procedures required throughout the case.
- Engage in "Meet and Confer" sessions with opposing counsel. During such sessions, the parties spell out and agree upon protocols and timing for sending of data potentially relevant to the matter. The eDiscovery team should be consulted in this process to ensure:
    - Requested data can be reasonably collected and produced;
    - The format of data transmission is compliant;
    - The agreed upon timing can be achieved without rushing so that potentially privileged or damaging data is not produced;
    - A "claw back" agreement is in place to protect against the inadvertent production of privileged or sensitive information.
- Follow proper chain of custody in collecting and documenting all evidence. In the digital world, proper tracking of evidentiary data collected throughout the process is essential to get to the truth of the matter.
    - Having proper protocols and chain of custody to track digital evidence is paramount to admissibility in court.
- Thoroughly question clients to obtain comprehensive knowledge on their usage of communication platforms. This ensures complete collection of all sources and devices, even in cases where the client may have dictated the communication rather than typing it directly.
    - Having an Electronically Stored Information (ESI)-based interview questionnaire form is helpful to ensure all topics are covered during the interview.
- Perform review of potentially relevant data in a dedicated eDiscovery review platform. These platforms have become very user-friendly and non-technical attorneys can be easily trained on proper usage.

- At a minimum, perform keyword searches that would capture potentially privileged or damaging text content during the review process.
- Sensitive medical or "Protected Health Information" (PHI) should be screened and potentially separated in the review population. This screening can be assisted by automated processes, such as checks for common patterns or ID numbers that are found in patient medical data.
- Utilize a document coding strategy to force attorney document reviewers to explicitly tag relevant data (i.e., nothing should be implicitly produced), and also potentially privileged data so it can be screened separately prior to any data production.
- Prior to production of data to the other side, perform a "privilege check" which would typically include:
    - A separate keyword search of the production set as a "sanity check;"
    - Redaction of sensitive materials, as appropriate;
    - Completion of a privilege log that outlines withheld materials.
- Productions should be directly prepared by the eDiscovery / litigation support team who will "sign off" on a complete and verified production before it is sent to the other side.

CONCLUSION

Having a repeatable eDiscovery process in place will protect counsel and their clients from producing data or other information that may be privileged, sensitive, or damaging to the case. This process should include having a plan for all data sources, including mobile phones. It is important to realize that eDiscovery / litigation support professionals bring not only modern technology but also their expertise which is invaluable when both designing and implementing the process.

CONTACT US

Mike Gaudet is a Managing Director in J.S. Held's Digital Investigations & Discovery group within the Global Investigations Practice. He has more than 20 years of experience providing solutions for corporations, legal teams, and government agencies related to data discovery and governance challenges. He is an expert eDiscovery practitioner and technologist. He has experience executing ad-hoc projects as well as designing and implementing Software-as-a-Services (SaaS) solutions.

Contact Mike Gaudet at mike.gaudet@jsheld.com or +1 281 415 5742.

Richard Chung is a Managing Director and a team lead in J.S. Held's Digital Investigations & Discovery group within the Global Investigations Practice. Based in New York, he has more than 18 years of experience in technology consulting. His expertise is in digital forensics and e-discovery, in connection with all aspects of investigations, litigation, and antitrust and merger matters. Richard has worked across a wide variety of industries, including financial services, pharmaceutical, healthcare, construction, energy, and technology. His extensive experience and decisive expertise make him a trusted advisor on a variety of technology consulting engagements involving data preservation, data analysis, document review, and document production.

Contact Richard Chung at richard.chung@jsheld.com or +1 347 786 8958.

Stephen O'Malley is a Senior Managing Director and serves as the practice leader for J.S. Held's Digital Investigations & Discovery group within the Global Investigations Practice. He has been engaged on some of the largest multinational investigations and has given expert testimony in the areas of analysis and restoration of electronic data, electronic discovery best practices, and testing of related computer software. He is an expert eDiscovery practitioner and data analyst. Stephen has significant experience in major fraud and corruption investigations including FCPA, Ponzi schemes, U.S. Department of Justice, and SEC investigations; in multijurisdictional litigations; in provision of evidence for litigation support; and in advanced data analysis.

Contact Stephen O'Malley at somalley@jsheld.com or +1 718 510 5617.