New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 252—NO. 43
TUESDAY, SEPTEMBER 2, 2014

STATE E-DISCOVERY

Decisions Address Relevance, Scope, Email and Privacy Issues

By **Mark A. Berman**

BIGSTOCK

State courts are savvy to issues concerning the discovery of electronically stored information (ESI), and recent trial decisions offer practical and pragmatic rulings on ESI. Although rarely stated, a reality known to—and often grudgingly admitted by—every litigator was articulated by the court in *MBIA Ins. v. Credit Suisse Sec. (USA)*,[1] where it observed that a party "cannot reasonably expect to uncover every single instance" relating to a specific event. No doubt with that understanding in mind, courts are addressing parties' concerns as to burdensome and overbroad requests seeking the production of ESI that is not predicated on the specific allegations of a party's claim. The failure to implement appropriate litigation holds is not being tolerated, with courts finding that they should have been implemented, but then trying to balance such failure with true prejudice to the complaining party in order to determine the degree of the spoliation sanction. Email discovery and the use of emails are now standard litigation practice, and recent decisions are making clear that emails should be produced in a searchable format and that non-parties should not be absorbing the cost of burdensome ESI discovery. Use of emails also should not be taken for granted as a ground upon which to move to dismiss, as a matter of law, based on "documentary" evidence under CPLR Rule 3211(a)(1).

Finally, as privacy concerns over electronic communications are driving ESI litigation, the recent trial court decision in *New York Eye Surgery Assoc. v. Kim*,[2] makes clear that it is difficult to

MARK A. BERMAN, *a partner at commercial litigation firm Ganfer & Shore, cochairs the social media committee of the Commercial and Federal Litigation Section of the New York State Bar Association.*

dismiss, as a matter of law, a well-pleaded claim under the federal Computer Fraud and Abuse Act and the Stored Communications Act, where there are competing claims as to whether the employer was "authorized" to "access" an employee's ESI.

Relevance and Scope

In denying a motion to compel in a complex financial securities action, the court in *MBIA*,[3] stated what all counsel know to be the realities of ESI discovery—that a party in complex litigation "cannot reasonably expect to uncover every single instance" in which an employee says something about a particular subject. The motion court noted that

> the very reason that [plaintiff] knows that so much inflammatory ESI exists is precisely because it has so much already. To be sure, in reviewing [defendant's] itemized justifications as to what constitutes relevant ESI, it appears that [defendant] may well have been somewhat overaggressive in determining the scope of relevance.

The motion court noted that the examples of ESI proffered by plaintiff

> do not give rise to a reasonable inference that [defendant's] determinations as to what constitute responsive ESI were made in bad faith. Nor has [plaintiff] convinced the court that [defendant] is hiding something materially worse than has already been produced that might tip the scales of this case in [plaintiff's] favor. Indeed, while non-transaction specific inflammatory emails do not speak well of [defendant], [defendant's] conduct with respect to the subject transaction is all that is at issue. This case is more likely to (and should) turn on the law (e.g., due diligence issues) and expert evidence (e.g., the nonconformance rate) rather than how many inflammatory emails [plaintiff] can read to a jury.

'New York Eye' makes clear that it is difficult to dismiss a well-pleaded claim under the federal Computer Fraud and Abuse Act and the Stored Communications Act, where there are competing claims as to whether the employer was "authorized" to "access" an employee's ESI.

In *Sipperley v. Diaz*,[4] the motion court held that the term "relevant" does not mean a "wholesale intrusion into the personal aspects of defendant's life, with no restriction as to the issues raised in the pleadings, and no indication that the material will contain, or lead to the discovery of admissible evidence" to justify seeking "all relevant electronically stored emails, from personal and business computers, cellular telephones and personal digital assistants." The court did, however, direct defendant not to "destroy or erase any communications which may relate to the issues raised in the complaint, pending termination of the litigation."

LinkedIn Production

Del Gallo v. City of New York,[5] in a wrongful death action, defendants sought the contents of plaintiff's "entire LinkedIn account" on the grounds that plaintiff testified at her deposition concerning "responses to former colleagues inquiries regarding her post accident condition and communication between [her] and employment recruiters are material to her damages claims." Defendants claim they are entitled to discovery of plaintiff's LinkedIn account to "learn about plaintiff's online description of her employment abilities, any employment offers she may have received, her acceptance of any offers, and so forth … [which] may help determine the amount of damages." The motion court granted disclosure concerning communications with recruiters, which plaintiff had agreed to produce. However, it denied discovery of plaintiff's communications with her former colleagues about her condition and held that "self-assessments"

that did not contradict or conflict with her claims and that "hoping" that same would be relevant to plaintiff's loss of enjoyment of life do not justify the production of anything else from plaintiff's LinkedIn account or for access to plaintiff's "Luminosity" account, an online brain game site.

Litigation Hold Required

In *Signature Med. Mgmt. Group v. Levy*,[6] a legal malpractice action, plaintiff asserted that defendant law firm failed in an arbitration to properly produce source data relied upon by its expert, which resulted in the exclusion of a certain exhibit, an expert report and expert testimony from the arbitration. Plaintiff claimed that the arbitration would have settled on a more favorable basis if such source data had been produced. Plaintiff moved to strike defendant's answer on the basis that emails concerning the source data sent to and by the individual attorney who represented it in the arbitration had been deleted by defendant law firm's outside computer consultant after the attorney had left the firm. Because plaintiff had not established that the emails could not be reconstructed as plaintiff may possess them, or may have the ability to recover them, the court denied plaintiff's motion to strike with leave to seek an appropriate sanction at trial. The court held that a lesser sanction may be appropriate upon a showing that defendants were responsible for the destruction of the emails and that plaintiff had been prejudiced. On renewal and reargument of the motion, plaintiff argued that the deletion may have been due to the actions of the law firm's administrator as opposed to its outside computer consultant. Nevertheless, the court denied such motion.

Because there was a triable issue of fact as to whether the emails were destroyed with a culpable state of mind, the court again denied plaintiff's motion for spoliation sanctions with leave to renew at trial.

Thereafter, on plaintiff's cross-motion for summary judgment or, in the alternative, for an adverse inference based on the spoliation of evidence, the motion court found that once the malpractice action had commenced,[7] the law firm "was under an obligation to place a litigation hold on its computer system to preserve [it's former attorney's] emails." Noting that *Voom HD v. Echostar Satellite*,[8] held that, in certain circumstances, it is insufficient in implementing a litigation hold to "vest total discretion" in an employee to search and select what ESI is relevant "without the guidance and supervision of counsel," the motion court found that the firm administrator required such guidance and supervision of counsel and that the defendant law firm had a duty at the time the emails were deleted from its computer system to have preserved them. However, because there was a triable issue of fact as to whether the emails were destroyed with a culpable state of mind where the firm's administrator's instructions to its outside computer consultant could be interpreted as directing that the emails be disabled as opposed to being destroyed, the court again denied plaintiff's motion for spoliation sanctions with leave to renew at trial.

Guidelines on Key Email Issues

- *Locks v. PRC Indus.*,[9] ("To the extent that the emails contained in the CD ROM provided in response to document request numbered 32 are not in their 'native, and in a searchable and sortable format,' or without all attachments thereto, they are to be properly produced.").
- *MBIA Ins. v. Credit Suisse Secs (USA)*[10] (plaintiff, as the requesting party, shall pay non-party for the "reasonable cost" of production of emails).
- *Oberman v. Textile Mgt. Global*[11] (an email is not "documentary evidence" upon which a motion to dismiss predicated upon Rule CPLR 3211(a)(1) may be made).

Computer Fraud and Abuse Act

In *New York Eye*,[12] employer commenced an action alleging violation of a non-competition and non-solicitation agreement, and employee physician counterclaimed alleging, among other things, violation of 18 U.S.C. §1030, the Computer Fraud and Abuse Act (CFAA); and 18 U.S.C. §2701, the Stored Communications Act (SCA). A private cause of action under the CFAA exists against anyone who, among other things, "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer." The physician alleged that unauthorized activity resulted in the modification, or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment or care of one or more individuals, "as access to the data allowed the Counterclaim Defendants to contact [the physician's] patients and interfere with their treatment by [the physician]." The motion court denied the motion to dismiss, finding that "Counterclaim Defendants' argument that they lawfully had access to [the physician's] computer records, files, and activities" is a factual issue, that is "more appropriately raised on summary judgment or trial." The physician also alleged that his telephone conversations were recorded and his emails and personal files on his office computer were accessed without his knowledge or consent, despite the fact that his "computer could only be accessed by logging in with a password that was unique to [him]." The physician also asserted that Counterclaim Defendants "intentionally, without authorization, accessed emails stored on an electronic communication service provider's system after they had been delivered, and thereby obtained access to the electronic communications while they were in electronic storage." Denying the motion to dismiss the physician's SCA claim, the motion court noted that courts "have held that allegations that an employer exceeded its authorized scope and accessed an employee's email are sufficient to survive a motion to dismiss."

1. 2014 N.Y. Misc. LEXIS 3192, 2014 NY Slip Op 31871(U) (Sup. Ct. N.Y. Co. July 17, 2014).
2. 2014 N.Y. Misc. LEXIS 3081, 2014 NY Slip Op 31808(U) (Sup. Ct. N.Y. Co. July 9, 2014).
3. 2014 N.Y. Misc. LEXIS 3192, 2014 NY Slip Op 31871(U).
4. Index No. 013885/2013 (Sup. Ct. Nassau Co. Aug. 15, 2014).
5. Index No. 107409/2011 (Sup. Ct. N.Y. Co. June 23, 2014).
6. Index No. 11724/2009 (Sup. Ct. Nassau Co. June 9, 2014).
7. See *Rodman v. Gold*, Index No. 15583/2010 (Sup. Ct. Suffolk Co. July 14, 2014) (plaintiff had an obligation, given his knowledge and access to the video-tape immediately after the accident, to preserve it once it became apparent that his injuries were severe enough to commence a personal injury action).
8. 93 A.D.2d 33, 42, 939 N.Y.S.2d 321, 328 (1st Dep't 2012).
9. 2014 N.Y. Misc. LEXIS 3308, 2014 NY Slip Op 31933(U) (Sup. Ct. Suffolk Co. July 9, 2014).
10. 2014 N.Y. Misc. LEXIS 3450, 2014 NY Slip Op 32025(U) (Sup. Ct. N.Y. Co. July 31, 2014).
11. 2014 N.Y. Misc. LEXIS 3173, 2014 NY Slip Op 31863(U) (Sup. Ct. N.Y. Co. July 11, 2014).
12. 2014 N.Y. Misc. LEXIS 3081, 2014 NY Slip Op 31808(U).

GANFER & SHORE, LLP
ATTORNEYS AT LAW

360 Lexington Avenue
New York, New York 10017
212.922.9250
mberman@ganfershore.com