



## Demystifying ESI for plaintiffs' lawyers

ELECTRONICALLY STORED INFORMATION (ESI) IS A VITAL SOURCE OF DISCOVERY AND EVIDENCE WHEN LITIGATING AGAINST GOVERNMENT AGENCIES AND CORPORATIONS

The discovery you need to effectively prosecute your client's claims will no longer be found in a filing cabinet within an appropriately labeled manila folder. No, no – that's a thing in the past. Your client's ESI will likely be found on their iPhone or their laptop, but an entity's ESI will be found in electronic systems that you, dear reader, know nothing about. The goal of this article is to help you understand and familiarize yourself with certain tools, resources and strategies that will help you navigate these virtual gold mines.

### Getting with the ESI times

I was recently on a panel where I shared some guidance regarding how to secure ESI in civil-rights cases. At the end of my presentation, a fellow panelist playfully exclaimed: "ESI?! What's that?" As a former public-entity defense attorney, I can confidently say that defense attorneys have a huge advantage

over plaintiffs' attorneys when it comes to ESI discovery. Defense law firms spend hundreds of thousands of dollars training their associates on how to understand their clients' systems of ESI, how to prevent an inadvertent disclosure of privileged and protected ESI, and perhaps most importantly, how to articulate to a judge *just how burdensome* it is for their client – say, a massive corporation with multiple offices or a county department with 20,000 public employees – to gather, collect, extract, review and produce ESI that is responsive to your whopping 13 requests for production of documents.

There is no question that society is moving towards virtual platforms in all aspects of our lives. If you, as a plaintiff's attorney, choose to rely on antiquated discovery strategies, your client will be at a disadvantage that could prove fatal come an MSJ or trial. We're talking discovering only 10% of what your client

is entitled to. This is especially true if you're a plaintiff's attorney who regularly goes up against police departments, trucking companies, hospitals, universities, and Big Tech such as Uber and Lyft. Let's get you schooled on some ESI.

### "ESI – what's that?!"

Under California law, ESI is broadly defined as "information that is stored in an electronic medium." (Code Civ. Proc., § 2016.020, subd. (e).) The term "electronic" is defined as "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities." (Code Civ. Proc., § 2016.020, subd. (d).)

This is in contrast to federal law, which defines ESI with greater specificity: "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations – stored in any medium from which

information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form.” (Fed. Rules Civ. Proc., rule 34(a)(1)(A).) So, that’s the legal definition of ESI, which should seem pretty straightforward. But as you will see, the ESI jargon you’ll encounter will be much more complex.

Speaking in lay terms, the “places” where an entity’s ESI is stored includes networks, databases, third-party systems, and Cloud-based ESI storage technologies (e.g., Dropbox, One Drive, Google Drive). An entity’s ESI may also be stored in employees/agents/officers’ workstations, home and shared folders, cellular telephones, text and instant-messaging services, and Cloud computing accounts (e.g., personal email accounts, twitter accounts, Facebook accounts).

Some common “types” of ESI include electronic mail, email attachments, email metadata information (e.g., message contents, header information, and logs of electronic mail system usage), user-created files contained on hard drives and/or networks (e.g., Microsoft Office Documents such as Word, Excel, Power Point, PDF, photographs, video and audio recordings), logs of activity used to process ESI on computer systems, embedded data (i.e., draft language, editorial comments, and other deleted matter retained by computer programs), and metadata (i.e., information describing the history, tracking, or management of an electronic file.)

In California, an attorney can serve requests for production of documents which specifies the format in which the ESI is to be produced, e.g., Word or Excel for original/native formats, TIFF or PDF for image formats, and OCR for searchable scanned text. (Code Civ. Proc., § 2031.030, subd. (a)(2).)

Sure, defense counsel can object to your preferred format, but they are still required to provide a format that is “reasonably usable,” which means the onus is on the defendant to convert the ESI into a format that is accessible. (Code Civ. Proc., § 2031.280, subds. (c), (d).)

Keep in mind, however, that the costs may shift to the plaintiff if the conversion is expensive. (Code Civ. Proc., § 2031.280, subd. (e).) Federal rules are similar in this respect – if you do not specify the format, defense counsel may produce the ESI in a format that is “ordinarily maintained” or in a “reasonably usable” format. (Fed. Rules Civ. Proc., rule 34(b)(2)(E).)

### Preservation letter

The second you are retained on a case you should send a preservation letter to the public/private entity involved and any third party that may have ESI relevant to the case. The preservation letter needs to specify with great detail the party names, witness names, time periods, and sources of electronic information, as well as the manner in which the ESI is to be preserved. You should know that this preservation letter will ultimately be passed along to the personnel within the entity’s information technology department, and that personnel will then follow the preservation roadmap *you* created to preserve *your* client’s evidence. Depending on the entity’s retention policies, the sooner you trigger the duty to preserve, the less likely there will be an inadvertent permanent deletion of critical evidence.

The preservation letter should – at the minimum – demand the following: (a) that the entity take steps to ensure that no data loss occurs from recycling computers, re-provisioning servers, re-configuring applications or other managing data created by custodians over the course of the litigation; (b) that the entity not modify or delete any electronic data files contained in online data storage and direct access storage devices attached to the entity’s mainframe computers, servers, or minicomputers; (c) that the entity cease any activity that may result in the loss of offline data storage for backups and archives (e.g., hard drives, flash memory devices, magnetic tapes and cartridges, CDs and DVDs), including rotation, destruction, overriding, or erasure of such media in whole or in part;

and (d) that the entity must not alter or erase electronic data contained on network stations or stand-alone personal computers belonging to employees/agents/officers, nor perform other procedures that may impact such data (e.g., data compression, disk defragmentation or optimization routines).

Of course, you should include in the letter a demand that digital recording equipment and surveillance video, and all data captured by these devices, be preserved. I typically take it a step further and demand that the entity preserve and maintain logs documenting who viewed the video evidence, when the video evidence was viewed, whether the video evidence was downloaded at the time of viewing, and if so, information regarding the server system or device the video evidence was downloaded to.

It goes without saying that a plaintiff must also preserve relevant ESI that she/he may have stored in cellular devices, laptops, desktop computers or social media platforms. Adverse inference instructions can go both ways. (See *Gatto v. United Air Lines, Inc.* (D.N.J. Mar. 25, 2013) U.S. Dist. LEXIS 41909, 2013 WL 1285285 [adverse inference instruction given to the jury regarding a plaintiff’s deactivation of a Facebook account].)

### Meet and confer

Once litigation begins, both California and federal law require the parties to meet and confer regarding ESI. The California Rules of Court provide that the parties must meet and confer prior to the initial case management conference regarding the following ESI issues: (a) preservation of discoverable ESI; (b) form or forms in which information will be produced; (c) time within which the information will be produced; (d) scope of discovery of the information; (e) method for asserting or preserving claims of privilege or attorney work product, including whether such claims may be asserted after production; (f) method for asserting or preserving the confidentiality, privacy, trade secrets, or

proprietary status of information relating to a party or person not a party to the civil proceedings; (g) how the cost of production of ESI is to be allocated among the parties; and (h) developing a proposed plan relating to the discovery of ESI. (Cal. Rules of Court, rule 3.724(8).)

The Federal Rules of Civil Procedure require an early meeting of counsel prior to the initial scheduling conference. During this meeting, the parties meet and confer regarding various litigation and discovery issues, including ESI. (Fed. Rules Civ. Proc., rule 26(f)(3).) Most district courts provide the parties with an ESI checklist that can be used during the meeting. You may find that defense attorneys prefer a more perfunctory discussion regarding ESI than what Rule 26(f) envisions. This is exactly why an ESI checklist is so helpful during this meeting. I've made it a practice to use a slightly altered version of the Northern District's ESI checklist in all of my cases, not just my federal cases: [https://www.cand.uscourts.gov/filelibrary/1118/ESI\\_Checklist-12-1-2015.pdf](https://www.cand.uscourts.gov/filelibrary/1118/ESI_Checklist-12-1-2015.pdf)

After the parties have met and conferred, you should weave into the joint report (or CMC statement if you're in state court) the following ESI paragraph: "The parties have met and conferred pursuant to Federal Rule of Civil Procedure 26(f) [California Rules of Court, Rule 3.724(8)] regarding reasonable and proportionate steps taken to preserve evidence relevant to the issues reasonably evident in this action. The parties anticipate *entering into a stipulation regarding discovery of electronically stored information* in order to ensure full cooperation and production of electronically stored information." (Emphasis added.)

Whether you are in state or federal court, I strongly urge you to enter into a stipulated order governing discovery of electronically stored information. You may receive some pushback in state court since such a stipulation is both not mandatory and uncommon. Still, and depending on the type of case you have and how voluminous you expect ESI

discovery to be, you should broach this stipulation to the state court judge during the case management conference to convince her or his honor that this stipulation will save the parties and the court resources and time as it will help guide the parties through ESI discovery.

### **Stipulated order governing discovery of ESI**

The stipulated order governing discovery of electronically stored information should contain the following paragraphs: (1) purpose; (2) cooperation; (3) ESI person most knowledgeable; (4) preservation; (5) search; (6) production formats; (7) phased discovery; (8) documents protected from discovery; and (9) modification. You can find a model stipulated order governing ESI discovery from the Central District of California at this link: <https://www.cacd.uscourts.gov/sites/default/files/documents/ADS/AD/ADS%20-%20Model%20Stipulated%20E-Discovery%20Order%20in%20PDF.pdf>. For our purposes, I'll go into detail regarding the most important paragraphs.

The ESI person most knowledgeable is the most powerful tool you have as a plaintiff's attorney when it comes to uncovering ESI. Sure, the government agency or private corporation will designate the person, but they must designate a person who is "knowledgeable about the technical aspects of e-discovery, including the location, nature, accessibility, format, collection, search methodologies, and production of ESI in the matter." Within the "ESI person most knowledgeable" paragraph, you'll want to include the name of the designated PMK for each of the ESI categories. For example, "Defendant Mega City designates Agent Smith with regard to Mega public employee's electronic communications and C drive for Mega employees Jane Doe and John Doe from January 1, 2012, to January 1, 2022."

The "production format" paragraph is also important. If the case is not overly complex, the following paragraph may do the trick: "The parties agree to produce

documents in PDF, TIFF, native (e.g., Word, Excel, PowerPoint) and paper file formats. If particular documents warrant a different format, the parties will cooperate to arrange for the mutually acceptable production of such documents. The parties agree not to degrade the searchability of documents as part of the document production process."

The final paragraph, which in my opinion is worthy of some discussion here, is the "phased discovery" paragraph. You should agree to phased discovery which allows an initial round of production upon service of the request for production of documents from a specific ESI storage medium (e.g., defendant employee's electronic mailboxes and email archives) with the understanding that the entity may be required to conduct additional searches within other ESI mediums (e.g., the C drive of the assigned internal affairs investigator). If your focus is to secure email communications between employees, you may want to include the following language: "When a party propounds discovery requests pursuant to Federal Rules of Civil Procedure, rule 34, the parties agree to phase the production of ESI and the initial production will be from the following sources and custodians: Email accounts of certain individuals, including their mailboxes and archived emails. Following the initial production, the parties will continue to prioritize the order of subsequent productions."

### **ESI person most knowledgeable**

The deposition of the person most knowledgeable regarding the entity's electronically stored information should be set at the outset of discovery. (Code Civ. Proc., § 2025.230; Fed. Rules Civ. Proc., rule 30(b)(6).) You'll gain a better understanding of the universe of ESI that exists within that specific government agency or private corporation virtual discovery fields. You'll also gain understanding of what search terms and parameters are workable within that entity's information technology operations. Below are some of the key

topics you'll need to cover during the ESI PMK deposition.

#### **Organizational structure**

Before you get too much into the weeds, you need to have an understanding of the virtual layout of that entity's electronic-mail system, document-management system and record-management system. You also need to familiarize yourself with the overall IT management and staffing and the various mediums that hold the ESI (e.g., home folders, shared folders, C drives, network servers, Cloud storage technologies) as well as the various units that exist within the department itself (e.g., network unit, database administration unit, data security, data center, software development).

Remember that the employee's mailboxes and email archives are the most common mediums where data resides. The other common mediums are home folders, shared folders, and local C drives. There are certain data centers where the server which stores employees' emails will be located. These are commonly referred to as the mail servers. There will also be an email archive system which keeps a copy of emails that are sent or received. Depending on the entity's retention policy, these archive systems will hold a copy of every email that is sent or received by an employee even if the email was deleted. (Hence why it is so important to issue the preservation letter the second you retain the client.)

Employees can store electronic files in various mediums, including home folders, shared folders, and local C drives within their own workstations. The home folders are considered private in that only the employee can gain access to the contents. Of course, the information technology department has capabilities to conduct searches within these home folders without physically going to each of the employee's work stations (and without the employee's knowledge).

Another location where an employee can store electronic files is in the C drive

located within the employee's workstation. Since the employee's workstation is connected to the entity's networks, information that is stored in that specific C drive can also be searched as the networks are remotely accessible.

#### **Retention policies**

Now that you understand the various locations where ESI may exist, you need to understand the backup system for those locations as well as the entity's retention policies. The importance of this is twofold – determining whether spoliation occurred and narrowing search parameters for time periods.

In California, “spoliation occurs when evidence is destroyed or significantly altered or when there is a failure to preserve property for another's use as evidence in current or future litigation.” (*Hernandez v. Garcetti* (1998) 68 Cal.App.4th 675, 680.) In federal court, “spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation.” (*United State v. Kitsap Physicians Serv.* (9th Cir. 2002) 314 F.3d 995, 1001.) There are two key questions that must be asked regarding spoliation: (a) when was the IT staff notified about the preservation letter; and (b) whether measures were taken to preserve the files that were due to be purged in accordance with the entity's then-existing retention policy.

#### **Search parameters**

Learning how to conduct searches within these mediums is critical. You need to ask the PMK what is the appropriate syntax for a particular query. What I mean by syntax is, for example, Boolean operators such as parentheses, asterisk, exclamation point, “AND,” “OR,” and “NOT.” Typically, mailboxes and email archive systems will have Boolean search capabilities. Here is a link to my go-to cheat sheet when I create queries using Boolean search connectors: [https://guides.law.stanford.edu/ld.php?content\\_id=37111030](https://guides.law.stanford.edu/ld.php?content_id=37111030).

I highly recommend that you come to the ESI PMK deposition with queries already constructed. You can then ask the PMK whether each of the queries and the syntax used to construct the queries is compatible with that entity's system. If the PMK testifies that the syntax is not compatible, use this opportunity to tailor the query with the appropriate syntax. (Trust me, this is time and money well spent.)

#### **Burden**

Another focus during the ESI PMK deposition is to elicit testimony which speaks to *just how burdensome* it is for the entity to search for and produce ESI in your case. Federal rules are friendlier to the entity as they do *not* require the production of ESI that is “not reasonably accessible because of the undue burden or cost” and good cause must be shown by the plaintiff before a court will order the entity to search the electronic mediums claimed to have been “not reasonably accessible.” (Fed. Rules Civ. Proc., rule 26(b)(2)(B).)

This is in contrast to California law where all electronically stored information is presumed to be accessible, and the responding party bears the burden to show inaccessibility. (Code Civ. Proc., §§ 2031.060, subd. (c); 2031.310.)

Again, you'll want to come to the deposition prepared with queries. You'll ask the ESI PMK the following questions: (a) is the syntax used in this query compatible with your system; (b) how long will it take a staff member to run this query in the system; (c) does the staff member have to be fully engaged with the system while the search is running or can she/he keep working on other tasks while the system is conducting the search; (d) once the system is done running the search, what is the extraction process; (e) how long is the extraction process; (f) can the extraction process be conducted in less time if the staff member uses a flash drive or external drive instead of DVDs?

These questions are key to undermining the defense argument that the IT department will have to spend one



to two months conducting these searches and will require several staffers to get the job done. The reality is that while the searches may take a month or two, and while a couple of staffers may be assigned the task of conducting the searches and retrieving the ESI, only about 10 minutes of their work days will require the staff member to be actively engaged with the searches.

### **Conclusion**

ESI is a mystery to plaintiffs' attorneys for many reasons. We don't know what ESI is. We don't understand the lingo. We're unfamiliar with information technology search terms and parameters. My hope here is to provide you with practical guidance regarding how to approach ESI discovery and how

to utilize certain tools to help you navigate these virtual gold mines.

*Denisse O. Gastélum is the founder and principal trial attorney at Gastélum Law, APC, where her practice focuses primarily on civil rights/police misconduct, sexual assault, wrongful death and catastrophic injury cases, representing plaintiffs in state and federal courts throughout the State of California.*