New York Law Journal
Matrimonial Law
WWW.NYLJ.COM
An ALM Publication
VOLUME 258—NO. 20
MONDAY, JULY 31, 2017

Accessing and Using A **Spouse's ESI** in a Divorce

BY KELLY FRAWLEY AND EMILY POLLOCK

SHUTTERSTOCK

With the multiple devices used by families, from smartphones to laptops to tablets, as well as the many storage options available for the information transmitted through and accessed by those devices, managing issues relating to electronically stored information (ESI) is an important part of family law practice.

Most practitioners have had experience with a client who has obtained an email or a text message showing that her spouse is having an affair, or a client who is convinced that the smoking gun that will prove that his spouse is secreting funds and hiding assets is available on her computer.

In instances where a client has obtained ESI directly—e.g., emails, photos, text messages—or has obtained a device containing ESI—e.g., a computer—the analysis for whether and to what extent the client is permitted to use such ESI in a divorce case hinges on whether the client had legitimate access to the device, its contents and/or the account from which the information was retrieved. These situations are distinguished from cases like *Schrieber v. Schrieber*, 904 N.Y.S.2d 886 (Kings Cty. 2010) and *Etzion v. Etzion*, 796 N.Y.S.2d 844 (Nassau Cty. 2005), which provide the protocol for seeking ESI through discovery. Instead, clients who have obtained ESI are not requesting the production of information through discovery, but are seeking to present to the court information that they have obtained through another means.

KELLY FRAWLEY *and* EMILY POLLOCK *are partners in the matrimonial and family law practice of Kasowitz Benson Torres in New York.*

In *Boudakian v. Boudakian*, 240 N.Y.L.J. 123 (Queens Cty.) 2008), for example, the wife took a computer that was kept in the home to a computer expert, who cloned the hard drive. The wife then discovered, among other things, pornographic videos that the husband had filmed in the marital residence and saved on the hard drive. The court determined that because the wife knew the password and the family had used the computer, she was permitted to access its contents, even if doing so required the assistance of a computer expert. The fact that the husband accessed an email account on the computer in question that was password protected did not impact the court's analysis.

Similarly, in *Gurevich v. Gurevich*, 886 N.Y.S.2d 558 (Kings Cty. 2009), the wife retrieved emails from the husband's email account by using the password he had provided to her during the marriage but had not changed until almost two years after the commencement of the divorce action. The court determined that the emails could not be excluded pursuant to CPLR §4506 as having been obtained through eavesdropping, because the stored emails were no longer "in transit" when she retrieved them and there was no basis for the husband's claim that the commencement of the divorce case provided an "implied revocation" of the wife's right to use the husband's password to access his emails.

The issue of whether the ESI was legally obtained if the spouse's password was not known to the client during the marriage but is easily guessed, like the spouse's favorite sports team or, ironically, the parties' wedding anniversary, remains unaddressed. In *Parnes v. Parnes*, 915 N.Y.S.2d 345 (3d Dep't 2011), the wife obtained communications between the husband and his counsel by rifling through the papers on her husband's desk, finding the username and password the husband had created for a new email account, and accessing the emails in that account. The Appellate Division, Third Department, agreed that the husband had gone to sufficient lengths to keep those emails on his computer confidential such that he had not waived the attorney-client privilege, but the court was not required to rule on whether the wife would have been able to use such email communications if they were not privileged attorney communications.

> In instances where a client has obtained ESI directly or has obtained a device containing ESI, the analysis for whether and to what extent the client is permitted to use such ESI in a divorce case **hinges on whether the client had legitimate access** to the device, its contents and/or the account from which the information was retrieved.

If the client has collected a device, the inquiry should be whether he had legal access to that device—whether it was a device that was historically used by the family or just by the other spouse; or was maintained in the home or outside the home. In *Byrne v. Byrne*, 650 N.Y.S.2d, 499 (Kings Cty. 1996), the wife secured a laptop owned by the husband's employer that was regularly used in the marital residence, including by the children. The wife did not copy the hard drive, but instead turned the computer over to her attorney. The court determined that it was appropriate for the wife to secure the computer in an effort to obtain the ESI contained thereon, because a family computer's memory is akin to a file cabinet contained in the residence for which she would be entitled to retrieve anything that is not otherwise protected by the attorney-client privilege. Accordingly, the court ordered that the memory files on the computer would be downloaded, an inventory of the materials would be provided to parties' counsel, the husband would have an opportunity to assert privilege claims if appropriate, and anything not subject to a resulting protective order would be released to both parties.

To avoid challenges to the collected ESI, the best practice is to obtain the consent of the other side, or a court order, before cloning a device's hard drive, as occurred in *Byrne*. Even if it seems likely that the cloning is permissible, as in *Boudakian*, it is preferable not to risk that the information would be suppressed if the court later determined that it was not. Having a jointly-retained expert perform the cloning also helps to allocate the costs and provide a mechanism to prevent the disclosure of privileged information.

It is not clear how a court would view ESI retrieved from a storage source that is disconnected from the device like an external hard drive, network-attached storage, or cloud service. It seems likely that the "file cabinet" analogy from *Byrne* would apply, permitting the use of documents that were easily accessed on shared drives or on drives that the client could access directly.

Regardless of the source, if ESI is a communication between the client's spouse and his counsel, the client should be advised that the ESI is inadmissible unless the spouse has waived the attorney-client privilege, as in *Parnes*, 915 N.Y.S.2d at 348, where the Third Department determined that the husband waived the privilege with respect to an attorney-client communication that was left on a desk located in a common area of the house. The client should not obtain or review any privileged communications, and any such communications that a client provides to counsel should be wholly disregarded.

New York ESI cases often include analyses of the related criminal law provisions. Clients who illegally obtain ESI should understand the potential criminal implications they might face, and clients whose ESI has been illegally obtained should understand how best to capitalize on that in the litigation. For example, invoking the Fifth Amendment privilege in a civil proceeding may cause the court to draw an adverse inference, as occurred in *Crocker C. v. Anne R.*, 26 N.Y.S. 3d 724 (Kings Cty. 2015), where an adverse inference was drawn against the husband who asserted the Fifth Amendment privilege when asked about the purchase and installation of spyware on his wife's cell phone. A client may want to consult a criminal law attorney if he has purchased and/or installed spyware, or has otherwise unlawfully accessed his spouse's ESI.

Practitioners should also consider whether it is in a client's interest to reveal ESI that the client has collected, even if it was lawfully obtained. For example, if the client is concerned about her spouse's stability in a custody proceeding and is able to access his emails because he has not changed his password, it may not make sense to reveal communications she has seen, risking that he will change his password and prevent ongoing monitoring. Further, if such access is revealed, the court might have a negative impression of her for snooping on her spouse. It is important to weigh whether the benefit of revealing ESI—even if admissible—outweighs the potential adverse impact of doing so.

Counsel should highlight for matrimonial clients the potential concerns relating to the acquisition by their spouse of the client's ESI as early in the divorce process as possible by suggesting that they change their passwords, know which devices are linked to shared storage sources (e.g., the cloud), and establish a new email account that is web-based, especially for attorney-client communications.