

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month



Court Allows Discovery of Personal Computers and Personal Email

Scenario

A plaintiff is pursuing litigation against a company and against several defendants in their individual capacities. The plaintiff believes that information relevant to her claims may exist on the personal computers and in the personal emails of the individual defendants and seeks discovery of materials in those locations. The individual defendants refuse to produce their personal emails, and the plaintiff moves to compel. The general counsel of the company seeks guidance on whether the motion to compel is likely to be granted.

Searches of Personal Computers and Personal Email May Be Allowed in Certain Circumstances

In *Sunderland v. Suffolk County, et al.*, the US District Court for the Eastern District of New York granted a plaintiffs' motion to compel discovery of personal computers and personal emails of certain individual defendants. The plaintiff was a transgender inmate with gender dysphoria at the Suffolk County Correctional Facility who required medically prescribed hormone therapy. The plaintiff alleged that while she was incarcerated, the defendants refused to give her the prescribed hormone treatments because the defendants deemed the treatments to be non-essential. The plaintiff further alleged that the defendants were dismissive of her medical condition and that they acted with "deliberate indifference" to her medical needs. She sued Suffolk County, two defendants in their official capacity and three physicians in their individual capacities (the "Individual Defendants").

During discovery, the plaintiff served requests on the Individual Defendants seeking documents and correspondence concerning gender dysphoria, gender identity, transgender issues or sexual preference, including all documents or correspondence sent to or from personnel involved in the medical care of inmates at the Suffolk County Correctional Facility. While the parties agreed on search terms, the parties disagreed on whether the plaintiff should be allowed to search the personal computers and personal email files of the Individual Defendants.

The court granted the plaintiff's motion to compel, ruling that the fact that the Individual Defendants were represented by the county did not immunize them from their obligations as individual defendants under the Federal Rules of Civil Procedure (FRCP) to produce all responsive documents in their possession, custody or control. The court further held that the requests fall within the broad scope of discovery permitted by FRCP 26(b) and that because the parties agreed to search terms and at least one of the requests was date-limited, the plaintiff's request was not unduly burdensome. The court noted that documents could exist on the Individual Defendants'

personal computers that could speak to bias or motivation, which could show why a personal computer was used for that communication (as opposed to a work-issued computer). Information speaking to bias or motivation could support the plaintiff's claim of deliberate indifference.

Personal Computers and Personal Emails May Not Be Off Limits in Discovery

Sunderland is instructive on two important points relating to potential discovery of personal computers and emails. First, *Sunderland* clarifies that courts will allow discovery of personal computers and personal email files of parties to a litigation, particularly if discovery is limited. Companies that allow employees to use personal computers and other devices for work may find themselves subject to broader discovery requests as litigants demand personal communications or files that may relate to their claims. This is particularly true if companies do not have rules regarding the use of personal devices. Because companies cannot as easily control personal computers and emails, a company may be blindsided if discovery sought from individual employees reveals documents or information that could be harmful to the company's case. A company also could run into trouble if, for example, it knows that an employee uses a personal computer and does not take steps to preserve the files and information on that computer under a litigation hold.

Second, *Sunderland* also clarifies that an employee's personal beliefs and private messages may not be shielded from discovery just because they are not work-related. The court here allowed the discovery to uncover communications that could show a party's bias or motivation in performing work-related tasks and that a party otherwise might think should remain private. While the opinion does not go into detail, the context appears that the plaintiff in *Sunderland* wanted discovery of personal computers and emails to find any communications showing the Individual Defendants making derogatory or disparaging comments regarding transgendered or homosexual persons on the theory those communications could prove the plaintiff's claim that the Individual Defendants acted with deliberate indifference to her needs.

Strategies and Best Practices

With the increasingly common blending of personal convenience with professional life, companies should consider taking steps to ensure that employees are not using personal computers, other technology or email for work.

- Companies could consider rules that forbid employees from using personal computers or personal email for anything relating to their work.
- If companies allow employees to use personal computers and devices for work, companies should consider requiring employees to use the computers/devices only while connected to a company server via a remote access terminal for applications that reside on the employer's service, such as a Citrix or VPN connection.
- In appropriate circumstances, a litigation hold could require the recipient to preserve not only information and data on company systems but also information and data on his or her own personal devices.
- If in litigation where personal computers or emails could become a part of discovery, a company should consider searching the employee's personal files in order to be prepared if a "bad" document comes to light. Collecting personal files at the start of discovery also could prevent any document retention issues.

Conclusion

Under certain circumstances, all responsive data within a litigant's custody, possession and control may be subject to discovery even if that data is housed in an individual litigant's personal

computer or telephone or personal email files. Companies are well advised to consider the possibility that an individual employee's personally held data may be responsive and consider taking precautions to preserve and review such data in appropriate cases.

For inquiries related to this Tip of the Month, please contact Meytal McCoy at mmccoy@mayerbrown.com.

To learn more about Mayer Brown's [Electronic Discovery & Information Governance](#) practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com, Ethan Hastert at ehastert@mayerbrown.com, or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.