

# The Metropolitan Corporate Counsel

www.metrocorpcounsel.com

Volume 16, No. 6

© 2008 The Metropolitan Corporate Counsel, Inc.

June 2008



James J. Shrager



Margaret Raymond-Flood



Fernando M. Pinguelo

## Why Your Business May Be At Risk . . .

*Seven misconceptions businesses have about electronically stored information, the electronic discovery amendments to federal and state court rules, and the direct impact these issues have on a business.*

**James J. Shrager,  
Margaret Raymond-Flood  
and Fernando M. Pinguelo**

**NORRIS McLAUGHLIN & MARCUS,  
P.A.**

Nearly all of the information now being created and stored by businesses is being created and stored electronically. Paper files and multiple versions of hard copy are becoming a thing of the past. It is no wonder that federal and state courts have amended procedural rules to recognize this trend, and included new obliga-

tions on lawyers and businesses (no matter how big or small) regarding electronically stored information (“ESI”).

The impact of these new court rules goes far beyond those lawyers and businesses actively involved in a lawsuit; yet businesses continue to remain unprepared to manage these new ESI obligations. In fact, a recent survey of 200 United States commercial businesses conducted by Canvasser Opinion found that almost half of the companies do not have a strategy or policy in place on how to deal with ESI in litigation or in internal investigations.

The new electronic discovery (“e-dis-

covery”) rules represent the federal and state courts’ first formal attempt to address real-life problems faced by trial lawyers in dealing with rapidly spawning electronic records. These rule amendments require businesses to: (1) understand their technology and keep track of ESI; (2) suspend any routine ESI deletion policies when a lawsuit is anticipated or risk exposure to severe sanctions, and (3) be aware of the new obligations imposed upon them.

Here are *seven* of the most common misconceptions businesses have about ESI and e-discovery obligations:

1. *Since we are not presently involved*

*Please email the authors at [jjshrager@nmmlaw.com](mailto:jjshrager@nmmlaw.com) or [mrfflood@nmmlaw.com](mailto:mrfflood@nmmlaw.com) or [fmpinguelo@nmmlaw.com](mailto:fmpinguelo@nmmlaw.com) with questions about this article.*

*in a lawsuit, there is no need to concern ourselves with these new rules.* The reality is that there need not be an active lawsuit or court order in place for there to be an obligation on a business to preserve ESI. Courts recognize that ESI by its nature is prone to loss because computers are repurposed or taken out of commission, backup tapes are reused and sometimes lost, and massive amounts of e-mails are routinely deleted. Also, it can be challenging, time-consuming, and expensive to reconstruct lost evidence after a lawsuit is filed. Businesses are held to a heightened obligation to preserve ESI as soon as a lawsuit is "threatened." In other words, courts require that businesses begin ESI preservation efforts as soon as they can reasonably anticipate a lawsuit. A business that waits to be sued before it begins to collect and preserve relevant data does so at its own peril and at the risk of significant monetary sanctions.

2. *If we were required to save data every time a lawsuit is threatened, our company would be crippled and we'd lose our business.* The reality is that the new rules recognize this problem and provide that a party need only preserve relevant ESI. While there is no duty to preserve, keep, or retain every document in your possession, a business is under a duty to segregate and preserve, in a safe place, what it knows or reasonably should know will likely be requested in a foreseeable lawsuit.

3. *We don't have to worry about these new rules because our lawyers will address any issues that may arise during litigation.* The reality is that waiting to be sued before you focus on these ESI obligations is too late and will be more costly in the long run because you simply cannot implement a plan of action after key evidence has been destroyed. You must understand your technology now and create procedures that demonstrate that you have a plan of action to segregate and preserve potentially relevant ESI if a lawsuit were filed. This plan should also include creating an ESI team (comprised of GC, IT, HR, and/or Risk Managers) and notifying and educating employees on what to do when faced with a potential lawsuit.

4. *Even if we were to lose relevant ESI evidence, the loss was accidental and not intended to destroy harmful information;*

*surely a court would understand.* The reality is that even accidental or innocent loss of relevant ESI is sanctionable when it could have reasonably been prevented. Courts have sanctioned companies for "innocent" destruction of ESI where there was no ESI preservation plan in place. Courts have compelled businesses to restore lost data. In one instance, it cost a company \$9.75 million to restore its lost data. Fortunately, the rules do allow a "safe harbor" that provides limited protection against sanctions for a business's inability to provide ESI that has been lost due to routine operations of an ESI system. However, this safe harbor is only available to those who lose data during normal operations which are part of a "routine" procedure and done in "good faith."

5. *Many of our employees work from home and use their own personal computers; therefore, we don't have to worry about those computers.* The reality is that the new rules widen the scope of ESI to include personal home computers, cell phones, copy machines, fax machines, voice-mail, instant messaging, PDAs, websites, flash drives, etc. As long as your employees are working for you, it does not matter where they are located or what device they are using to generate electronic information related to your business. Plus, ESI covers more than just e-mails. Any drawings, writings, charts, spreadsheets, photos, graphs, sound recordings, images, or any other data compilation stored in any medium on these and future devices are subject to the rules; and your business is expected to keep track of it.

6. *Once data is deleted, it's gone forever.* The reality is that in most circumstances, delete does not mean gone forever. Since every electronic document leaves a "fingerprint" behind, chances are that a computer forensics expert can recover the data. That cost may be imposed upon a party who is not covered by the rules' safe harbors.

7. *We're too small of a business to have to worry about these changes.* The reality is that if you are a business with a computer or any other device that generates electronic data, you are within reach of the new rules.

The law on e-discovery is so unexplored that even some judges and lawyers are not prepared for the ramifi-

cations. Therefore, the rules place a significant premium on knowledge and preparation. Principles of basic fairness, good records management, an understanding of your data and devices, and professional guidance will likely be the hallmarks in these changing times.

---

**"The impact of these new court rules goes far beyond those lawyers and businesses actively involved in a lawsuit; yet businesses continue to remain unprepared to manage these new ESI obligations."**

---

The last place a business wants to be is in court before a judge unprepared for e-discovery issues, and facing severe sanctions. Even worse, a major concern for businesses is that they face the possibility of being innocent of any wrongdoing but may potentially face significant sanctions for "sloppiness" or "ignorance" for failing to fully understand the e-discovery rules and requirements. Because ESI and e-discovery rules present novel and often difficult technical issues, and because those issues are new to businesses, courts and lawyers, early and continual attention to ESI is essential.

---

**James J. Shrager, Margaret Raymond-Flood and Fernando M. Pinguelo are Litigation Partners with Norris McLaughlin & Marcus and they co-chair the firm's Response to Electronic Discovery and Information (REDI) Group which works with clients to develop strategies and implement cutting-edge technologies to manage issues related to information technology. Notably, they recently lectured at the Judicial College of New Jersey on the new e-discovery rule amendments. Fernando was involved with New Jersey's first case addressing the new e-discovery rules.**