September 2011

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

E-Discovery in Criminal Investigations

Scenario

A senior corporate executive is under investigation by the Department of Justice for accounting fraud. In the course of discovery, he learns that the investigators and prosecutors secured a warrant to seize a large number of personal emails from an Internet-based electronic mail service. The executive is unsure whether or not the prosecutors can lawfully make use of this material in their investigation or at trial.

Civil Litigation v. Criminal Investigations

Unlike their civil counterpart (and to the criticism of some), the Federal Rules of Criminal Procedure are largely silent on e-discovery. Thus, the rules governing e-discovery, while well-developed in the civil context, are far less developed in the context of a criminal investigation. Further, the nature of a criminal investigation materially impacts the rights of the parties involved to obtain and use electronically stored information. Targets of a criminal investigation—be they corporations or individuals—must walk a fine line between obstructing government investigators and vigorously protecting their rights.

When the government opens a criminal investigation, it has at its disposal a number of prosecutorial powers permitting the expansive collection of information about the target of an investigation. This includes issuing a grand jury subpoena directed toward documents and obtaining a search warrant directed toward the collection of data. However, the criminal nature of an investigation also affords the target certain protections that are not available in civil litigation. That is, the target of a criminal investigation may invoke the Fourth Amendment to shield the collection or use of certain data or the Fifth Amendment to protect against the potential testimonial nature of a document production.

Balancing the Rights of the Target with the Need to Investigate Suspected Illegal Activity

Given the dominance of electronically stored information in modern society and the prevalent use of electronic means of communication, it is not surprising that the government is frequently interested in gaining access to the electronic data of the target of an investigation. The question for the target thus becomes whether he or she is afforded constitutional protections under the Fourth or Fifth Amendments that may prohibit or restrict the government's ability to obtain and use that electronic data. While the federal courts have previously considered (at least in the paper context) whether the act of producing a document itself may be sufficiently incriminating to

invoke the Fifth Amendment, surprisingly, they are just beginning to grapple with the key question of how to balance the individual's expectation of privacy with the government's need to investigate suspected illegal activity when it comes to electronic data.

First, individuals do have a reasonable expectation of privacy in the content of certain electronic communications. Recent federal court decisions have made clear that, at least with respect to email communications, individuals have a reasonable expectation of privacy, and that the government is required to obtain a warrant in order to access and use that information in a criminal investigation and trial.

Second, even with a warrant in place, the government is not free to rummage through one's person or things. The Fourth Amendment requires that a warrant describe with particularity the place to be searched and the person or thing to be seized. Government agents conducting a warrant search must adhere to these restrictions. This can be a challenge with electronic data, as computers typically contain a great deal of information that is outside the scope of the criminal investigation. The government's potential need to examine large quantities of electronic records to investigate potential illegal activity thus raises difficult Fourth Amendment issues that are not present in a search of paper files.

Third, in yet another twist, the collection of large quantities of electronic records makes it more likely that those electronic files will contain attorney-client communications. Warrants increasingly require the government to take affirmative steps to avoid reviewing privileged materials, going so far as to require use of a "filter agent"—a disinterested investigator responsible for ensuring that case-investigators do not view privileged communications.

Fourth, the Supreme Court has recognized that the act of producing documents may be testimonial in nature: that is, by producing documents, a witness may be admitting that the documents existed, were in his or her possession or control, and were authentic. Accordingly, under some circumstances, the target of an investigation may invoke the Fifth Amendment to refuse to produce documents where the act of production itself may be incriminating. It should be noted, however, that there is a circuit split as to the availability of the "act of production" doctrine as applied to corporate representatives (although even where an individual produces records in his or her capacity as a corporate representative, the government may not introduce evidence that the documents were provided by a specific custodian).

Best Practices for Challenging the Seizure of Electronic Data

In challenging a search of personal electronic data, it is essential to consider the wide array of protections afforded by the Fourth Amendment and to ask the right questions.

Did the target have a reasonable expectation of privacy in the data obtained? The target should carefully consider the type of data obtained by the government, and whether the target had a reasonable expectation of privacy in that data (whether email communications or other types of data, and even if the data is stored by a third party).

Did the government obtain a warrant? The government must obtain a warrant in order to properly obtain and use electronic data in which an individual has a reasonable expectation of privacy.

Did the warrant clearly state what was sought by the government agents in obtaining personal email? The government must specify what it seeks to obtain and must support its efforts with a showing of probable cause.

Did the warrant adequately limit the breadth of enforcement to those items for which the government had probable cause to search? Even where a warrant states with particularity the

information sought, it must take additional steps to limit collection only to materials for which it has probable cause to examine.

Is it possible that the target's personal electronic data contained a request for, or receipt of, legal advice? If so, the government must take adequate precautions to ensure protection of these privileged materials. The government must adhere to any limitations on its search designed to protect the attorney-client privilege. Frequently, a filter agent will be employed to ensure that document materials are screened for confidentiality and privilege prior to review by the government. The filter agent must be unassociated with the prosecution.

Did the warrant contain material misrepresentations or omissions? If so, the target of a government investigation may be entitled to a Franks Hearing, where a court scrutinizes the government's efforts to secure a warrant.

Will the act of producing documents itself be incriminating? If so, the target of a government investigation may be entitled, under some circumstances, to refuse to produce the documents.

For inquiries related to this Tip of the Month, please contact Michael E. Lackey at mlackey@mayerbrown.com, Therese Craparo at tcraparo@mayerbrown.com, Patrick M. Kellermann at pkellermann@mayerbrown.com, or Michelle N. Webster at mwebster@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.
