



Employers Face New Obligations to Preserve Electronic Data

By Rick Kaiser

Employers need to add another item to their list of New Year's resolutions. Due to recent amendments to the Federal Rules of Civil Procedure, an employer must now safeguard potentially relevant electronic data when it reasonably suspects a current or former employee may file a lawsuit. The amendments signal the judiciary's recognition that electronic data, *i.e.*, email and other relevant electronic data, can inadvertently disappear with the click of a mouse or the absence of an electronic data retention policy.

Even though these amendments do not technically apply to Washington courts, employers are well advised to follow them as state courts generally look to the federal rules when interpreting their own. Acting now can reduce costs and headaches in the event an employer gets sued, regardless of which court has jurisdiction.

Why the Amendments Were Necessary. The amendments reflect the courts' recognition that the old rules did not adequately address the malleable nature of electronic data and the different devices available to access or alter it. Simply put, smoking gun documents no longer exist. Their electronic counterparts do!

Federal court decisions involving situations where a party destroyed or failed to produce electronic data also prompted the amendments. For example, a U.S. District Court judge entered an adverse inference instruction against an employer after finding that it intentionally destroyed emails and failed to safeguard backup tapes that were relevant to an employee's discrimination claim. At trial, the jury found for the employee and awarded her thirty million dollars in damages. *See Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2002). More recently, a Clark County Superior Court judge entered a default judgment against the defendant because it failed, among other things, to establish an adequate system for responding to discovery requests seeking electronic data. *See Magana v. Hyundai*, Clark County Superior Court, Case No. 00-2-00553-2.

What the Amendments Require - New Burdens. Among other things, the amendments require the parties to meet as soon as practicable after the lawsuit is filed and prepare a report outlining how they will handle production of electronically stored data, regardless of which party possesses it. Fed. R. Civ. P. 26(f)(3).

The amendments also require each party to disclose and provide the opposing party a copy and/or description of any electronically stored data that it may use to support its claims or defenses. Fed. R. Civ. P. 26(a)(i)(B). For employment litigation, that means all emails, internet activity, and other electronic data that an employer may use to defend its conduct toward the employee. More important, the data must be produced in the form it is stored - a paper copy is not the same as the electronic copy of the document.

What the Amendments Allow - Costs Shifting and Safe Harbors. The amendments do provide an "undue burden" defense that should shield employers from being obligated to respond to overly broad discovery requests that demand, for example, "all electronic records relating to (the employee's) work." Fed. R. Civ. P. 26(b)(2). In that instance, the employer still is under a duty to identify the data, but has an opportunity to persuade a court that accessing it, or a substantial portion of it, would create an undue burden. If the court agrees, the employee would bear the costs incurred for accessing the data.

Further, the amendments provide that a court cannot sanction a party for failing to provide electronic data lost as a result of the routine, good faith operation of an electronic information system. Fed. R. Civ. P. 37(f).

How Employers Should Respond. In light of these new developments, employers should consider taking the following steps to better defend when a current or former employee signals an intent to sue.

Create an Electronic Data Retention Policy. The policy should generally set forth how an employer retains electronic data, what it permits on its network, and what it doesn't, i.e., personal emails, etc. As relevant here, the policy should:

- Identify the data that is subject to the policy and set forth different time frames for data retention.
- Identify a specific process for destroying data in the regular course of business.
- Identify who is responsible for safeguarding the stored data in a secure and easily accessible format.

Create a "Litigation Hold" Policy. When a current or former employee signals an intent to sue, the employer has a duty to preserve documents. Now, that duty unquestionably extends to electronic data. As a result, employers should set forth a procedure to ensure they retain all data. As relevant here, the policy should:

- Ensure a "Litigation Hold" is put on all electronic data that may be potentially relevant to the lawsuit. The hold should secure these documents and effectively stop any routine destruction of electronic data and should apply to all computers, including home computers used for telecommuting.
- Identify designated people to ensure the "Litigation Hold" is in place and all employees understand the importance of securing all potentially relevant electronic.
- Identify designated people to also interview key players and witnesses about the relevant data and its whereabouts.
- Create a process for the designated people to collect all of the data and secure it in a location where it can be retained in an electronic format.
- Ensure that all employees understand the "Litigation Hold" policy is in place until the lawsuit is completely over.

*This Employment Law Note is written to inform our clients and friends of developments in labor and employment relations law. It is not intended nor should it be used as a substitute for specific legal advice or opinions since legal counsel may be given only in response to inquiries regarding particular factual situations. For more information on this subject, please call Sebris Busto James at (425) 454-4233.