



THINK NONE OF YOUR CASES ARE EDISCOVERY CASES? THINK AGAIN.

Brandon J. Hechtman Wicker Smith O'Hara McCoy & Ford P.A.
Dennis Kiker Granite Legal Systems

Think about it. Where did you get the information that you have acted on today? How much of it came from a book or letter? How much came from your computer, tablet, or phone? The odds are great that the vast majority of the information that you work with every day comes from a computer. Yet it is remarkable how often attorneys say that their cases are not eDiscovery cases. The truth is that the overwhelming majority of business information is created and maintained on computer systems, including mobile devices. Whether a case is an eDiscovery case is not a question of how large the case is. It is a question of where the information is. And more often than not that information is on a computer or other device. In other words, it is virtually impossible to complete discovery without the “e” anymore. Indeed, there are serious legal, ethical and practical concerns with acting on the misconception that your case is not an eDiscovery case. Simply ignoring eDiscovery may be illegal, unethical, and place you and your client at a strategic disadvantage. If that sounds a bit overstated to you then read on.

LEGAL OBLIGATIONS

Legally, eDiscovery is an integral part of the discovery process. Attorneys have legal obligations to ensure that electronic data is collected and preserved. Although many of the Federal Rules of Civil Procedure referencing eDiscovery are permissive in nature, several are not. Consider the following:

- FRCP 16(b) – The pretrial scheduling order “may provide for disclosure or discovery of electronically stored information.” Do you want it to? If not, is that because you do not want to put undue pressure on the opposing party, or because you do not want that pressure on your client? Does this decision comply with your district’s local rules?
- FRCP 26(a) – Required disclosures include “electronically stored information...that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses.” You might imagine that you are not planning to use any electronically stored information (“ESI”) to support your claims or defenses, but you would probably be wrong. Remember: where does your client keep

all its business information? In boxes, or on computers or in the cloud?

- FRCP 26(b) – “Parties may obtain discovery regarding any non-privileged matter that is relevant to any party’s claim or defense.” At the risk of being redundant, the vast majority of the information that will be relevant to your case is stored on computers and is discoverable.
- FRCP 26(f) – Parties must “discuss any issues about preserving discoverable information,” and their discovery plan must include “any issues about disclosure or discovery of electronically stored information.” This is one of the few clear mandates in the Federal Rules. Are you discussing preservation of information with opposing parties? Do you include disclosure and discovery of ESI in your discovery plan? Have you considered how to preserve the data, including not only locally stored information, but data that is in the cloud?
- FRCP 26(g) – Attorneys must certify that, “with respect to a disclosure, it is complete and correct” and “with respect to a discovery...response..., it is consistent with these rules.” Is it possible to comply

with this rule without addressing ESI in your disclosures and discovery responses?

- FRCP 34(a) – Parties may request ESI within the scope of Rule 26(b). Not only “may” they, but invariably they will. Just check the boilerplate definitions in the next RFP you receive. The question is whether you are responding (see Rule 26(g) above).
- FRCP 37(e) – A court may not impose spoliation sanctions “for failing to provide electronically stored information” only if it is “lost as a result of the routine, good faith operation of an electronic information system.” If currently proposed amendments go into effect, a party will only be sanctioned if it failed to take reasonable steps to preserve information. So, how good is your client’s legal hold process for ESI? Does it even have one? This is particularly concerning with regard to enterprise systems because users maintain data in different ways and may transport it to different platforms (desktop, laptop, tablet, and/or phone). Without a defined process to preserve the data in each location you could be faced with a spoliation problem.

Moreover, over the past 10 years, courts have repeatedly reminded attorneys that they are responsible and accountable for proper identification, preservation and production of relevant ESI. From the seminal *Zubulake* decisions (“[c]ounsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched”) to more recent decisions such as *Procaps S.A. v. Patheon, Inc.*, Case No. 12-24356-CIV-GOODMAN (S.D. Fla. Feb. 28, 2014) (issuing sanctions because outside counsel “permitted its client to self-collect ESI and documents, allowed some of its client’s executives to use a single search term to collect e-mails, and failed to realize that its client never actually implemented the litigation hold”), judges have increasingly taken counsel – inside and out – to task for discovery failures committed by their clients. Note that an attorneys’ search should not end with consulting the IT department. Usually, one should identify target ESI custodians (people who created, used, or viewed the information) and ask them how they view and edit ESI. More often than not, attorneys will find ESI stored locally on personal devices. Attorneys should also ask whether those people are communicating on mobile devices; like e-mail, text messages can be especially revealing.

ETHICAL OBLIGATIONS

The ABA Model Rules of Professional Conduct include both explicit and implicit

requirements that attorneys be conversant with eDiscovery:

- a) Rule 1.1 – The ABA revised the commentary to Rule 1.1 in 2013 to state that attorneys “should keep abreast of changes in the law and practice, including the benefits and risks associated with relevant technology” to remain competent.
- b) Rule 1.5 – The rule on fees has not changed. The standard is reasonableness. However, consider the implications if leveraging eDiscovery could actually reduce overall costs in a case?
- c) Rule 1.6 – Confidentiality is the hallmark of the attorney-client relationship. Maintaining that confidence can be difficult in the modern world. A number of recent cases highlight the risk of inadvertent disclosure of privileged information in eDiscovery. See, e.g., *First Tech. Capital, Inc. v. JPMorgan Chase N.A.*, No. 5:12-CV-289-KSF-REW, 2013 WL 7800409 (E.D. Ky. Dec. 10, 2013) (privileged waived for failure to take reasonable steps to prevent disclosure where the average document was reviewed for only 9.84 seconds).
- d) Rule 3.4 – Did you know that you are ethically required to “make reasonably diligent effort to comply with a legally proper discovery request by an opposing party”? If you have not included ESI in your discovery response plan, where does that leave you?

The DC Bar has added to its competency requirement that an attorney understand the risks/benefits of technology. The California Bar explicitly includes eDiscovery with regard to attorney competence and the duty of confidentiality. Other states are certain to follow suit, as predicted in the ABA Commission on Ethics 20/20 Resolution.

PRACTICAL CONSIDERATIONS

The greatest surprise for many attorneys is not that they are required to engage in eDiscovery; it is that they should *want* to. Why? Because:

- a) Most information is stored on computer devices. If you are not identifying that information, you simply do not know what you are missing. You only know this: you are missing most of the information, and that can never be a good thing.
- b) The information that you are missing could be harmful, or helpful. In either case, you want to know. For every “smoking gun” e-mail, experience shows that there are a dozen innocuous or even helpful ones. You can be sure your op-

ponent will look for the smoking gun, but who will find the information that supports your case if you do not?

- c) Cases are decided on the facts and the law. Generally counsel with a quicker and greater command of the facts has a decided strategic advantage in posturing the case for settlement or preparing for trial.
- d) The most common fear associated with eDiscovery is cost. Of course, spoliation or just not knowing the facts can cost you dearly as well. But, eDiscovery costs need not be a great concern. Technology has advanced significantly over the past decade, and there are a variety of tools, including “predictive coding,” that can help control, or even reduce, the overall cost of eDiscovery. It is important that counsel consult with those internally and externally that can facilitate the efficient and economical collection and review of ESI. Further, it is incumbent upon attorneys to understand and leverage these tools for their clients’ benefit.

Like it or not, eDiscovery is a permanent part of the litigation landscape. Attorneys that embrace it will not only ensure compliance with their legal and ethical obligations, they will realize a significant strategic advantage over attorneys that do not. As for the latter, well, they can always hope those new-fangled computers are just a fad.



Brandon J. Hechtman is an associate at Wicker Smith O'Hara McCoy & Ford P.A. in Coral Gables, FL. Brandon is admitted to practice in Florida, the Southern and Middle U.S. District Courts of Florida, and the District of Columbia. He primarily practices commercial and probate litigation in federal and state courts. He can be reached at bhechtman@wickersmith.com.



Dennis Kiker is a consultant at Granite Legal Systems in Houston, Texas, specializing in eDiscovery consulting and technology. He is a Martindale-Hubbell AV-rated attorney and legal consultant working with law firms and their clients to facilitate and improve discovery response. He is a member of the State Bar of Arizona and the Virginia State Bar. He can be reached at dkiker@granitelegal.com or 713-652-0881.