haynesboone

March 30, 2017

Failing To Prevent Inadvertent Disclosures Can Be Costly

By Pierre Grosdidier

Originally published in Law360 (subscription required)

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 court also denied the party's motion to disqualify opposing counsel, but it held that "some sanction [wa]s appropriate," and it awarded the party certain costs. *Harleysville Ins. Co. v. Holding Funeral Home, Inc.*[1] *Harleysville* illustrates how an e-discovery fluke can compromise a case.

This case is significant because the practice of loading files that contain privileged information to cloud storage accounts that are not explicitly password-protected, the so-called file link method, is not uncommon. Counsel then transmit the account hyperlink to the intended recipient by email and assume that the files are safe because the hyperlink is so complicated that it acts as a *de facto* password. Because no one else knows the hyperlink, no one can access or stumble upon the data cache.[2] In effect, the sender assumes that the very small likelihood of a breach does not justify the administrative burden of creating a password. In *Harleysville*, this assumption proved erroneous. Opposing counsel obtained the hyperlink and Harleysville paid a heavy price.

There are several file transfer alternatives including File Transfer Protocol (FTP), which typically requires a username and a password sent separately. Alternatively, the file link method can be used with hyperlinks that automatically expire after a set amount of time, typically not more than two weeks. Practitioners speak of this device as placing a "time-out" or a "fuse" on a hyperlink. For a party loading data to otherwise unprotected cloud accounts, the takeaway from this case is to always use fused hyperlinks; the shorter the time-out period, the better. As a separate precaution, a party receiving confidential data should download the data timely and place the sender on notice that the download is complete and that the cloud storage space can be cleared or the account disabled. These precautions might have avoided the mishap that struck Harleysville.

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 an unprotected Box, Inc. cloud-based account for the benefit of an employee of the National Insurance Crime Bureau ("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 (the "Files") to the same unprotected account to be retrieved by Harleysville's counsel.

Holding later subpoenaed NICB's file for the fire and found the hyperlink in the investigator's email. Without notice to Harleysville, Holding accessed the Box, Inc. account and found, downloaded, and reviewed the Files. Harleysville discovered the problem when it reviewed Holding's own production, which contained the Files. When the parties could not resolve the matter amicably, Harleysville moved to disqualify Holding for its improper and unauthorized access to information allegedly protected by the attorney-client privilege and the work-product doctrine. Holding opposed the motion arguing that "Harleysville waived any claim of privilege or confidentiality" when it uploaded the Files to the unprotected and "access[ible] by anyone" Box, Inc. account.[3]

The court first resolved whether Harleysville waived its attorney-client privilege and work-product doctrine claims. As a threshold matter, it 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] The court also

proceeded under the assumption that the Files contained some information that legitimately warranted protection from disclosure, without deciding the issue.

Harleysville waived any claim of attorney-client privilege.

In addressing whether Harleysville waived its claim of attorney-client privilege as to the Files, the court first analyzed whether the disclosure was involuntary or inadvertent. An involuntary disclosure is one that is accomplished 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 this the case, all unwanted disclosures would arguably be involuntary.[6]

Using the Virginia Supreme Court's five-factor test, the court then analyzed whether Harleysville's disclosure waived the attorney-client privilege, which 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 the party asserting the claim of privilege or protection for the communication has used its unavailability for misleading or otherwise improper or overreaching purposes in the litigation, making it unfair to allow the party to invoke confidentiality under the circumstances.[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.[9] Finally, the court noted, the investigator left the Files accessible in the account for six months.[10] Harleysville's counsel also accessed the Files and, therefore, 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.[11]

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." Somewhat surprisingly, given the facts of the case and this *dictum*, the court did not refer to the duty of technical competence advocated in Comment 8 to the ABA's Model Rule 1.1, which Virginia adopted on December 17, 2015.[12] Regarding "Maintaining Competence," Comment 6 to Virginia's Rule 1.1 states that "[a]ttention should be paid to the benefits and risks associated with relevant technology."[13]

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 privilege or 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).[14]

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 case law 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 a misaddressed communication to someone outside the privilege scope or the inadvertent inclusion of a privileged document with a group of nonprivileged documents being produced in discovery. 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.[15]

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 Internet.[16] 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.

Having concluded that Harleysville waived any claim to protect the Files, the court sanctioned Holding, per applicable ethics rules, for having failed to contact Harleysville after downloading the Files to reveal that Holding had accessed them. The court observed that, in case of doubt, Holding should have solicited the court for its opinion of the matter, but "Counsel chose not to do so, however, and, therefore, the court believes that such conduct requires some sanction."[17] The court declined to disqualify Holding's counsel, but ordered that it bear Harleysville's motion costs.

As noted, hyperlinks to cloud storage accounts are very complicated and effectively act as their own passwords. In a hypothetical variation of *Harleysville*'s fact pattern, assume the account is password-protected and the investigator sends the password in a separate email. Both emails (link and password) eventually end up in opposing counsel's hands, as in *Harleysville*. Would a court treat opposing counsel's access to the account differently if done using the password versus using only the hyperlink, which is arguably a *de facto* password? Given the increasing use of cloud storage accounts, this fact pattern might be just around the corner.

---

[1] No. 1:15-cv-00057, --- F. Supp. 3d ---, 2017 WL 1041600 (W.D. Va. Feb. 9, 2017) (mem. op.) (Sargent, M.J.).
[2] Barring a sophisticated and criminal hacking effort.
[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*. (*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*.
[10] *Id*.
[11] *Id*. at 4.
[12] *See* Virginia Rule of Professional Conduct 1.1, Cmt. 6 ("Maintaining Competence").
[13] *Id*.
[14] *Harleysville*, 2017 WL 1041600, at 4 (*citing* Fed. R. Evid. Rule 502(b)).

[15] *Id*. at 5 (*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))).
[16] *Harleysville*, 2017 WL 1041600, at 5 (citing two Fourth Circuit district court cases).
[17] *Id. at* 6.