New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 253—NO. 40
TUESDAY, MARCH 3, 2015

STATE E-DISCOVERY

Cases Address Use of ESI And Ethics Issues With the Cloud

By **Mark A. Berman**

Courts are "tooling down" and becoming circumspect on how electronically stored information (ESI) is used in discovery and motion practice. The recent decisions discussed below address the production of metadata, the detail required in an ESI privilege log, the use of emails on a motion to dismiss, and the implication of changing a person's ESI password. In addition, in *LM Bus. Assoc. v. State of New York*,[1] new jurisprudence has been created regarding a conversion cause of action as it relates to computers.

In addition, the New York State Bar Association recently issued Opinions 1019 and 1020 concerning ESI and opined that where "reasonable" precautions are used to safeguard confidential client information, lawyers may access such information remotely from their home and may use in transactional work "cloud-based" technology to store such client information.

Production of Metadata Deferred

In *The Garden City Group v. Hughes*,[2] an action involving a covenant not to compete, the parties served competing document requests with plaintiff seeking the production of a variety of electronic communications. Plaintiff sought defendant's communications with clients of plaintiff from both defendant's personal and his new employer's email accounts. Plaintiff's request for the production of metadata concerning such documents was denied, however, with leave to renew until after defendants produced the ordered documents.

Deficient ESI Privilege Log

In *Carpezzi-Leibert Group v. Henn*,[3] an action involving a sales representative's alleged failure to comply with the terms of a non-solicitation agreement, the court agreed to review defendants' document production in camera regarding certain entries that defendants had previously redacted. Defendants' counsel provided the court with copies of the unredacted documents and a redaction log seeking to document the reasons for the redactions. With respect to that log, the court found:

> [Defendants'] privilege log does not provide sufficient detail for the court to determine whether the remaining redactions, particularly with respect to Henn's text messages and iPhone calendar entries, are properly redacted. Accordingly, defendants are directed to provide a more detailed privilege log, identifying the names of the individuals with whom Henn exchanged the redacted text messages in the attached documents, and providing further, non-conclusory, explanation as to whether such individuals, as well as the individuals identified in the redacted iPhone calendar entries, are CLG clients, prospects, employees, or former employees.

BIGSTOCK

In 'W&G Wines,' the court ruled that "the Internet printouts proffered by defendant … are subject to interpretation and their reliability and authenticity have not been sufficiently established.

Website Printout Insufficient

In *W&G Wines v. Golden Chariot Holdings*,[4] defendant moved to dismiss the complaint, pursuant to CPLR Rule 3211(a)(1), based on documentary evidence, and annexed printouts of plaintiff's promotional materials from the Internet as evidence that plaintiff allegedly violated certain liquor laws and its lease. In denying the motion, the court ruled that "the Internet printouts proffered by defendant from plaintiff's Facebook page, Yelp, and other sources, are subject to interpretation and their reliability and authenticity have not been sufficiently established. Defendant's cross-motion cannot be granted on this type of printed evidence."[5]

Restoration of Password

In *Lefcourt v. Samowitz*,[6] the court conducted a preliminary injunction hearing relating to a business dispute concerning partners, where defendant had changed plaintiff's password to certain client information in connection with his starting a competing business. The court enjoined defendant from denying "plaintiffs access to the customer information, email accounts, invoices, telephone numbers and inventory of Expendables Plus and to restore to the plaintiffs full access to customer information, email accounts, invoices, telephone numbers and inventory in which the defendant has an ownership interest or over which the defendant maintains control." The court also directed defendant to "maintain, preserve and share all electronic files of Expendable Plus" under defendant's control.

'Conversion' Rejected

In *LM Bus.*, the State Insurance Fund, the State Police, and the Workers' Compensation Board conducted an investigation into suspected fraudulent activities by a group of affiliated businesses, including claimants, that were owned and operated by nonparty Mark Boerman. As part of that investigation, a warrant was issued to search claimants' offices and to seize relevant evidence. Attached to the warrant application

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.*

was an appendix that set forth certain "general considerations for determining whether any particular computer within the purview of the warrant would be 'remove[d] from the premises' for 'process[ing] by a qualified computer specialist in a laboratory setting,' or whether it would be analyzed on site without the need for removal." Thereafter, Boerman pleaded guilty to offering a false instrument for filing in the first degree in full satisfaction of the indictment. After sentencing, Boerman moved for an order for the return of the seized computers. The motion was granted and the court directed that the computers be returned to Boerman "as soon as practicable." The computers were returned within several months. It is undisputed that the seized computers were "integral to the operation of claimants' businesses." The Court of Claims rendered an interlocutory judgment in claimants' favor on the issue of liability with respect to, among other claims, conversion, with damages to be determined following a trial.

The Appellate Court reversed on the issue of liability for conversion. The court noted:

> A search warrant specifically authorized law enforcement to "search for and seize" six categories of items, including "[a]ll computers and computer storage media and related peripherals, electronic or computer data." Claimants have never challenged the validity of the search warrant. Moreover, the unchallenged warrant placed no time limit on the retention of the items seized, and the authorization to "seize" the computers was not terminated until County Court ordered the property returned following Boerman's guilty plea. We therefore conclude that defendant's exercise of control over the computers did not constitute conversion inasmuch as it had the proper authority to exercise such control.

Remote Access Must Be Secure

New York State Bar Association Committee on Professional Ethics Opinion 1019 (Aug. 6, 2014) answered affirmatively the question that a law firm may "provide its lawyers with remote access to its electronic files, so that they may work from home" provided that precautions taken to safeguard the disclosure of confidential client information are "reasonable."

Opinion 1019 is predicated upon Rule 1.6(a) of the New York State Rules of Professional Conduct which provides that a "lawyer shall not knowingly reveal confidential information." Comment 17 to Rule 1.6 further provides:

> When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. The duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

Opinion 1019 stated that "the key to whether a lawyer may use any particular technology is whether the lawyer has determined that the technology affords reasonable protection against disclosure and that the lawyer has taken reasonable precautions in the use of the technology."

Opinion 1019 stated that "the key to whether a lawyer may use any particular technology is whether the lawyer has determined that the technology affords reasonable protection against disclosure and that the lawyer has taken reasonable precautions in the use of the technology." Opinion 1019 further opined that "reasonable care" to protect a client's confidential information against unauthorized disclosure may include consideration of the following steps:

(1) Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;

(2) Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;

(3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or

(4) Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

In addition, Opinion 1019 noted that "in view of rapid changes in technology and the security of stored data, we suggested that the lawyer should periodically reconfirm that the provider's security measures remained effective in light of advances in technology. We also warned that, if the lawyer learned information suggesting that the security measures used by the online data storage provider were insufficient to adequately protect the confidentiality of client information, or if the lawyer learned of any breaches of confidentiality by the provider, then the lawyer must discontinue use of the service unless the lawyer received assurances that security issues had been sufficiently remediated."

Lawyers' Use of Cloud Storage

Relying on many of the same precepts as in Opinion 1019, the New York State Bar Association Committee on Professional Ethics Opinion 1020 (Sept. 12, 2014) opined that a lawyer "representing a party to a transaction [may] use a cloud-based technology so as to post documents and share them with others involved in the transaction." Noting that in Opinion 842 (2010) it opined that a lawyer may use the "cloud" to store confidential client information provided that the lawyer takes reasonable care to protect it, Opinion 1020 states, with respect to transactional usage concerning "cloud" technology:

> [U]se of electronically stored information may not only require reasonable care to protect that information under Rule 1.6 [to ensure that confidential information is not breached], but may also, under Rule 1.1, require the competence to determine and follow a set of steps that will constitute such reasonable care.

In conclusion, Opinion 1020 noted "[w]hether a lawyer for a party in a transaction may post and share documents using a cloud data storage tool depends on whether the particular technology employed provides reasonable protection to confidential client information." Lastly, Opinion 1020 stated that the "inquirer must, for example, try to ensure that only authorized parties have access to the system on which the information is shared."

1. 124 A.D.3d 1215 (4th Dep't 2015).
2. Index No. 602121/2014 (Sup. Ct. Nassau Co. Jan. 7, 2015).
3. 2015 N.Y. Misc. LEXIS 249, 2015 N.Y. Slip Op 30132(U)(Sup. Ct. N.Y. Co. Jan. 28, 2015).
4. 46 Misc. 3d 1202(A) (Sup. Ct. Kings Co. Dec. 19, 2014).
5. The author's article, "Decisions Address Relevance, Scope, Email and Privacy Issues," NYLJ, Vol. 252 No. 43 (Sept. 2, 2014), also addressed the use of an email as "documentary evidence."
6. Index No. 603365/2014 (Sup. Ct. Nassau Co. Jan. 23, 2015).

GANFER & SHORE, LLP
ATTORNEYS AT LAW

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