MAYER·BROWN

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

Protecting Information on Cloud-Based File Sharing Services

Scenario

A company is in the process of setting up a cloud-based file sharing service. The general counsel is concerned about, among other things, protecting unauthorized access to confidential and privileged materials she and others intend to post to the site. She has sought advice from the company's outside counsel for advice on best practices for setting up and operating cloud-based document sharing services to protect the materials posted to such sites from inadvertent access.

Cloud-Based File Sharing Services

Cloud storage has revolutionized the way businesses share information, both within and outside the organization. Many cloud storage services—most prominently Dropbox and Box—include a feature that lets users share files with anyone who receives a hyperlink to that file. Anyone who has (or can guess) that hyperlink can access the file or account associated with it. Although this feature of cloud storage sites allows easy information sharing, there may be significant legal consequences if, during litigation, that hyperlink is the only means of access control. This issue recently arose in *Harleysville Insurance Company v. Holding Funeral Home, Inc., et al.*, No. 1:15-cv-00057 (W.D. Va., Feb. 7, 2017), in which a US district court held that a party that shares access to information using hyperlinks, without further access control, waives any claim of privilege or work product protection over that information.

Harleysville—Facts

The plaintiff, Harleysville Insurance Company, suspected that a defendant had set a fire that destroyed the defendant's property. During Harleysville's investigation of the defendant's insurance claim, a Harleysville employee sent to the National Insurance Crime Bureau ("NICB") a hyperlink to a file in a Box account that contained a surveillance video of the fire scene. There was no further access control for the file: anyone with the link could access the Box account and the information stored there. Later, Harleysville uploaded its entire investigation and claims file to the same Box account without applying any further access control.

During discovery, defense counsel subpoenaed NICB's documents related to the fire claim. NICB complied with the subpoena and included in its responsive production a copy of the email containing the link to the Box account. Defense counsel typed the link into a web browser, accessed the Box account and—without informing Harleysville's counsel—downloaded Harleysville's entire claims file, including potentially privileged information.

Only later did Harleysville's counsel realize that defense counsel had downloaded the claims file.

Harleysville moved to disqualify defense counsel, arguing that downloading the claims file was an improper, unauthorized access to privileged information. Defense counsel argued that by placing the claims file on an unsecured Box account, where anyone with the right link could access it, Harleysville waived any claim of privilege.

Harleysville—the Court's Decision

The US District Court for the Western District of Virginia agreed with defense counsel, applying Virginia law to hold that "Harleysville has waived any claim of attorney-client privilege with regard to the information posted" to the Box account. The court found that, because "anyone, anywhere" with the link to the Box account could access the claims file, Harleysville "conceded that its actions were the cyber world equivalent of leaving its claims file on a bench in the public square and telling its counsel where they could find it."

The court rejected Harleysville's argument that defendant counsel's access to the files amounted to ethical misconduct that would render the disclosure "involuntary" and void any waiver. Instead, it held that Harleysville's subjective "intention is not determinative of whether the disclosure was involuntary or inadvertent." Instead, because Harleysville intentionally uploaded the claims file to the insecure Box account, Harleysville permitted defense counsel to access it, and the disclosure was an inadvertent result of Harleysville's carelessness.

For similar reasons, the court also rejected Harleysville's attempt to claw the document back under Federal Rule of Evidence 502, which provides that, notwithstanding the disclosure of otherwise privileged information, the privilege is not waived if (1) the disclosure was inadvertent; (2) the holder of the protection took reasonable steps to prevent the disclosure; and (3) after the disclosure, the holder of the protection took reasonable steps to rectify the error, including requesting that the other party destroy or sequester the protected documents. The court held that (1) the disclosure was not inadvertent because Harleysville intentionally uploaded the claims file to the Box account, and (2) Harleysville had not taken "reasonable steps" to prevent the disclosure because it had uploaded its entire claims file in a manner that made it available to anyone with access to the hyperlink.

The *Harleysvill*e court's holding of waiver is particularly striking because it also held that defense counsel had failed to comply with their ethical obligation to inform Harleysville that they had come into possession of information subject to a potential privilege claim. The court, relying on Virginia state bar ethics rules and state court decisions, held that defense counsel had an obligation to notify Harleysville once they discovered they had potentially privileged information. But they did not. And, the court reasoned, defense counsel should have realized that the materials in the Box account may have been privileged once they examined them. Despite these failures, the court concluded that disqualifying defense counsel was inappropriate because Harleysville had waived privilege and work product protections over the claims file.

Practical Steps for Avoiding Waiver

The *Harleysville* court analogized uploading information to a cloud storage site without specific access control to leaving documents on a park bench for anyone in the world to see. To avoid such findings, companies should familiarize themselves with the access control features of any tool they use to share information and take affirmative technical steps to restrict access to any materials posted to such a site—especially confidential or privileged information. Such controls include password protections and limiting user access to only the documents that each particular user needs access to.

For inquiries related to this Tip of the Month, please contact Geoffrey Pipoly at

gpipoly@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 or Ethan Hastert at ehastert@mayerbrown.com.

Please visit us at www.mayerbrown.com.