779-preview

Mon, 6/21 1:05AM 5:01

SUMMARY KEYWORDS

data, emails, electronic discovery, e discovery, litigation, electronically stored information, electronic, social media postings, process, crucial, ediscovery, analysis, data retention policies, text messages, volume, computer, asi, magnetic tapes, discovery, trial

00:01

Good morning. My name is Kirby Drake, and I'm with the firm of konchog lp. Today I'm here to talk about examining the ebb and flow of electronic discovery, tips, tools and ethics. So the discovery phase of litigation is crucial and increasingly depok dispositive, as fewer and fewer cases go to trial. At the same time, discovery itself is now overwhelmingly focused on electronic information winning computer files, emails, and social media, and the risk of destruction of evidence leading to spoliation and possibly sanctions are higher than ever. So looking at the second slide, many of the second many of the problems of discovery arise from issues of language. So let's first start with a good definition of E discovery or electronic discovery, generally defined as the electronic aspect of identifying, collecting and producing electronically stored information, sometimes referred to as ASI. In response to requests for production in a lawsuit or investigation is AI typically exists in a medium that can only be read using computers, such as cache memory, magnetic disks, which may be computer hard drives, or floppy disks, optical disks, such as DVDs or CDs, and magnetic tapes. But it can also include emails, text messages, documents, presentations, databases, voicemail, audio and video files. Social media postings and websites can be found in a variety of devices, including desktop and laptop computers, network servers, tablets, and phones, emails where a lot of the crucial electronically stored information or asi may be found. People often say Frank and very honest things in emails. Everyone in ediscovery knows that people writing emails will, much like the kids in the old Art Linkletter show say the darndest things. They seem to forget that emails might someday be discovered and used against them in a court of law or public opinion. Of course, text messages and social media postings can be even worse these days. private emails, text messages. Social media postings, even when made private can have a way of becoming public, especially when discovered in litigation and introduced into evidence at trial. So there's many things that can influence ediscovery. And how easy or difficult it can be to do in a lawsuit can depend on the size and the nature of the company

and the industry as well as whether it's a civil or criminal case. We can also look at data infrastructure, there's questions of whether whether the data is centralized or widely dispersed. Also have to ask whether there are data retention policies in place that might control how the data is maintained. But you also have to look at how it might be enforced. With a with a more corporate client, you might ask whether there are dedicated internal IT resources that can be assigned to handle an E discovery task. And of course, there's always time constraints, you have production deadlines and litigation, you may have retention schedules that that govern what the company or client may do. And then of course, the resources that are available, you may have to ask whether there are specialized tools or expertise needed to access the data, and whether there is encrypted or sensitive data involved. So the graphic on slide four provides a good model of the typical ediscovery process. While we don't necessarily have time to go through each part in depth today, we'll highlight a few items. We start with the volume of data, and then we focus on the relevance as you move through the process. So we want to start by first getting the electronic house in order to mitigate the risks and expenses. We identify the potential sources of electronically stored data, such as through illegal hold interviews of employees, and other other means to hopefully define the scope of the data involved. Then we move into the preservation and collection process. This will mitigate the risk of loss of data and hopefully be able to collect the data in a manner that is legally defensible. Sometimes, we look at grouping the processing, review and analysis steps together. This reduces the volume of VSI and it converts the USI two forms that are more suitable for review and analysis. So you want to discern at an item level exactly what data is contained in the whole universe that submitted and hopefully then begin to reduce the data by selecting what what items of data are appropriate to move to the next level of review. This has to happen with a strict adherence to process auditing, quality control, analysis and validation and of course Chain of Custody considerations.