IS NEW TECH CLOUDING THE ISSUE OF ATTORNEY-CLIENT PRIVILEGE?

BY STEPHEN K. LEWIS, ESQ.

Recently, a federal court in Virginia ruled that parties can waive privileges by placing data in the cloud, reasoning that such, "…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." *Harleysville Ins. Co., v. Holding Funeral Home, Inc.,* at 9 (US Dist.Ct. W.D. VA, 2017). In today's environment, it's almost certain your firm is using a cloud provider for data sharing. Email systems simply don't allow large data transfers. It is even possible your office uses multiple services. And, while most cloud providers enable secured sharing, as evidenced by *Harleysville,* not all firms are sharing in a secure fashion. Thus, if you are not 100 percent sure how your office shares large files, this is a good time to make certain.

Thus far, there is no case law directly on point in Nevada. Nonetheless, we have some instructive cases, instructive opinions and *Harleysville*. Thankfully, the *Harleysville* court conducted a reasonably thorough examination of law and fact in its Memorandum Opinion, prior to holding that "…posting of the Claims File to the internet waived any attorney-client privilege or any work-product protection over the information contained in the file." *Id.* at 17. Thus, attorneys have plenty of points with which to distinguish their own cloud debacles, should they ever arise.

In *Harleysville,* the cloud provider used was Box.com. Unfortunately, there was nothing unique about how Box.com was utilized. If your office sends unsecured links, it is important to realize that whoever "has" the link also has unfettered access to the linked data. Remember, a link (or "hyperlink") is a highlighted word or image, activated by clicking, that then takes the user to a website, file or document located elsewhere. Remember, a link can also be typed into an internet search engine, forwarded to others or copied. Thus, one does not need to be the original recipient, or even receive an email containing the embedded link, in order to use it; one simply needs the link itself.

Think of a standard link like the physical key to a house. Whoever has the key can open the front door and gain access to what's inside. Obviously, a key can be copied and used by whoever possesses it. Just as a house key lacks the ability to choose who holds it, so does the standard link. The holder of the link gets the data. But it gets worse.

continued on page 24

continued from page 23

IS NEW TECH CLOUDING THE ISSUE OF ATTORNEY-CLIENT PRIVILEGE?

With most cloud providers, a standard link is active forever. As with a house key, there is nothing preventing anyone from copying it and handing it out to anyone and everyone; this is what happened in *Harleysville*. That weight you may be feeling is the realization that the risks an unsecured link carries are far greater than losing a privilege argument. Anything sent via link is at risk.

Furthermore, It should not surprise you to learn that different people use different cloud providers to share information. Often, staff members use their personal cloud accounts to share work data simply because it is easier for them. Yet, as stated in *Harleysville,* a firm " should be responsible for ensuring that its employees and agents understand how the technology works, and, more importantly, whether the technology allows unwanted access by others to its confidential information." *Id.* at 10. So, you are required to be aware of the risks your firm is taking.

Accordingly, it's time to talk to your staff and confirm every service each member uses, whether or not those services allow secured shares and if your office is securing all shares.

Some readers may be thinking, "of course!" but if you are just learning of these risks, you may be in the majority. And don't expect to be excused by pleading ignorance. The magistrate stated, "[B]ecause of his previous use of the Box Site, this employee either knew - or should have known …." *Id.* at 9. So, if you are not 100 percent sure of your shares, it's time to become sure. If you have any unsecured links, disable them or remove the data from the cloud.

So, what does this mean in Nevada? While there is no case directly on point here, there are a few cases to which we can look for some direction regarding what our courts might do. *See Merits Incentives LLC v. Eighth Judicial Dist. Court,* 127 Nev. Adv. Op, 63 (Nev, 2011) and *Las Vegas Sands Corp. v. Eighth Judicial Dist. Ct.,* 318 P.3d 618 (Nev., 2014). We can also look to the State Bar of Nevada's Standing Committee on Ethics, Opinion No. 33, from February 9, 2006, along with the newly issued American Bar Association (ABA) Opinion 477, for guidance.

In the *Merits* matter, an attorney received and reviewed documents anonymously delivered to his law firm by a third party. After review, counsel disclosed the documents in a Rule 16.1 production, designating the documents and the way in which they were received. Some of the documents were believed to be privileged and/or work-product by opposing counsel. As such, opposing counsel filed a motion to disqualify the reviewing attorney. The trial court denied the motion, finding the recipient attorney did nothing wrong or unethical in receiving and/or concealing his possession of the data, and the Supreme Court affirmed. However, the court did prohibit use of the confidential documents in the matter. *Merits* at 727.

In 2014, *Las Vegas Sands Corp. v. Eighth Judicial Dist. Ct.* addressed a waiver of privilege matter. In this case, counsel utilized privileged information to refresh a witness's recollection during testimony. Opposing counsel then demanded the privileged document. Thus, we have a case in which counsel affirmatively placed the privileged data at issue, certainly not to the extent that it was done in *Harleysville,* but more so than in *Merits. See Las Vegas Sands Corp. v. Eighth Judicial Dist. Ct.,* 318 P.3d 618 (Nev., 2014). Again, we see the Nevada Supreme Court upholding a waiver of the privilege, albeit a limited waiver. However, the court did not issue a complete waiver, but limited it to impeachment only. *Sands* at 623. The court allowed opposing counsel to inspect the documents, cross-examine the witness on the contents and admit the evidence for the purpose of impeachment only.

continued on page 26

continued from page 24

IS NEW TECH CLOUDING THE ISSUE OF ATTORNEY-CLIENT PRIVILEGE?

What we can see in both Nevada cases is that the Supreme Court is not overly protective of the attorney-client privilege. It therefore seems safe to assume that using the cloud and sharing information through an unsecured link could bring about the same result: a waiver.

SBNV Opinion 33, although a few years old, appears to apply to the cloud disclosure issue. Opinion 33 states that a lawyer must act "competently and reasonably" in safeguarding confidential client data. If we are to take the *Harleysville* analogy to heart, equating the sending of data through an unsecure link to leaving a file on a park bench, it will be hard for any attorney to argue they acted "competently and reasonably" when faced with a link breach. At this point, with technology changing faster than cases can move through the courts, perhaps the state bar can supplement Opinion 33, or even issue a new opinion on the same point.

Most recently, ABA Opinion 477 was issued. It takes a nice long look at the cloud. But a summary can be quickly digested; "A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access." This is quite similar to SBNV Opinion 33, falling squarely within the *Harleysville* ruling. Namely an attorney must take

reasonable efforts to prevent inadvertent access. But what is reasonable? The ABA Cybersecurity Handbook sets forth the standard of reasonable efforts:

"... [The ABA rule] adopts a fact-specific approach to business security obligations that requires a 'process' to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments."

Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. These factors include:

- The sensitivity of the information,
- The likelihood of disclosure should additional safeguards not be employed,
- The cost of employing additional safeguards,
- The difficulty of implementing such safeguards, and
- The extent to which these safeguards adversely affect a lawyer's ability to represent his or her clients.

The ABA Opinion goes on to state, "lawyers must establish policies and procedures, and periodically train employees … supervising lawyers must follow up to ensure the policies are being implemented ... and update these policies." This sounds eerily like *Harleysville*.

Simply put, gone are the days when firms could just fax something and then forget it. As technology changes, so too must the practitioner, who must make every effort to understand how this new technology works. **NL**

STEPHEN K. LEWIS is the current C.O.O. of local software security start-up, StoAmigo. Prior to working with StoAmigo, Lewis litigated with Patti, Sgro & Lewis for more than a decade, spent time as in-house counsel and worked with a California law firm.