METROPOLITAN
CORPORATE
COUNSEL®
APRIL 2015
WWW.METROCORPCOUNSEL.COM

Take Practical Steps Now to Ease the Burden of E-Discovery in the Future

Andrew W. Schwartz / Sills Cummis & Gross P.C.

Sills Cummis & Gross P.C.

The rapid introduction of new technology and software often leads companies to regularly augment and upgrade their technology and software systems. This has caused dramatic increases every year in the amount of electronic data generated even by small companies. While this data revolution has enhanced business operations, making them more efficient and cost effective, it often has the opposite effect in the event of a lawsuit. The sheer amount of data that must be preserved and reviewed during a litigation results in substantial costs to the company and may lead to discovery issues due to the accidental destruction of data. The legal press is replete with frequent reminders of the hazards of not planning for and properly addressing e-discovery. Courts have imposed sanctions for the untimely identification of custodians, delays in implementing litigation holds that lead to the loss of data, failing to preserve relevant electronically stored information, and omitting relevant data sources from productions. Such sanctions have ranged from substantial monetary fines to the ordering of adverse inferences at trial.

Proposed changes to the Federal Rules of Civil Procedure, expected to be implemented later this year, are designed in part to moderate the impact of e-discovery on litigation.

Andrew W. Schwartz

Of counsel to the Sills Cummis & Gross P.C. Product Liability, Employment and Labor, and Health Care Practice Groups. The views and opinions expressed in this article are those of the author and do not necessarily reflect those of Sills Cummis & Gross P.C.

aschwartz@sillscummis.com

The most notable of the proposed changes affecting e-discovery is the elimination of adverse inferences at trial for the negligent destruction of data. Such severe penalty will now be limited to situations in which the court finds "that the party acted with the intent to deprive another party of the information's use in the litigation." *Proposed Rule 37(e)(2).* In cases in which the negligent loss of data causes actual prejudice to another party, courts will be limited to granting relief that is "no greater than necessary to cure the prejudice." *Proposed Rule 37(e)(1).* The Committee Note suggests that, in this situation, relief may range from forbidding a party from introducing certain evidence at trial to allowing the parties to present evidence and testimony to the jury regarding the loss of information. *See* Committee Note to Proposed Rule 37(e). Thus, while the harshest of remedies will no longer apply to the negligent loss of data, courts will still be empowered to impose substantial penalties.

> ***There are certain practical steps companies should take now that will assist with the preservation of relevant data upon the commencement of litigation and support a finding that the company acted reasonably.***

The Committee Notes further suggest that companies that act reasonably to timely preserve and produce electronic data may avoid any sanctions, even if data is accidentally lost. Specifically, under Rule 37(e) "'reasonable steps' to preserve suffice; [the Rule] does not call for perfection." *Id.*

There are certain practical steps companies should take now that will assist with the preservation of relevant data upon the commencement of litigation and support a finding that the company acted reasonably. Specifically, corporate counsel should develop an understanding of the scope of technology at use within the company, prepare a plan together with the IT department to preserve data on each device in use, and identify the devices used by individual employees. In combination, these steps will allow for the timely implementation of a data preservation plan at the outset of litigation.

Know Your Computer and Electronic Data Systems

The duty to preserve data extends to *all* sources of electronic information at a company, not just the data found on common devices in use, such as desktop computers. In order to ensure that all relevant data is preserved, it is important that corporate counsel understand where such data may be found. This requires at least a general understanding of the devices and software programs in use at the company, i.e., a data map of the company's technology. Absent such knowledge, relevant sources of data may be overlooked and data lost before it may be preserved. For example, companies may be sanctioned for not taking adequate measures to preserve the text messages of employees, a data source quickly becoming more prominent. *See, e.g., Passlogix v. 2FA Tech., LLC, 708 F.Supp.2d 378 (S.D.N.Y. 2010).*

The starting point for a plan to preserve data is the computers used on a daily basis by

company employees, whether a desktop or laptop (or possibly both). In many companies, these devices will generate the substantial part of the data that needs to be preserved and produced, including emails, memoranda, spreadsheets and other similar electronic documents. The location where data generated on the company's computers is stored should be identified – whether it is on each computer's own hard drive, on a network server, or elsewhere, such as in the cloud (servers maintained by third-party providers for storing data). Next, other sources of relevant data should be added to the list. This may include more commonplace devices, such as tablets and smart phones, as well more diverse technology, including share rooms, e-rooms and cloud-based systems. Consideration must also be given to the company's website and use of social media– data uploaded to Facebook, Instagram, and Twitter may also need to be preserved and reviewed for discovery.

Once a list of sources of electronic data has been created, it should be periodically updated to stay current in advance of any litigation. To ensure completeness, the IT department should be instructed to alert corporate counsel's office of any substantive technology changes. Such alerts should include not only the addition of new sources of data, but also the retirement of old technology, which may still need to be preserved and accessed as part of e-discovery.

Establish a Protocol for Implementing a Hold on Data

For each device identified that may contain relevant data, a protocol should be created that identifies the specific steps necessary to preserve the data. For some devices, it may be as simple as creating a back-up on a separate storage device. For other devices, however, preservation may be more complicated – especially to the extent a project may be ongoing at the time litigation is commenced. Backups of data maintained by the company should be prepared to be certain that no data is altered, or lost by accident or omission during the litigation. Providers of any cloud-based systems used by the company should be contacted to determine if there are particular steps that need to be followed to preserve data stored in the cloud. In addition, the plan should also include a procedure to capture and preserve employee voicemails and text messages.

The protocol must also address the company's use of an "auto-delete" function on any of its devices or software systems. Many companies employ an auto-delete feature on their email systems to avoid the excessive accumulation of data. In some cases, the auto-delete function on email systems may remove emails in as little as ninety days. Thus, time may be of the essence at the start of a litigation to disable the auto-delete on email systems to avoid the loss of relevant data. Likewise, the company should plan for the suspension of any routine document destruction policy (for both electronic and paper documents).

Creation of a protocol in advance of litigation will enable its rapid implementation and help avoid the loss of data that may result if, after litigation is commenced, the company must first determine the necessary steps to preserve data from deletion.

Track Employees' Use of Technology

The company should next identify the specific employees who use a particular technology. This knowledge will be key to identifying potential custodians of relevant data and implementing the company's data preservation plan at the outset of litigation as to specific devices and employees. A questionnaire should be sent to individual employees requesting that they identify all company electronic devices they use, presently and in the recent past, as well as other potential sources of data, including personal computers and phones. The questionnaire responses should be updated periodically.

As appropriate for the nature of the company's work, consideration should be given to having employees identify specific projects (or products) on which they have worked. To the extent reasonably possible, a master list should be created of projects at the company, the employees assigned to them, and the devices on which project data has been stored. This list should then be used to identify the initial custodians to contact to preserve data at the outset of litigation involving a specific project. A model litigation hold notice should be created that may be sent to the relevant employees upon notice of litigation (note that it is important to confirm electronically the receipt of the notice).

Putting the Protocol to Work

If the foregoing procedures are followed at the time that litigation is reasonably anticipated, corporate counsel will be well positioned to identify the devices that may contain relevant data, the steps necessary to preserve that data, and which employees should receive a litigation hold notice. Thus, even before retaining outside counsel, the company will be able to initiate its data preservation protocol. Following this plan will allow the company to represent to the court that it acted in a reasonable manner to preserve relevant data.