Westlaw Journal
INSURANCE COVERAGE
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 27, ISSUE 28 / APRIL 21, 2017

EXPERT ANALYSIS

Share With Care: A Recent Decision Demonstrates the Perils of Sharing Links Without Passwords

By Stephen D. Palley, Esq., and Peter A. Halprin, Esq.
Anderson Kill PC

A recent decision from the U.S. District Court for the Western District of Virginia highlights a potential problem with file sharing.

A link to a set of documents that is not password protected can leave those documents vulnerable to disclosure to unintended parties — and may constitute waiver of attorney-client privilege.

The recent decision, *Harleysville Insurance Co. v. Holding Funeral Home Inc.*, No. 15-cv-57, 2017 WL 1041600 (W.D. Va. Feb. 9, 2017), is an insurance coverage dispute arising out of a fire loss.

The issue before the court was whether, by using a non-password-protected link to send claim file materials, the insurance company waived attorney-client privilege and work product protections.

During the course of its investigation, the insurance company placed its entire claims file in a folder on a cloud-based file sharing and storage site and provided a hyperlink to its counsel so that he could access the information.

In addition to the claims file, the folder included information from an insurance company investigator.

Anyone possessing the link could gain access to the claims file by clicking on the link, which was not password protected.

During the course of discovery in the lawsuit, the policyholder's lawyer saw a reference to the link in a document, clicked the link, and thereby had access to the entire claims file as well as all of the materials uploaded by the insurance company investigator.

In responding to discovery, the policyholder's lawyer produced documents that were downloaded from the file sharing site.

The insurance company filed a motion to disqualify the lawyer for what it characterized as "unauthorized access" to privileged information, citing attorney-client privilege and work product protections.

The District Court disagreed with the insurance company's position and ruled that the attorney-client privilege and work product protections were waived.

Key to the court's ruling was the fact that the link to the filing sharing site was not password protected.

And, as such, "the information uploaded to this site was available for viewing by anyone, anywhere who was connected to the internet and happened upon the site by use of the hyperlink or otherwise."

In short, the insurance company knew or reasonably should have known that by using an unprotected link, third parties could access the material.

Per the court:

> In essence, [the insurance company] has 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. It is hard to imagine an act that would be more contrary to

> protecting the confidentiality of information than to post that information to the World Wide Web.

Although the insurance company's disclosure of its claims file provided the policyholder with the full file, the result is a cautionary tale for policyholders.

Policyholders using cloud-based services to provide access to information should consult their technology professionals to ensure that files are adequately protected both on the cloud and when they are being transferred.

To that end, policyholders should also consider using password protection when transmitting links as well as assigning an expiration date when access to the folder will expire.

The degree of care taken to protect against third-party access to information will likely be a factor when a court is evaluating whether a waiver has occurred.

In the words of the court:

> The technology involved in information sharing is rapidly evolving. Whether a company chooses to use a new technology is a decision within that company's control. If it chooses to use a new technology, however, it 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.

File sharers, take note.

Stephen D. Palley, (L) a trial lawyer based in the Washington office of **Anderson Kill PC**, represents policyholders seeking insurance coverage, with a particular focus on emerging technology, software development and the construction industry. He can be reached at spalley@andersonkill.com or 202-416-6552. **Peter A. Halprin**, (R) an attorney in the firm's New York office and co-deputy chair of the its cyberinsurance recovery group, concentrates his practice in commercial litigation and insurance recovery, exclusively on behalf of policyholders. He can be reached at phalprin@andersonkill.com or 212-278-1165. A version of this expert analysis was first published March 31 as an Anderson Kill Policyholder Alert. Republished with permission.