



NEWMAYER & DILLION LLP  
ATTORNEYS AT LAW

## **A Reminder to Developers About the California E-Discovery Act**

**By: Therese A. Vickers**

The California Electronic Discovery Act, now in its second year, was the most dramatic change in civil litigation since the creation of the Civil Discovery Act in 1986. It requires that civil litigants preserve and potentially produce countless digital documents and electronic information stored on everything from their servers to their cell phones in addition to documents traditionally produced in litigation. As the courts are becoming more familiar with the Act and its enforcement, the purpose of this article is to remind developers of the importance of this law and how it impacts their litigation.

Under prior California law, evidence in civil litigation consisted primarily of witness testimony, documents and tangible things. Under the E-Discovery Act, data or information electronically stored on devices such as cell phones, voicemail systems, blackberries, palm pilots, computers, laptops and/or networks, PDAs (personal data assistants), etc., is subject to discovery and may be retrieved, printed and ultimately become evidence in civil cases. This means that a hastily drafted email or off the cuff voicemail may become Exhibit "A" in your opponent's case.

### **What is "ESI"?**

California law defines "electronic" as technology having "electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities." "Electronically stored information", or ESI, is simply information stored in an electronic medium on devices such as those listed above. ESI is now expressly subject to the rules of civil discovery.

### **Five Things Developers Should Know About the E-Discovery Act**

#### **1. Preservation of ESI:**

Since the Legislature has required that ESI be discoverable in civil cases, it is important to develop an ESI *evidence preservation policy* and take steps to ensure the policy is followed. If ESI containing relevant evidence is destroyed, deleted, overwritten, altered or otherwise lost, you may lose evidence needed to prove or defend your case or you may be subjected to a claim of lost evidence, spoliation of evidence or sanctions for failure to preserve and/or produce relevant evidence. Because California law does not specifically identify the extent of a party's obligation to preserve ESI, it is important to develop your own policy and make sure it is followed. Compliance with one's own preservation policy is a significant defense to allegations that ESI has been improperly lost or destroyed. The duty to preserve ESI is broader than the duty to produce it.

## **2. Scope of Production of ESI:**

The scope of discovery including ESI remains fairly broad. Discovery is permissible if the information or document is relevant to the subject matter of the action and either admissible in evidence or reasonably calculated to lead to the discovery of admissible evidence. The E-Discovery Act does not change the scope.

The E-Discovery Act broadens the methods of discovery from “inspecting” documents to “copying, testing or sampling” documents and ESI. Sampling is often used to determine whether broader discovery should be sought or allowed based upon a sample of information produced. A digital forensic expert will normally assist in the sampling, gathering of relevant documents for production, identifying and protecting privileged documents, as well as reviewing and searching the documents produced by your opponent. This represents a new and potentially very expensive burden on developers in civil litigation.

The E-Discovery Act also allows a party to move for a protective order in lieu of production. However, the party seeking a protective order bears the burden of showing that the information sought is not reasonably accessible because of undue burden or expense.

## **3. Form of Production of ESI:**

Under the E-Discovery Act, the party requesting ESI may specify the form in which each type of ESI is to be produced. The responding party, however, may object to the requesting party’s specified form but must then state in its response the form in which it intends to produce the information. Unless the parties agree, or the court orders otherwise, if the demand does not specify a form for producing each type of ESI, the responding party must produce it in the form in which it is ordinarily maintained or is reasonably usable. If a dispute arises regarding the form, the parties should raise the issues with the court as early as possible to avoid incurring large costs on either side.

Parties may produce ESI in “native format”, which includes all metadata, or in a “reasonably usable form”, which does not include metadata. Metadata is the hidden information affiliated with a document which provides information such as: the document history, creation date, author, editors, access dates and revision history of the document. Usually production in native format is less expensive, but counsel may not want to produce the metadata. The form of production will be determined on a case by case basis.

## **4. Inadvertent Production of Privileged Data:**

With so many documents being discoverable under the E-Discovery Act, documents that are privileged or protected as attorney work product may be produced inadvertently. The E-Discovery Act allows a party to claim the privilege or protection for the document even after it was inadvertently produced. This is called the “claw back provision”, and it only applies to ESI that was inadvertently produced not other documents that were inadvertently produced. The responding party must either return the

information and all copies of it to the producing party or file a motion with the court disputing the claim of privilege within 30 days of receiving the claim. However, once the privileged document or information has been produced, you cannot unring the bell. The opposing party may have read the privileged document and learned information which he could not legally acquire.

### **5. Safe Harbor Provision:**

The law provides a safe harbor provision to a party and its counsel stating that the court shall not impose sanctions on a party or its counsel for failure to provide ESI that was lost, damaged, altered, or overwritten as a result of the routine and good faith operation of an electronic information system. However, to avoid sanctions under this provision, it appears that the party will be required to provide a full explanation of the mistake and why the mistake was in “good faith.”

### **Recommendations:**

1. Prepare an *evidence preservation policy* to preserve ESI and review/revise your *document destruction policy*. Make sure everyone in your company knows this policy.

2. Follow your policy and preserve ESI as early as possible to avoid claims of spoliation of evidence or sanctions for failure to preserve and/or produce relevant evidence.

3. Consult with your attorneys early to review and preserve all evidence relevant to the lawsuit, including ESI, especially if you receive a preservation letter and litigation hold from opposing counsel.

4. Be careful what information is put into emails, voicemails, text messages, instant messages, documents in computers or any other electronic devices in which ESI exists and can be retrieved.

5. Consult with your counsel regarding the form of production of ESI early in the case. Once a protocol for producing ESI is negotiated, all parties will be required to follow it.

### **Conclusion**

The E-Discovery Act was a dramatic change in the California discovery statutes. Now that ESI is discoverable in civil cases, developers should consult with their attorneys early in the case to discuss the issues identified above regarding ESI and how to best minimize costs in light of the sweeping new burdens placed on them by this litigation.

*Therese Vickers is a senior associate in the firm's Newport Beach office focusing on complex construction litigation. She can be reached at [therese.vickers@ndlf.com](mailto:therese.vickers@ndlf.com).*