Full disclosure

How to comply with rules of discovery concerning your electronically stored information

State and federal court rules have always provided that a business's information is discoverable if it is relevant to litigation and not protected by attorney-client privilege. However, the federal court rules and, more recently, the Michigan court rules, have been amended to recognize the expanding use and importance of electronically stored information (ESI). The rules make it clear now that ESI is discoverable, too.

"The discovery rules used to speak of 'documents,' " says Robert B. Holt Jr., partner with Secrest Wardle. "Now, the Michigan rules include 'electronically stored information' of all types."

Smart Business spoke with Holt about the disclosure of ESI and how to protect your business.

Robert B. Holt Jr.
Partner
Secrest Wardle

What kinds of documents are classified as discoverable under the amended rules?

The federal rules address discovery of documents or electronically stored information, including such things as writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations, stored in any medium. Both the state and federal rules are broad enough to include discovery from office computer systems, servers, laptops, backup and archive devices, flash drives and even cell phones and smart phones.

The type of information that can be discovered is expanding, mostly because the volume and type of information that businesses create are expanding so dramatically. Information that used to be exchanged in a series of phone calls is now exchanged in a series of e-mails or instant messages, which can live forever. A modest laptop computer can store the information found in a mid-sized library.

What's more, in addition to the printed information that we can see in an e-mail or word processing document, there is also embedded data, or 'metadata,' that can tell us who created the information, and if and when it was modified. This unseen data can be the subject of discovery, too.

How can a business protect itself from disclosing more information than it has to?

The law recognizes that a business is not under a duty to keep every document, or every bit of electronically stored information, forever. Different businesses will have different information retention policies, often based on the nature of the business and the requirements of regulatory or taxing agencies.

Both the state and the federal rules provide that, absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide electronically stored information if that information is lost as a result of the routine, good-faith operation of an electronic information system. This is known as the 'safe harbor' provision in the discovery rules.

'Routine' is the key word. You cannot implement an ESI destruction or deletion policy after litigation is threatened. You must create the 'safe harbor' before the litigation wave hits the shore.

If you have a system in place for the routine elimination of information that is not essential to your business, you should not have to produce that information in the event of litigation, provided that you've operated your system in good faith. This can avoid the substantial time and expense of producing information that could have been routinely deleted. Moreover, it can minimize the potential for disclosure of information that you don't want your adversary to see.

How can you avoid sanctions for failing to produce information?

The key is to take clear and decisive action to preserve ESI as soon as you know that the information is potentially relevant to pending or future litigation. At that point, an internal litigation hold letter should go out from the CEO, president or other highly placed corporate officer to those who have or may have relevant electronic information, directing them to locate and save all documents and information germane to the subject matter of the actual or anticipated lawsuit.

The timing of the litigation hold letter, if a lawsuit hasn't yet been filed, will vary from case to case. The appropriate author, the subject and the recipients will vary, too. These items should be discussed with your in-house counsel or outside counsel. Ideally, you should have a plan in place for internal litigation hold letters before they are needed.

What are the penalties if ESI is lost or destroyed before it can be produced?

The sanctions can be severe if you're caught outside the 'safe harbor,' that is, if information is gone because you didn't operate your system in a routine, good-faith manner or because you failed to suspend deletion of relevant ESI at a time of actual or likely litigation. The 'adverse-inference' jury instruction is a fairly common sanction. Courts have sanctioned the offending business by telling the jury that it could infer that the ESI (often e-mails) that was 'lost' contained information that was adverse to the business that lost it.

In a Florida State Court case against Morgan Stanley & Co., an adverse-inference jury instruction for spoliation of evidence led to a $1.4 billion verdict. And in federal court in New York, in a recent case involving the liquidation of hedge funds, the plaintiff-investors had routinely destroyed e-mails relating to possible securities fraud four years after becoming aware of the fraud.

The judge called it 'gross negligence' and instructed the jury that it could presume that the lost evidence would have been favorable to the opposing party. In deciding whether to adopt the presumption, the jury could take into account the 'egregiousness' of the investors' conduct in failing to preserve the evidence.

These are not things that you want a judge to be telling a jury about your business. Preparation, knowledge and timely action are the best ways to protect your business. <<

ROBERT B. HOLT JR. is a partner with Secrest Wardle. Reach him at (248) 851-9500 or rholt@secrestwardle.com.

Insights Legal Affairs is brought to you by Secrest Wardle