E-discovery

Protect the contents of cloud file-sharing accounts with fused hyperlinks.

BY PIERRE GROSDIDIER

A party uploaded privileged documents into a cloud file-sharing account unprotected by a password. Opposing counsel found the hyperlink through discovery happenstance, accessed the account, and downloaded and read the documents. The court held that the party waived both the attorney-client communication privilege and the work-product doctrine immunity as to the documents. The decision, *Harleysville Ins. Co. v. Holding Funeral Home, Inc.*, illustrates how an e-discovery fluke can compromise a case.[1]

Harleysville is significant because counsel routinely transfer files via cloud file-sharing accounts, the so-called file link method. The files are safe because the account access hyperlinks are so complicated and unique that they act as de facto passwords. For example, Harleysville's hyperlink was https://nationwide.box.com/s/brajdu818uvivfxibbitld520ozx60ml.[2] But in this case Harleysville failed to redact an email, opposing counsel discovered the hyperlink, and Harleysville paid dearly. Harleysville might have used a password-requiring file transfer alternative, such as File Transfer Protocol, or FTP. But even this arrangement would not have solved Harleysville's problem absent a redaction of either the account username or password from the produced emails. Alternatively, Harleysville might have used the file link method with a hyperlink that automatically expired after a week or two, a so-called fused or timed hyperlink. An expired hyperlink will deny account access and, therefore, always defeat the consequences of a redaction oversight.

The facts as set forth by the court are bewildering albeit not overly complicated. Harleysville Insurance Company filed a declaratory action against its insured, Holding Funeral Home, on the ground that arson caused the fire that destroyed Holding's funeral home. Harleysville's investigator uploaded a surveillance video of the fire scene to a Box cloud file-sharing account for the benefit of an employee of the National Insurance Crime Bureau, or NICB. The investigator also sent the NICB employee an email with the account hyperlink. Later, the investigator loaded Harleysville's complete claims and investigation files to the same unprotected account for transmittal to Harleysville's counsel.

Holding later subpoenaed NICB's file for the fire and found the hyperlink in the investigator's unredacted email. Without notice to Harleysville, Holding accessed the Box account and found, downloaded, and reviewed the files. Harleysville discovered the breach and moved against Holding, arguing inter alia that the attorney-client privilege and the work-product doctrine protected the files. Holding retorted that "Harleysville waived any claim of privilege or confidentiality" when it uploaded the files to the unprotected and "access[ible] by anyone" Box account.[3] The court first held that Virginia law governed the issue of waiver of confidentiality as to attorney-client communications, and federal law that of waiver of the work-product's protection.[4] It then proceeded under the assumption that the files contained some legitimately protectable information, without addressing the issue.

Harleysville waived any claim of attorney-client privilege.

In addressing whether Harleysville waived the attorney-client privilege, the court first analyzed whether the disclosure was involuntary or inadvertent. An involuntary disclosure proceeds through criminal or bad faith conduct, without the consent of the party asserting the privilege. An inadvertent disclosure results from mistakes or insufficient protective precautions by the privilege's proponent. The court found that Harleysville's disclosure was inadvertent because it unknowingly granted access to the files when it failed to deploy adequate security measures to protect their confidentiality.[5] That Harleysville did not intend to share the files with Holding was not dispositive. Under Virginia law, intent "is not determinative of whether the disclosure was involuntary or inadvertent." Were intent determinative, all unwanted disclosures would arguably be involuntary.[6]

Using the Supreme Court of Virginia's five-factor test, the court then analyzed whether Harleysville's disclosure waived the attorney-client privilege. The *Walton* test considers:

(1) the reasonableness of the precautions to prevent inadvertent disclosures;
(2) the time taken to rectify the error;
(3) the scope of the discovery;
(4) the extent of the disclosure; and
(5) whether [enforcing confidentiality would be unfair].[7]

The first, second, and fourth factors informed the court's decision that Harleysville had waived its privilege claim. The court opined that the record showed that the investigator had taken no precautions to prevent the files' disclosure.[8] The investigator "either knew—or should have known—that" any uploaded information was completely exposed to anyone who had the hyperlink. Moreover, the investigator uploaded the files' "vast" amount of data to this unprotected account. Finally, the court noted, the investigator left the files accessible in the account for six months. Harleysville's counsel also accessed the files and likewise knew that the account was unprotected but did nothing. Describing Harleysville's conduct as "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 found that the disclosure waived the attorney-client privilege.[9]

The court's analysis expressly discounted the third *Walton* factor, namely the import of the "production of a few privileged pages among voluminous pages of production," because there was "no claim

that the third factor—the scope of discovery—contributed to this inadvertent disclosure." But, alternatively, a party in Harleysville's position might leverage this factor to its advantage by arguing that its error was to fail to redact the hyperlink-containing email, which resulted in the production of *one* privileged page in what the *Harleysville* court otherwise described as a "vast" production.

The court concluded its analysis of this first issue by averring its belief "that its decision on this issue foster[ed] the better public policy." Companies who elect to adopt today's rapidly evolving information-sharing technology should ensure that their "employees and agents understand how the technology works, and, more importantly, whether the technology allows unwanted access by others to its confidential information." The court's admonition tracks the duty of technical competence advocated in comment eight on the American Bar Association's Model Rule 1.1 ("Maintaining Competence"), which the Virginia State Bar adopted in 2015. Comment six on Virginia's Rule 1.1 states that "[a]ttention should be paid to the benefits and risks associated with relevant technology."

Harleysville waived any claim to the work-product doctrine.

The court then turned to Harleysville's work-product privilege claim, which the court held was governed by Federal Rule of Evidence 502(b). This rule states that an inadvertent disclosure

> does not operate as a waiver if . . .
> (1) the disclosure is inadvertent;
> (2) the holder of the . . . protection took reasonable steps to prevent disclosure; and
> (3) the holder promptly took reasonable steps to rectify the error, including . . . following Federal Rule of Civil Procedure 26(b)(5)(B).[10]

Stated otherwise, "[a] disclosure operates as a waiver of work product protection unless Rule 502 applies," with the protection's proponent bearing the burden of proving that each of the rule's elements are met. Based on admittedly sparse caselaw defining the term "inadvertent disclosure," the court held that Harleysville's information release did not qualify as "inadvertent 'under federal law.'" In reaching this conclusion, the court cited indirectly to an unpublished Fourth Circuit case, which held that:

> [A]n inadvertent waiver would occur when a document, which a party intended to maintain as confidential, was disclosed by accident such as [through communication or production errors]. In contrast, when a client makes a decision—albeit an unwise or even mistaken, decision—not to maintain confidentiality in a document, the privilege is lost due to an overall failure to maintain a confidence.[11]

The court reasoned that Harleysville did not argue that its investigator acted unintentionally. Moreover, the court observed, Harleysville took no measures to prevent and to remedy the disclosure. The court also compared the investigator's unprotected upload of the files to information disclosed in public meetings or posted on the internet.[12] In both cases cited by the court, the disclosing parties waived their claims that the work-product doctrine protected the shared information. For these reasons, Rule 502's exception did not apply to avert Harleysville's waiver of the work-product doctrine.

The file link method is safe to use because enabling hyperlinks are de facto passwords, with the added advantage of being almost impossible to guess.[13] But no password and no hyperlink are safe from inadvertent disclosure, as in this case. The takeaway is to always use fused hyperlinks; the shorter the fuse, the better. **TBJ**

Notes

1. No. 1:15-cv-00057, 2017 WL 1041600 (W.D. Va. Feb. 9, 2017) (mem. op.) (slip copy) (Sargent, M.J.).
2. Memorandum in Support of Plaintiff's Motion Requesting the Disqualification of Defendants' Counsel, *Harleysville Ins. Co. v. Holding Funeral Home, Inc.*, No. 1:15-cv-00057, Exhibit 3 (W.D. Va. Dec. 21, 2016) (Pacer Doc. 53-3).
3. *Harleysville*, 2017 WL 1041600, at *2.
4. *Id.* (citing *Continental Gas Co. v. Under Armour, Inc.*, 537 F. Supp. 2d 761, 769–70 (D. Md. 2008)).
5. *Id.* at *3.
6. *Id.* (citing *Walton v. Mid-Atl. Spine Specialists, P.C.*, 694 S.E.2d 545, 551 (Va. 2010)).
7. *Id.* at *4 (*citing Walton*, 694 S.E.2d at 552).
8. *Id.* ("the court has no evidence before it that *any* precautions were taken to prevent this disclosure") (emphasis in original).
9. *Id.* at *5.
10. *Harleysville*, 2017 WL 1041600, at *5 (citing Fed. R. Evid. Rule 502(b)).
11. *Id.* at *6 (citing *ePlus Inc. v. Lawson Software, Inc.*, 280 F.R.D. 247, 255 (E.D. Va. 2012) (citing *McCafferty's Inc. v. Bank of Glen Burnie*, Case No. MJG–96–3656, 1998 U.S. Dist. LEXIS 12861 (4th Cir. Apr. 23, 1998) (unpublished))).
12. *Id.* (citing two Fourth Circuit district court cases).
13. Barring a sophisticated and criminal hacking effort.
14. *Law360* published a first version of this article on March 30, 2017, under the title "Failing to Prevent Inadvertent Disclosures Can Be Costly" (subscription required).

This article, which was originally published by Law360, *has been edited and reprinted with permission.*[14]

The author is very grateful to his colleague T. Wisinski for his insightful comments regarding this article.

PIERRE GROSDIDIER

is counsel to Haynes and Boone's Business Litigation practice group in Houston. He specializes in complex commercial litigation, especially disputes with construction, engineering, or software elements. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, is certified in construction law by the Texas Board of Legal Specialization, and is a registered professional engineer in Texas (inactive).