



FEATURE



Collection and Retention of Electronic Data: What Every Business Owner, Manager, and HR Professional Needs to Know

[By Michael Goldfarb]

A client recently asked a question about an email she got advertising “New Rules for E-Discovery: How to Find Your Blind Spots and Reduce Exposure.” She wanted to know if she should be concerned about these new rules with respect to the collection and retention of electronic data collected by her business.

Due to the proliferation of electronic data in everyday business, the federal laws have been amended to meet the challenges of requesting such information during the course of litigation. Parties to litigation acquire information from each other through the process of discovery, generally through the use of such tools as “requests for production of documents” or “subpoenas.” While businesses have to be aware of what might be sought during the course of litigation and the consequences of failing to comply with such a request, there is no need to alter your entire way of storing data because of the rule amendments.

Essentially, the amendments are designed to give guidance on how the discovery of electronic data is to be handled and not so much on what particular types of data a company must retain. Having said that, what you need to keep in mind are several rules of thumb in terms of what to save versus what can routinely be deleted:

1. Any data you are currently required to maintain in paper form must also be retained if collected in electronic form
2. Any electronic data pertaining to an employee who has filed a claim or lawsuit and which data was not routinely deleted prior to the filing of the claim or suit must be retained
3. Any electronic data not routinely deleted must be retained
4. Any data routinely deleted and not mandated by state or federal law to be retained may be deleted.

Here is a brief history of the electronic stored information amendments to the federal code of civil procedure. My suggestion is keep these tips in mind, share them with your IT personnel, the principles of the company, management and your HR department, and convert them into company policy. By using such an approach your company should be more than able to deal with any discovery demand thrown at you in the event of litigation. A lot of what you must retain versus delete is common sense. Always keep that in mind. To that end, the “Safe Harbor” provisions laid out below will provide you with solid guidelines.

Background of Amendments

The Advisory Committee on Civil Rules began analyzing the problem of e-discovery in the 90s and published its proposed amendments in 2004. After some changes, the amendments were approved by the Judicial Conference of the US Supreme Court.

Areas Covered by the Amendments

1. definition of discoverable material;
2. early attention to issues relating to electronic discovery, including the format of production;
3. discovery of electronically stored information from sources that are not reasonably accessible;
4. the procedure for asserting claim of privilege or work product protection after production; and

5. a “safe harbor” limit on sanctions under Rule 37 for the loss of electronically stored information as a result of the routine operation of computer systems.

1. Definition of Discoverable Material

The amendments include the use of a very broad definition of what type of electronic data is discoverable: “electronically stored information.” This term was added to Rules 26(a)(1), 33, and 34. Presumably, this would permit the inclusion of ESI as presently stored and as it may be kept in the future.

2. Early Attention to Electronic Discovery Issues

Rule 26(a)(1)(B) now includes ESI as a matter to be included in a party’s initial disclosures, Rule 16(b)(5) adds provisions for the disclosure or discovery of electronically stored information as an item that may appropriately be included in the court’s scheduling order, and Rule 26(f) added ESI to its list of issues that must be included in the meet and confer process, even going so far as to make ESI part of a discovery plan. Clearly, there is now greater emphasis on the importance of ESI in the discovery phase of a case and the need for its regulation.

3. Form of Production

Rule 34(b) now also focuses attention on the form of production of electronically stored information by permitting the requesting party to designate the way in which it is produced without specifying any single format for production. There is also



FEATURE

a framework for resolving disputes over the form of production. In the event of an objection and failure of the requesting party to specify a format for production, the rules now place the burden on the responding party to notify the requesting party of the format in which they intend to produce the electronically stored information. The responding party can produce the data either (1) in a form in which the information is ordinarily maintained, or (2) in a reasonably usable form.

4. Rule 26(b)(2): Sources That Are Not Reasonably Accessible

Amended Rule 26(b)(2) provides the responding party with two options when faced with responding to an ESI production request based on whether the data sought is reasonably accessible or not. If the source of the ESI is not reasonably accessible because of undue burden or cost, the responding party need not comply. A motion to compel may be filed, and then the court will render a decision.

5. After-Production Retroactive Claims of Privilege/Work Product Protections

Rule 26(b)(5) now sets forth a procedure whereby a party who has produced ESI may retroactively raise claims of privilege and work product protections. The party seeking to establish the privilege or work product claim must notify the receiving parties of the claim(s) and the grounds for it. All receiving parties must return, sequester, or destroy the specified information and await a court decision as to whether the assertion of the privilege is valid.

6. "Safe Harbor"

There are protections for an employer who through routine operation and in good faith deletes electronic data. Rule 37(f) states that absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system. This amendment

addresses the routine modification, overwriting, and deletion of information that is part of the normal use of ESI.



About the Author

Michael Goldfarb has been a practicing attorney in California for the last 15 years, and he is also the president of Holman HR, a nationwide provider of human resources consulting services. Michael has represented management and employers of all sizes on a variety of employment law matters. He is a sought after lecturer to business groups, non-profit associations, and universities, and has written numerous articles in the area of employment law. Michael resides with his wife Lily in Thousand Oaks, California.

EmploymentCrossing is the largest collection of active jobs in the world.

We continuously monitor the hiring needs of more than 250,000 employers, including virtually every corporation and organization in the United States. We do not charge employers to post their jobs and we aggressively contact and investigate thousands of employers each day to learn of new positions. No one works harder than EmploymentCrossing.

Let EmploymentCrossing go to work for you.