Weekly Wright Report (10/9/17)

TECHNOLOGY LAW

Loss of Privilege When Using New Technology… Or OMG, What Have We Done?!?!

As technology makes transmission, sharing and storing information easier and more efficient, so too does it create pitfalls and traps for the unwary. This lesson was learned the hard way by Harleysville Insurance Company in a case brought against it by a fire damaged funeral home. *See Harleysville Insurance Co. v. Holding Funeral Home, Inc., No. 1:15 -cv-00057, 217 US Dist. LEXIS 18714 (W.D.VA. February 9, 2017).* Harleysville sought a declaratory judgment on whether its policy covered the fire damage. Harleysville is owned by Nationwide Insurance Company. Nationwide posted a video about the fire to a file-sharing service, Box, Inc. Nationwide subsequently emailed the National Insurance Crime Bureau giving it a hyperlink to the Box, Inc. site. The Box, Inc. site was not password protected and was accessible to anyone using the hyperlink. Later, Nationwide uploaded Harleysville's entire claim file to the same Box, Inc. site. This included Nationwide's investigation file. Among other things, the file contained documents produced by or to and from Nationwide's and Harleysville's attorneys. Nationwide sent Harleysville's attorneys the same hyperlink that had been given to the National Insurance Crime Bureau. The funeral home, Holding, subpoenaed the files of the National Insurance Crime Bureau. The Bureau responded to the subpoena by producing documents received from Harleysville. However, the documents also included Nationwide's email with the Box, Inc. hyperlink. Using that hyperlink, Holding's attorneys were able to gain access to the Box, Inc. site which contained the claim files of both Nationwide and Harleysville, including information that would have been protected by the attorney-client privilege. When Harleysville's attorneys discovered that Holding had access to its potentially privileged materials, it complained and requested Holding's counsel to destroy its copies. However, Holding's attorneys had already reviewed the material.

The court found that even though Harleysville's disclosure was inadvertent, it waived the attorney-client privilege. Harleysville did not take any precautions to prevent disclosure. There was sufficient evidence that Nationwide and Harleysville knew or should have known that the information uploaded to the Box, Inc.'s site was not protected and that the information was available to anyone that had access to the internet. Harleysville failed to take any remedial action until it was too late. The Court noted that by failing to password-protect the files on the Box, Inc.

7 Saint Paul Street, 18th Floor · Baltimore, Maryland 21202 · Phone: 410-659-1300 · Toll Free: 1-888-894-7602 · Fax: 410-659-1350

site, it had done "the cyber world equivalent of leaving its claims file on a bench in the public square and telling its counsel where they can find it." In its opinion, the Court urged the commercial world to be very cautious when using "rapidly evolving" technology to share information. Businesses should be held responsible for making sure that their employees and agents are aware of how the technology works and whether they allow unwanted access by others to confidential information.

The takeaway from this case is that employees should only use technology vetted and approved by their company employer. The company should investigate the file-sharing service to make sure that it has security features and other criteria deemed appropriate in light of the confidentiality of the information. The company may also limit the number of employees that have access. The company should require password or log-in information in order to access the site. In addition, the technology used should not be a permanent storage facility for information that be confidential and privileged. The company can require that all of the information be removed from the site after a stated amount of time. Ask Jimmy jconstable@wcslaw.com.

Should You "Friend" Your Employees on Social Media?

There are different philosophies about whether supervisors should connect with employees on social media, specifically Facebook. Some managers and business leaders emphatically say, "No Way!" They don't want subordinates to know their business and they want to remain ignorant about what their employees are doing outside of work.

But for managers who accept friend requests from employees, they are invited into the personal world of that employee. After a while, the employee may forget that their boss has an insight into their personal life, photos, thoughts, "likes" and other "shares." Managers can learn helpful information that contradicts the employee's representations to his employer, for example, an employee who participates in weekend demolition derbies while also claiming to be totally disabled from a workers' compensation injury (true story) or an employee calling off sick and cannot finish a project, yet they're tagged in a beach photo that same day (another true story). Friending a subordinate can be helpful in learning the truth.

But be wary. That same employee may also be following the boss's posted or tagged events and keep tabs on their political affiliations, travels, personal expenditures, where they eat and who they associate with outside of work.

The best guidance is to determine if there are any benefits to connecting on Facebook, and be able distinguish a "Facebook Friend" from a real one. Ask Laura lrubenstein@wcslaw.com.

7 Saint Paul Street, 18th Floor · Baltimore, Maryland 21202 · Phone: 410-659-1300 · Toll Free: 1-888-894-7602 · Fax: 410-659-1350