

## Pitfalls and Use of Email in White Collar Criminal Cases

A recent Supreme Judicial Court decision serves as a stark reminder of the importance of email in white collar criminal prosecutions and how the government's ability to obtain search warrants for emails must be properly balanced against a criminal defendant's right to preserve the confidentiality of emails with his or her attorney. In *Preventive Medicine Associates, Inc. v. Commonwealth*, 465 Mass. 810 (2013), the court ruled that a criminal defendant's e-mails, created after charges have been brought, may be searched provided that there is increased judicial supervision to help preserve the attorney-client privilege for emails between the defendant and the defendant's counsel.

In *Preventive Medicine Associates*, a company and its owner were charged with Medicaid fraud. After the indictment was issued, the Commonwealth applied for and was granted search warrants for two e-mail accounts associated with the company. In response, the Commonwealth received discs containing over 80,000 e-mails. After defense counsel learned that some of the defendants' e-mail accounts had been seized, they filed emergency motions to stop the Commonwealth's review.

Striking a balance between the government's need for information gathering and the right of a defendant to confidentially communicate with his or her attorney (the attorney-client privilege), the court ruled that the Commonwealth may seize a defendant's e-mail using an ex parte search warrant only if there is proper judicial supervision over the process. Thus, going forward, the Commonwealth must begin the process of seeking a warrant for such materials by: a) informing the judge when seeking e-mails of one under indictment; b) describing the relationship between the pending indictment and the search warrant; and c) explaining the need for using a search warrant rather than a subpoena.

Then, only a Superior Court judge may issue a search warrant seeking an indicted defendant's e-mails and only after a strict process is established to make sure that attorney-client communications are not disclosed to the government prosecutors and the defendant is given an opportunity to object to the procedure being used. The case contains a detailed discussion of the type of processes that can be employed.

Electronic communication is important both as a communication tool and as evidence in all forms of litigation, including white collar criminal prosecutions. While some investigative steps, such as court ordered wiretaps, are difficult to obtain and require substantial government resources to implement, seizing a target's email can provide an easy and quick road map to prove alleged criminal knowledge and intent. Therefore, during the early stages of representing a client, a defense attorney must carefully examine the client's email practices and devise an action plan to address the implications of this new procedure.

This case is an important guide for criminal law practitioners dealing with post-indictment privilege issues. It also highlights how critical electronic communication is in modern litigation and the need for attorneys and their clients to take aggressive steps to devise a system to maintain the confidentiality of their communications.