A Timely Analysis of Legal Developments

ASAP®

March 18, 2013

EEOC Sanctioned for Failing to Produce Class Claimants' Social Media ESI and Other e-Discovery Misconduct

By Angelo Spinola, Danielle Kitson, Paul Weiner, and Katherine Hinde

In *EEOC v. The Original HoneyBaked Ham Company of Georgia Inc.*, 2013 U.S. Dist. LEXIS 26887 (D. Colo. Feb. 27, 2013), the U.S. District Court for the District of Colorado sanctioned the Equal Employment Opportunity Commission (EEOC) for failing to provide social media discovery and for causing unnecessary delays in the e-Discovery process.

The case involves claims filed by the EEOC against the defendant, HoneyBaked Ham, alleging a manager sexually harassed a class of women. The company sought, among other things, social media evidence and text messages to dispute the claimants' liability and damages claims. In November 2012, the court ordered all claimants to turn over to a special master social media communications and any cell phone used to send or receive text messages during the relevant time period for a forensic collection and review. The court further ordered claimants to provide access to any email account, website, or cloud-based storage location that they used to post communications or pictures.

After the EEOC changed its position about how the court's discovery order was to be implemented, and otherwise failed to follow the e-Discovery process, the company filed a motion for sanctions. On February 28, 2013, the court granted the motion and held that the EEOC's shifting behavior in implementing the court-ordered discovery process—while shy of bad faith—improperly delayed the proceedings and unfairly forced the company to spend more money in litigation. The court crafted a unique sanction against the EEOC under Federal Rule of Civil Procedure (FRCP) 16(f) to curb further misconduct.

The court's decision is the first published decision of its kind to impose sanctions for e-Discovery misconduct under FRCP 16, as opposed to the more traditional methods of awarding sanctions under FRCP 37 or the court's inherent authority to impose discovery sanctions. Significantly, a sanction under FRCP 16 does not require a finding of bad faith. Rather, a party need only engage in some kind of unreasonable or obstreperous conduct that delays the discovery process, as the court held the EEOC did in this case.

The court's decision is also a powerful reminder that, just like defendants, plaintiffs have e-Discovery obligations, thus providing employers with strong offensive discovery tools they can use in defending against both single-plaintiff and class action claims alike. Moreover, the decision underscores that in today's digital world, where individuals who are plaintiffs in litigation create and control a wealth of electronic data—personal computers, PDAs, personal email accounts,

social networking sites and blogs, including professional networking sites like LinkedIn—the refrain of yesteryear that individuals do not possess any relevant electronically stored information ("ESI") in traditional "asymmetrical" employment cases rings hollow.

Factual Background

The EEOC brought this sexual harassment class action lawsuit against The Original HoneyBaked Ham Company of Georgia, Inc. in September 2011, alleging that a male store manager harassed subordinate female employees. A group of allegedly aggrieved individuals ("claimant class members") asserted that as a result of sexual harassment and retaliation inflicted by their manager they suffered severe emotional and financial damages.

During the discovery process, it became apparent that the claimant class members had used text messages, email, and social media to discuss the case and their claims and to communicate amongst themselves regarding the lawsuit. Further, several class members posted pictures and comments directly related to the allegations in the case, such as statements about how stress-free their lives were or the bar they had frequented the night before. As a result, the company served discovery requests that asked the claimant class members to identify and produce relevant data from cell phones, email addresses/accounts, Facebook pages, blog posts, and similar sources that they used during the relevant time period. The EEOC opposed production and ultimately produced very little of the information requested. Through its own investigative efforts, the company discovered highly relevant information on the claimant class members' Facebook pages and filed a motion to compel, requesting an order compelling the production of the requested ESI.

The Order on the Motion to Compel—A Virtual "Everything About Me" Folder

In November 2012, a federal magistrate judge issued an order largely granting the company's motion to compel. While acknowledging that the discovery requests could constitute a significant intrusion into claimant class members' semi-private lives, the court found that the intrusion was justifiable, citing several reasons, including the fact that the claimant class members themselves had put such matters at issue by choosing to participate in the lawsuit.

The court further instructed why broad discovery of social media ESI was appropriate, explaining that the creation of social media content is akin to a litigant affirmatively assembling:

> . . . a file folder titled "Everything About Me," which [the claimant class members] have voluntarily shared with others. If there are documents in this folder that contain information that is relevant or may lead to the discovery of admissible evidence relating to [the] lawsuit, the presumption is that it should be produced. The fact that it exists in cyberspace on an electronic device is a logistical and, perhaps, financial problem, but not a circumstance that removes the information from accessibility by a party opponent in litigation.[1]

Squarely addressing the privacy objection posed in opposition to production, the court rejected it and reinforced its assessment that, rather than commanding greater protection against discoverability *per se*, social media information may actually be more readily discoverable, instructing:

> If all of this information was contained on pages filed in the "Everything About Me" folder, it would need to be produced. Should the outcome be different because it is on one's Facebook account? ***There is a strong argument that storing such information on Facebook and making it accessible to others presents an even stronger case for production, at least as it concerns any privacy objection.*** It was the claimants (or at least some of them) who, by their own volition, created relevant communications and shared them with others.[2]

Accordingly, the court held there was "no question the Defendant has established that the documents it seeks contain discoverable information" and ordered the EEOC to produce the following ESI for each of the claimant class members:

- Any cell phone used to send or receive text messages from January 1, 2009 to the then-present time;

1 *EEOC v. The Original HoneyBaked Ham Co. of Ga., Inc.*, 2012 U.S. Dist. LEXIS 160285, at **3-4 (D. Colo. Nov. 7, 2012).

2 *Id.* at **5-6 (emphasis supplied).

- All necessary information to access any social media websites used by a claimant class member during said period ; and
- All necessary information to access any email account or blog or similar/related electronically accessed internet or remote location used for communicating with others or posting communications or pictures during said period.

To accomplish this production, the court ordered the parties to engage a forensic expert as a special master to whom the EEOC would produce the information, followed by an *in camera* review by the court, to ensure the production of only discoverable information.

The court further ordered the parties to collaborate to produce: (1) a questionnaire to be given to the claimant class members with the intent of identifying all such potential sources of discoverable information; and (2) instructions to be given to the special master defining the parameters of the information he would collect.

Order on Defendant's Motion for Sanctions

After the court entered its order, the EEOC generally refused to produce the court-ordered social media ESI. For example, the EEOC initially requested that the court grant it permission to use its own internal technology personnel, in place of the court-ordered special master, to save on costs. The court granted the EEOC's request, with the specific requirement that the technology personnel's process be transparent to the company. The parties then began extensive negotiations regarding both the protocol to be used for data collection and the questionnaire to be given to the claimant class members.

After a month of negotiations, including the exchange of multiple draft questionnaires and data protocols, conference calls, and court hearings, the EEOC reversed its position on various issues. Lodging privacy and privilege objections, the EEOC objected to allowing the company's attorneys to observe a test run of the EEOC's internal data processes and requested that the court return to its original order to appoint a special master. Additionally, the EEOC withdrew specific commitments that it had made regarding the language of the questionnaire, even reversing positions on language that the EEOC itself had proposed.

As a result of this conduct, the employer filed a motion for sanctions. While the court did not grant the full extent of sanctions the company requested, it found that the EEOC's reversals increased the company's legal costs and unnecessarily delayed the proceedings.

However, the court found that the EEOC's behavior did not rise to the level of "bad faith," as required for sanctions under FRCP 11 or the court's inherent authority. The court further found that the EEOC's conduct did not fit squarely into FRCP 37(d) or (f), and while it was a close question under FRCP 37(b), the court was not prepared to find that the EEOC disobeyed "the letter" of a particular order (although it noted that the EEOC had not been faithful "in spirit").

The court held that a sanction under FRCP 16(f)(1) was appropriate and necessary under the circumstances, citing a case from the U.S. Court of Appeals for the Tenth Circuit. The court noted that FRCP 16 gave the court the power to impose sanctions for actions that negatively affected the court's management of its docket and caused unnecessary burdens on the opposing party, instructing:

> I do not believe it is the proper application of justice to stand idly by while the Plaintiff's flip-flopping harms the Defendant in a tangible way that is violative of the spirit of the Federal Rules of Civil Procedure.[3]

Accordingly, the court sanctioned the EEOC under FRCP 16(f)(1) for causing an unnecessary cost burden on the company and for delaying the case, and awarded reasonable attorneys' fees and costs expended by the company in bringing the motion.

Takeaways: Continuing the Trend of Holding Plaintiffs to Their 21st Century e-Discovery Obligations

Even in single plaintiff cases, plaintiffs have baseline duties and responsibilities with respect to e-Discovery and can face serious consequences for failing to fulfill them.[4]

3 *Id.* at **11-12.

4 *See generally* Paul Weiner, *Plaintiffs Have Their Own Duty to Preserve*, Nat'l L.J., Dec. 20, 2011 (baseline e-Discovery duties and obligations apply just as forcefully to individuals that are plaintiffs in litigation—who often anticipate litigation well in advance of any defendant and there are a multitude of sources of data that modern-day plaintiffs possess and control).

The court's order here continues this trend and further demonstrates the benefit of aggressively seeking e-Discovery of plaintiffs in 21st century litigation as long as the defendant abides by the same standards. Among other things, the court's order on the motion to compel follows the trend of other courts across the country that have held that, in addition to basic sources like home computers and personal e-mail, data from social media accounts,[5] instant messages,[6] and text messages generally must be produced by plaintiffs in litigation.[7] The court's orders further underscore that, in response to discovery requests seeking such ESI from plaintiffs, privacy objections are not well founded.[8]

Finally, the court's reliance on FRCP 16 to impose e-Discovery sanctions against the EEOC highlights a different approach to obtaining sanctions against plaintiffs for e-Discovery delays and misconduct. This application of FRCP 16(f) breathes new life into the Tenth Circuit's 1984 holding in *Mulvaney v. Rivair Flying Services, Inc.*, 744 F.2d 1438 (10th Cir. 1984), where the appellate court instructed that courts have "broad discretion" to use sanctions to ensure that lawyers and parties meet their obligations towards "the expeditious and sound management of the preparation of cases for trial."

As applied in this case, FRCP 16(f) is a powerful tool in an employer's arsenal to invoke against plaintiffs, including the EEOC, who may unnecessarily slow down, obstruct, or otherwise impede the e-Discovery process while not actually engaging in conduct that rises to the level of "bad faith" as required for sanctions under other rules. As the Tenth Circuit instructed in *Mulvaney*, the application of FRCP 16(f) is appropriate even if the discovery misconduct does not rise to the level of bad faith because the court was "dealing with the matter most critical to the court itself: management of its docket and avoidance of unnecessary burdens on the tax-supported courts, opposing parties or both. The primary purpose of sanctions in this context is to insure reasonable management requirements for case preparation."[9]

It is also important to underscore that employers should ensure their own house is in order from an e-Discovery standpoint before aggressively pressing plaintiffs about potential discovery abuses. From a strategic standpoint and to avoid these types of issues arising for both parties, employers should attempt to proactively negotiate a reasonable and efficient e-Discovery protocol – one that addresses e-Discovery issues for both parties – with opposing counsel as early in a case as possible.[10] However, in cases where plaintiffs refuse to then follow the agreed-upon or court-ordered protocol, employers may have no option but to approach the court for appropriate relief.

Angelo Spinola is a Shareholder in Littler Mendelson's Atlanta office, Danielle Kitson is a Shareholder in the Denver office, Paul Weiner, the firm's National eDiscovery Counsel, is a Shareholder in the Philadelphia office, and Katherine Hinde is an Associate in the Denver office. If you would like further information, please contact your Littler attorney at 1.888.Littler or info@littler.com, Mr. Spinola at aspinola@littler.com, Ms. Kitson at dkitson@littler.com, Mr. Weiner at pweiner@littler.com, or Ms. Hinde at khinde@littler.com.

5 *See, e.g., McMillen v. Hummingbird Speedway, Inc.*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *3 (Jefferson County Sept. 9, 2010) (ordering plaintiff to provide his Facebook and MySpace user names and passwords to counsel for defendants; rejecting plaintiff's argument that communications shared among one's "private" friends are somehow protected against disclosure in discovery and instructing "'no social network site privilege' has been adopted by our legislature or appellate courts").

6 *See, e.g., In re: Air Crash Near Clarence Center NY*, 2011 U.S. Dist. Lexis 146551 (W.D.N.Y. Dec. 20, 2011) (directing plaintiffs to produce relevant electronic communications, including social media accounts, emails, text messages, and instant messages).

7 *See, e.g., Smith v. Café Asia*, 246 F.R.D. 19 (D.D.C. 2007) (court ordered plaintiff to preserve text messages stored on cell phone as they might bear on defendant's claim that plaintiff invited the alleged sexual harassment forming the basis for her claims).

8 *See, e.g.*, Niloy Ray, Aaron Crews, and Paul Weiner, *A Litigator's Guide to Discovery of Social Media ESI in Civil Actions*, The Legal Intelligencer, Jan. 29, 2013 ("Indeed, the very idea that social media ESI is somehow 'private' in the first instance is dubious."); *EEOC v. Simply Storage Management, LLC*, 270 F.R.D. 430, 434 (S.D. Ind. 2010) ("A person's expectation and intent that her [social media] communications be maintained as private is not a legitimate basis for shielding those communications from discovery."); *Beye v. Horizon Blue Cross Blue Shield of New Jersey*, 2007 U.S. Dist. LEXIS 100915, at **11-12, 13 (D.N.J. Dec. 14, 2007) (rejecting plaintiffs' privacy arguments and ordering minor-plaintiffs in class action case to preserve and produce "writings shared with others including entries on websites such as 'Facebook' or 'Myspace,'" because they may be relevant to the core issue of whether eating disorders are non-biologically-based mental illnesses: "While the plaintiffs suggest that allowing the Order to stand may require the plaintiffs to have to choose between pursuing this litigation or disclosing private information about their child, that decision was made when the plaintiffs decided to file an action which required them to disclose information concerning their children's eating disorders, something they have described as an extremely sensitive topic.").

9 *Mulvaney*, 744 F.2d at 1441.

10 *See, e.g.*, The Sedona Conference®, *The Sedona Conference Cooperation Proclamation* 1 (2008) (cooperation in discovery is required by the rules of civil procedure, consistent with zealously representing a client, and in today's digital world a hallmark of effective advocacy), *available at* www.thesedonaconference.org. Over 225 state and federal judges across the country have publically endorsed the Sedona Conference Cooperation Proclamation.