

2. A ruling from the U.S. District Court for the District of Nebraska finding that a narrowly tailored connectivity analysis of one Defendant's electronic devices conducted by an expert, as opposed to compelling production of a full forensic mirror image of the devices, was proportional to the needs of the case for purposes of determining whether the devices contained evidence that trade secrets were misappropriated from Plaintiff's devices.

In *TK Elevator Corp. v. Abels*, No. 21-cv-3116, 2022 WL 17551765 (D. Neb. Dec. 9, 2022), U.S. Magistrate Judge Cheryl R. Zwart addressed whether a full forensic inspection of all electronic devices used by a former employee was proportional to the needs of the case, where Plaintiff claimed the inspection was necessary to determine whether a USB device was used to misappropriate Plaintiff's ESI or whether a more narrow connectivity analysis would suffice.

In this action for theft of trade secrets and violation of an employment agreement, Plaintiff requested an order compelling Defendants to produce certain relevant devices used by Defendant Bret Abels to a neutral third-party examiner for forensic examination and search. As described by Magistrate Judge Zwart, Plaintiff sought a "mirror image" of these devices, "generally described as a forensic duplicate, which replicates bit for bit sector for sector, all allocated and unallocated space, including slack space, on a computer hard drive." *Id.* at *10.

Magistrate Judge Zwart began her analysis of this issue with a discussion of the proportionality factors inherent in Federal Rules of Civil Procedure 34 and 26. But she noted that Rule 34(a) does not give the requesting party the right to search through all of the responding party's records, and that Rule 26(b)(1) allows for discovery of nonprivileged and relevant matter that is proportional to the needs of the case.

Magistrate Judge Zwart stated that "[c]ourts start from the position that granting a forensic inspection of an opponent's electronic storage device is highly intrusive" and that "skepticism concerning whether a party has produced all responsive, nonprivileged material from the target electronic devices is not a sufficient reason, standing alone, to warrant production" of a device. But she explained that there can be justifications for the production, including in cases where the device itself and the possible discovery of electronic data about its use is relevant to the claims and defenses in the suit or where there are discrepancies or inconsistencies in the responding party's discovery responses.

In this case, Defendant had searched Abels' devices during discovery, but Plaintiff sought to independently verify the response and search the devices for additional information. In particular, Plaintiff claimed that its confidential information may have been removed from its own devices via a USB device and then used by Defendants, and that a forensic inspection of Defendants' devices would either prove or disprove that theory.

Magistrate Judge Zwart ultimately concluded that permitting a forensic inspection of the devices was not proportional. *Id.* at *11. She first noted that Plaintiff had identified only four documents that were allegedly misappropriated. In this regard, she found that an inspection of Abels' personal and company-issued devices (including mobile devices, electronic data storage devices, computers, file-hosting services, and email accounts) was "extremely broad." She further found

that the proposed search would be “intrusive, costly, time-consuming, and encompass documents well beyond the scope of this lawsuit” and would require “deduplication, a review by counsel for irrelevant and privileged information and information which must be labeled confidential or attorney’s eyes only pursuant to the parties’ protective orders.” She concluded that the “facts asserted do not justify the type of sweeping search proposed.”

However, Magistrate Judge Zwart noted that a more limited search was justified based on “certain concerning inconsistencies in the facts as presented,” including that there was inconsistent evidence as to whether Abels had a personal cell phone, personal computer, USB drive, Dropbox account, or personal email address.

Specifically, Magistrate Judge Zwart ordered that a USB connectivity analysis be conducted on Abels’ personal and company-issued devices, assuming that Plaintiff could “provide the serial number of the USB device allegedly used to access” the computer Plaintiff had issued to Abels when he worked for Plaintiff. *Id.* at *12. She noted that a forensic inspection of Abels’ devices would determine whether the USB device plugged into the computer Plaintiff had issued to Abels was used to transfer files to Defendants’ devices. Magistrate Judge Zwart explained that the connectivity analysis was a more “narrowly tailored approach which will provide the information” Plaintiff sought, that is, whether the USB inserted into Plaintiff’s device was retained and could have been used by Abels to access Plaintiff’s documents after he left Plaintiff’s employ. She therefore ordered the connectivity analysis to be conducted promptly and that the parties should notify the court if further inspection of devices was required after the narrow connectivity analysis was completed.