Reasonable Accessibility and the Discoverability of ESI

By Gregory M. Boyle, William P. Wallenstein, and J.H. Jennifer Lee

The advent and proliferation of technologies such as mobile Internet cards and web-conferencing tools mean that corporate executives and directors can now perform their duties anywhere, at any time. These developments have altered pretrial litigation in prominent ways, expanding the scope of discovery well beyond the parameters of the workplace. Although the Federal Rules of Civil Procedure were recently amended to include rules governing the discoverability of electronically stored information (ESI), the amended rules provide little guidance to corporate litigants regarding the discoverability of information that is stored outside their offices or networks. Rather, courts have been left to decide the boundaries of corporate litigants' preservation, disclosure, and discovery obligations.

This article discusses whether corporations are obliged to preserve, disclose, and produce relevant ESI that is stored on their executives' and directors' personal hard drives and private email servers. The discussion does not purport to answer specific questions regarding the discoverability of particular ESI; whether ESI is discoverable is, in large part, dependent on the facts and circumstances of each case. Instead, the discussion is intended to provide a starting point for litigators and their clients when considering preservation, disclosure, and discovery obligations in the current climate of ever expanding mobile technologies.

Discussion

In 2007, the Federal Rules of Civil Procedure were amended to include rules designed to manage discovery of ESI. Specifically, Federal Rule of Civil Procedure 26(b)(1)(B) now provides that litigants are entitled to discover any "reasonably accessible" ESI, which is likely to lead to the discovery of admissible evidence. This same rule provides that ESI that cannot be gathered absent undue burden or cost is not "reasonably accessible." But before rushing to the courthouse to argue that ESI is not discoverable because it is stored on the home computer or personal email server of a corporate executive or director, corporate litigants and their attorneys should think again.

Traditional Custody and Control Rules Are Inapplicable

It is unlikely that corporate litigants can avoid producing responsive ESI, even if that information is stored exclusively on one of their executive's or director's home computer or personal email server. Under Federal Rule of Civil Procedure 34(a)(1), upon request, corporate litigants are obliged to produce discoverable information that is within their "custody and control." Traditionally, courts have held that evidence is within a party's "custody and control" if the party has either (a) actual possession of the evidence or (b) the legal right to obtain the evidence upon demand.[1] Similarly, courts typically refuse to hold that evidence is within a corporation's "custody and control" when the evidence is created and stored in a corporate executive's or director's home, meaning such information is not discoverable from the corporation.[2] Recently, however, courts have refused to apply traditional "custody and control" concepts in cases regarding the discoverability of ESI.

A number of courts have held that corporations are obligated to produce ESI created and maintained outside the company's network or stored exclusively on the home computer or personal email server of a corporate executive or director.[3] As one court explained, where an executive uses a computer "for work benefiting [the] corporation[,]" that work is discoverable.[4] In another case, the court went so far as to suggest that corporate litigants may, under certain circumstances, be obligated to turn over ESI even when a third party controls and maintains the information.[5] In *In re Triton*, the court ordered the production of relevant ESI, which was stored on the company's current and former outside directors' personal computers and even admonished the corporation that "it would have been prudent and within the spirit of the law for Triton to instruct its officers and directors to preserve and produce any documents in their [i.e. the directors'] possession, custody, or control."[6] The *Triton* decision suggest that the traditional definition of "custody and control" may not be completely applicable in the electronic age and that corporate litigants may be ordered to produce responsive information that their executives and directors create and maintain outside of the office, notwithstanding substantial privacy and privilege concerns.

Privacy and Privilege Objections Are No Obstacle

In general, corporate litigants have been unable to prevent the production of ESI stored on their executives' and directors' home computers or personal email servers through broad privilege or privacy objections.[7] Rather than recognizing such claims, courts have used innovative solutions to assuage privacy and privilege concerns. Instead of preventing discovery of files created or maintained on the home computers or personal email servers of corporate executives or directors, courts tend to order that a third-party be commissioned to conduct

Gregory M. Boyle is a partner and William P. Wallenstein and J.H. Jennifer Lee are associates with Jenner & Block LLP's office in Chicago, Illinois. Gregory M. Boyle is coeditor of the *PP&D* newsletter.

Published in *Pretrial Practice & Discovery*, Volume 17, Number 2, Winter 2009.

a forensic analysis and retrieve the responsive documents or that a specific protocol be used to retrieve the information.[8] By ordering that parties obtain the requested ESI in this manner, courts have been able to safeguard objectionable data and ensure that private and privileged information be required to be produced.

ESI and Litigation Holds

Even if a party takes the position that "custody and control" should be interpreted narrowly and refuses to produce files on executives and directors' personal computers, care should be taken in deciding whether to preserve such ESI. As *Triton* suggests, corporate litigants and their lawyers may have an affirmative obligation to ensure that relevant emails and other ESI, which are stored on corporate directors' and executives' home computers and personal email servers, be retained and that litigation holds be extended to preserve such information.[9] The case law suggests that corporate entities have a duty to preserve relevant documents that are stored on the home computers and personal servers of their directors and executives and that the duty attaches as soon as litigation is reasonably anticipated.[10] Where litigants and their counsel fail to extend litigation holds to information stored on corporate directors' and employees' home computers and personal email servers, they may be subject to sanctions for spoliation of evidence.[11]

Endnotes

1. *See In re* Bankers Trust Co., 61 F.3d 465, 469 (6th Cir. 1995); Chaveriat v. Williams Pipe Line Co., 11 F.3d 1420, 1427 (7th Cir. 1993); Searock v. Stripling, 736 F.2d 650, 653 (11th Cir. 1984).
2. *See, e.g.*, Nalco Chem. Co. v. Hydro Techs., Inc., 148 F.R.D. 608, 618-19 (E.D. Wis. 1993) (issuing protective order regarding requested employee information, which was outside corporation's "custody and control").
3. *See, e.g.*, U & I Corp. v. Advanced Med. Design, Inc., No. 8:06-CV-2041-T-17EAJ, 2008 WL 821993, at * 9-10 (M.D. Fla. Mar. 26, 2008) (compelling production of personal hard drives used by corporate employees); Benton v. Dlorah, Inc., No. 06-CV-2488-KHV, 2007 WL 3231431, at *3 (D. Kan. Oct. 30, 2007) (holding that emails on litigant's home computer were discoverable); Hardin v. Belmont Textile Mach. Co., No. 3:05CV492-MU, 2007 WL 2300795, at *3 (W.D.N.C. Aug. 7, 2007) (holding that information on party's home computer was discoverable because the computers were "used for work benefiting [the] corporations" and because the computers were under the party's control); Ball v. Versar, Inc., No. IP 01-0531-C H/K, 2005 WL 4881102, at *3 (S.D. Ind. Sept. 23, 2005) (compelling production of trustee's home computer, which was used to transmit and receive email related to the trust); In re Triton Energy Ltd. Sec. Litigation, No. 5:98CV256, 2002 WL 32114464, at *6 (E.D. Tex. Mar. 7, 2002) (holding that documents on outside directors' personal computers should have been preserved and produced); *see also* Hoover v. Florida Hydro, Inc., No. 07-1100, 2008 WL 4467661, at *5 (E.D. La. Oct. 1, 2008) (denying motion to quash subpoena of party's friend and former roommate's personal computer records).
4. *Hardin*, 2007 WL 2300795, at *3.
5. *In re Triton*, 2002 WL 32114464, at *6.
6. *Id.*
7. *See, e.g., Hoover*, 2008 WL 4467661 at *6 (overruling general objection to production of home computer based on privacy-related concerns); *Hardin*, 2007 WL 2300795 at *4 (holding that materials on home computers were not per se "privileged" where the computers in question were alleged to contain "family data" and other personal information).
8. *See, e.g., Hoover*, 2008 WL 4467661 at *6 ("To the extent that these [privileged] communications would be retrieved during the forensic search, the protocol may be fashioned so as to exclude the names of Hoover's attorneys."); *In re Triton*, 2002 WL 32114464, at *6 ("In an effort to alleviate these [privacy and privilege] concerns, the Court will appoint a special master to review the information retrieved from the computer storage systems.").
9. *In re Triton*, 2002 WL 32114464, at *6 ("The Court is of the opinion that it would have been prudent and within the spirit of the law for Triton to instruct its officers and directors to preserve and produce any documents in their possession, custody, or control.").
10. *See Benton*, 2007 WL 3231431 at *4 (extending the standard expounded by the court in Zubalake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003), which requires parties to preserve relevant information, and/or information that will likely be requested during discovery to include the duty to preserve such information, which is stored on litigants' home computers).
11. *See, e.g.*, Cannon U.S.A., Inc. v. S.A.M., Inc., No. 07-01201, 2008 WL 2522087, at *10 (E.D. La. June 20, 2008) (awarding fees and costs where litigant failed to disclose responsive documents stored on home server); *U & I Corp.*, 2008 WL 821993 at *9–10 (imposing fees and costs and stating that, under their inherent powers, federal courts may "dismiss an action for misconduct that abuses the judicial process and threatens the integrity of that process"); *Ball*, 2005 WL 4881102 at *5 (awarding reasonable fees and expenses where litigant did not produce litigant's home computer and stating that "[c]ounsel's failure to advise Ball to retain his e-mail does not exonerate the Trustees for this discovery violation. Rather, it is compelling evidence supporting the instance of a discovery violation.").