



## THE RISKS OF OVERSHARING ON THE CLOUD

By Joshua Stein, principal of Joshua Stein PLLC

*Joshua Stein  
Joshua Stein PLLC  
501 Madison Avenue, Suite 402  
New York, NY 10022  
joshua@joshuastein.com  
joshuastein.com*

**L**awyers, their clients and their adversaries in litigation and deals share information and documents constantly. Once, this took time, coordination and affirmative efforts to make sure the right information got to the right people. The information existed on paper, so if someone then wanted to share it with someone else, that required another round of photocopying and more coordination.

Computers and, particularly, “the cloud” changed all that. Anyone with a computer can collect information, put it in a folder on their computer and with a few keystrokes, share that folder with anyone anywhere. That person can share it again with anyone else. This is incredibly powerful and represents one of many reasons that transactions happen much faster than in 1985. But it also creates new opportunities for embarrassment and error.

A recent insurance coverage litigation demonstrates exactly how the cloud can go wrong as a channel for sharing information. In that litigation, an insurance company uploaded video surveillance footage to a cloud website operated by the Box file-sharing service. After the insurance company uploaded that video file into a Box folder, someone at the company shared the folder with lawyers who represented the holder of the insurance policy in dispute. So far so good: that’s how it was supposed to work.

Later, though, the insurance company used the same Box folder to hold its entire claim file, including lots of information that was

supposed to remain privileged and not available to opposing counsel. But the opposing counsel still had access to that Box folder. Apparently, no one remembered opposing counsel had been given the necessary access credentials. Opposing counsel visited the folder again, and (innocently or otherwise) downloaded a copy of the insurance company’s entire claim file.

The insurance company tried to disqualify the policy holder’s counsel because of its access to the insurance company’s privileged and confidential information. This led to a complex dispute about attorney-client privilege, how a waiver worked, whether a waiver had occurred, and whether unintentional sharing of privileged information constituted a waiver. All those issues may be incredibly interesting to litigators, courts and professors of civil procedure.

The actual decision by the court, however, should be incredibly interesting to anyone who does business and uses the cloud to share confidential information. The court decided that the insurance company lost the ability to assert attorney-client privilege — and in effect lost any confidentiality — for its entire claim file as soon as the file was inadvertently shared with opposing counsel.

In the court’s words, the insurance company “unknowingly provided access to information by failing to implement sufficient precautions to maintain its confidentiality.” The employee who uploaded the video and later uploaded the entire claim file “should have known . . .

that the information uploaded to the site was not protected in any way and could be accessed by anyone who simply clicked on the hyperlink.” Under such circumstances, the attorney-client privilege was lost, as well as the related “work product” privilege that sometimes applies.

The court said the insurance company had taken actions that were “the cyberworld equivalent of leaving its claims file on a bench in the public square and telling [the other side] where they could find it.” Any company that uses new technology, the court said, should properly train its employees on its risks and proper use. That didn’t happen here.

The moral of the story is rather straightforward: whenever one sets up a channel to share information over the internet, one must take care to remember who has access to that channel. When in doubt, create a new and separate channel. Before adding information to an existing channel, it pays to recheck how that existing channel works. After a channel has served its purpose (here, sharing of the video file with the other side), one should shut it down. Moreover, if one wants to share important information outside the organization, one probably shouldn’t rely on folder-sharing products like Box or Dropbox. Instead, plenty of very organized and well-structured online services exist to share information, control access to each item, and track who sees what.

To read the case, search for “Abingdon Harleysville Holding.”