New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 252—NO. 87
TUESDAY, NOVEMBER 4, 2014

STATE E-DISCOVERY

iPhones, Twitter, Deleted Emails And ESI Under CPLR 3211(A)(1)

By **Mark A. Berman**

NYLJ

A commercial division decision in *Advanstar Comm. v. Pollard*,[1] recently answered in the negative the question of whether an employer's remote "wiping" of an employee's personal iPhone violated the Stored Communications Act, 18 U.S.C. §2701(a). Discovery of social media includes non-private tweets and Twitter subscriber information, and two recent motion court decisions in *Juice v. Twitter*[2] and in *Kerner v. Lopiccolo*[3] ordered the production of tweets, finding that the proper predicate for their relevance had been established. It is no surprise that courts are questioning affidavits attesting to the purported unavailability of relevant emails and, in *Alberta v. Fossil Indus.*[4] after reviewing an expert computer forensic affidavit, the court directed that emails be produced in the format agreed to and that full and complete responses to the discovery demands be provided or defendant's answer would be stricken. Finally, recent First Department decisions address whether emails are proper "documentary evidence" under CPLR 3211(a)(1), and concluded that such a determination is fact-dependent.

Remote 'Wiping' of iPhones

In *Advanstar*,[5] an employee gave notice to his employer that he was resigning and that he would be going to work for a competitor. The employer that day then remotely "wiped" the entire contents of the employee's *personal* iPhone from which the employee had been able to send and receive emails from his employer's email account and communicate with business contacts. As a result, the employee claimed that he "lost his personal and business contacts, personal and business notes,

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.*

text messages, instant-messaging messages, voicemails, several hundred photographs of his family and friends, personal journals, videos, and music." The employee moved for partial summary judgment on counterclaims alleging trespass to chattel, violation of the Stored Communications Act (SCA) and conversion predicated upon the loss of his personal information and data from his *personal* iPhone. The motion court ruled that "[b]ased on the lack of any inspection of [defendant's] iPhone or any meaningful account of what exactly [the employee] lost when his iPhone was allegedly remotely wiped clean, a factual issue exists as to what information, if any, [the employee] lost."

Summary judgment was granted in favor of the employer on the Stored Communication Act claim, as the motion court found that cell phones are not a "facility through which an electronic communication service is provided." The motion court also held that data, including emails, text messages and pictures stored on a hard drive or cell phone, does not fall within the definition of "in electronic storage" as required under the SCA. The motion court specifically noted that the employee did not allege that the employer "accessed the information or data on his iPhone that he had not yet read or received. Rather, [the employee] is claiming that the [employer] conducted a remote sweep of his cell phone, thus wiping out information and data he had stored on his phone."

Twitter Discovery

In *Juice*,[6] the motion court, in a proceeding seeking pre-action disclosure, directed Twitter to disclose basic subscriber information and Internet protocol addresses sufficient to identify the individual(s) who owned or operated a certain Twitter account and who logged into or tweeted from that account during a specified period and to preserve documents containing the information sought to be disclosed. Petitioner, Lemon Juice, contended that he needed such disclosure in order to name defendants in an action alleging prima facie tort, intentional infliction of emotional distress, fraud and malicious prosecution. Twitter objected to providing pre-action disclosure in the absence of a court order finding that Lemon Juice is entitled to such information.

Recent First Department decisions address whether emails are proper "documentary evidence" under CPLR 3211(a)(1), and concluded that such a determination is fact-dependent.

The motion court found that in calling the account "LemonJuice@moseh718," the creator of the account gave the public the false impression that Lemon Juice was its owner and operator and had "obtained a digital image of the infant victim while she was testifying against her rapist in direct violation of a court order not to take such photographs and posted such image to the subject account for the "entire world to see." The motion court found that the "creator's conduct was especially heinous because it created the false appearance that Lemon Juice openly disregarded the privacy of an infant sex crime victim" and it created the "false impression that Lemon Juice was attempting to expose, humiliate and intimidate the infant victim while she was in the process of testifying against her tormentor." The motion court held that it "is a reasonable inference from these facts that the creator was seeking to humiliate Lemon Juice, tarnish his reputation and expose him to criminal prosecution by framing him." As such, the motion court held that "Lemon Juice had met his burden of demonstrating that he has a meritorious cause of action for intentional infliction of emotional distress" and therefore was entitled to discovery from Twitter to determine who should be named as a defendant. Finally, the motion court held that "[t]hose who suffer damages as a result of tortious or other actionable communications on the Internet should be able to seek appropriate redress by preventing the wrongdoers from hiding behind an illusory shield of purported First Amendment rights."

In *Kerner*,[7] discovery of private Twitter and Facebook messages was permitted in a breach of contact action where a review of plaintiff's public Twitter and Facebook messages revealed comments about the

incident that formed the predicate for her breach of contract claim, including that plaintiff had posted comments about attending another event on the date of the incident while claiming that she was confined to bed for two days following the incident. The motion court found that the evidence submitted made it "reasonable to believe that the private portions of [plaintiff's] pages may contain further evidence relevant to [d]efendant's defense and prosecution of the counterclaims." The court ordered plaintiff to provide access to her private social media messages from the date of the incident to the present as well as cell phone records for the date of the incident.

Metadata Must Be Produced

In *Alberta*,[8] plaintiff sought the disclosure of specific warranties that accompanied each purchase order and, since the "transactions were accomplished through emails, plaintiff demanded, and the court directed, that these emails be provided in their native electronic format, together with their associated metadata, which the defendant failed to furnish." Defendant's president claimed that it used a specific software that "bundles" emails into a "contacts" file upon sending, and then transfers the emails from a particular contact into a "note field," and that this is the "native format" of the communications and that "metadata is not preserved in this format." To oppose plaintiff's position, defendant utilized a computer forensic expert to contradict the underlying premises to plaintiff's position, who indicated in pertinent part:

- how the user utilizing this software saves an email, attachment or file to a "contacts" file is largely a matter of choice of the user or its IT department;
- defendant's software is not an email system and a user cannot generate or send or receive an email using such software and the software is being used as a storage and archiving tool;

In 'Kerner', discovery of private Twitter and Facebook messages was permitted where a review of plaintiff's public Twitter and Facebook messages revealed comments about the incident that formed the predicate for her breach of contract claim.

- the metadata for the underlying emails and attachments sought by plaintiff was necessarily once contained in some email system that defendant used when it sent and received emails;
- defendant failed to disclose what email system it had been using or what happened to the original emails and files it subsequently stored; and
- defendant did not indicate whether it was using an archiving system in which to store files or whether they were stored on a desktop, server or backup system and the expert opined that, if defendant possessed such underlying files, it would have been incumbent upon it to produce or at least disclose them in response to a request for authenticating metadata. The expert also noted that, if defendant no longer possessed such underlying files, it would not be in a position to offer its files with any authenticating information about dates.

The motion court found defendant's responses "inadequate under the circumstances" and that "such inadequacy warrant[ed] the drawing of an inference of willful conduct on the part of the defendant which frustrated the schedule of discovery agreed to by counsel and fixed in an order of the court." Accordingly, the motion court ordered that "the answer served by the defendant shall be dismissed unless it furnishes the emails in the format agreed to and full and complete responses to the discovery demands of the plaintiff."

Lack of Hold Didn't Merit Sanctions

In *L&L Painting v. Odyssey Contr.*,[9] sanctions were sought based on the failure to preserve emails relating to work on a project during a certain period from the *personal* email accounts of certain management employees, which *personal* email accounts were used for "business purposes" while working on the project. The motion court held that plaintiff's duty to preserve the emails arose, at the latest, when it commenced the lawsuit, and a litigation hold should have been implemented on or before that date and perhaps earlier, when, by its own

acknowledgment, litigation had been anticipated. Plaintiff did not dispute that no litigation hold had been implemented and did "not explain what, if any, steps it otherwise took or was advised to take to preserve potentially relevant electronically stored documents." Plaintiff was not able to recover the subject emails because they had been transmitted through personal email accounts not connected to plaintiff's main office computer network and had been deleted by an automatic delete feature.

The motion court, as in *Chin v. Port Auth. of N.Y. & N.J.*, 685 F.3d 135 (2d Cir. 2012), rejected

> the notion that a failure to institute a "litigation hold" constitutes gross negligence per se, "'the better approach is to consider [the failure to adopt good preservation practices] as one factor' in the determination of whether discovery sanctions should issue." 685 F.3d at 162 (citation omitted). Moreover, even a finding of gross negligence does not, in all cases, obviate the need to demonstrate the relevance of the evidence sought.

The motion court held that while plaintiff was "negligent in failing to institute a litigation hold or otherwise act in a timely manner to preserve the emails in question, the facts do not support a finding of bad faith or gross negligence against" plaintiff. In addition, defendant had not "made an adequate showing of the relevance of the missing emails to its remaining counterclaims or how they would support its defenses; its reliance on the presumption of relevance is insufficient to establish a right to sanctions."

Emails as 'Documentary Evidence'

This column previously reported on a case addressing whether emails are appropriate "documentary evidence" upon which a motion to dismiss under CPLR Rule 3211(a)(1) may be predicated,[10] and three recent cases also have now addressed this issue. See *Amsterdam Hospitality Group v. Marshall-Alan Assoc.*[11] ("As Professor Siegel recognizes, 'even correspondence' may, under appropriate circumstances, qualify as documentary evidence. In our electronic age, emails can qualify as documentary evidence if they meet the 'essentially undeniable' test"); *Art & Fashion Group Corp. v. Cyclops Prod.*[12] ("Email correspondence can, in a proper case, suffice as documentary evidence for purposes of CPLR 3211(a)(1)," but "the emails, when read in their entirety, do not conclusively refute plaintiffs' allegations."); *Baron v. Suissa*[13] ("Generally, printed materials such as letters and emails are not considered 'undeniable' or out-of-court transactions which are equivalent to documentary evidence").

1. 2014 N.Y. Misc. LEXIS 4104 (Sup. Ct. N.Y. Co. Sept. 19, 2014).
2. 44 Misc. 3d 1225(A) (Sup. Ct. Kings Co. Aug. 29, 2014).
3. Index No. 12008-13 (Sup. Ct. Nassau Co. Sept. 17, 2014).
4. 2014 N.Y. Misc. LEXIS 4110 (Sup. Ct. Suffolk Co. Sept. 8, 2014).
5. 2014 N.Y. Misc. LEXIS 4104.
6. 44 Misc. 3d 1225(A).
7. Index No. 12008-13.
8. 2014 N.Y. Misc. LEXIS 4110.
9. 2014 N.Y. Misc. LEXIS 4300 (Sup. Ct. N.Y. Co. Sept. 25, 2014).
10. See Mark A. Berman, "Decisions Address Relevance, Scope, Email and Privacy Issues," N.Y.L.J. Sept. 2, 2014.
11. 120 A.D.3d 431, 433, 992 N.Y.S.2d 2, 4 (1st Dep't Aug. 28, 2014).
12. 120 A.D.3d 436, 438, 992 N.Y.S.2d 7, 10 (1st Dep't Aug. 28, 2014).
13. 44 Misc. 3d 1229(A), 2014 N.Y. Misc. LEXIS 4039, at *6-7 (Sup. Ct. Suffolk Co. Sept. 4, 2014).

GANFER & SHORE, LLP
ATTORNEYS AT LAW

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