Jurisdiction for an International Computer Fraud Lawsuit?

The proper jurisdiction for suing someone for engaging in computer fraud from a foreign country, directed at a company in the United States, is the place where the wrongfully accessed computer server is located if the defendant knew the location of the computer server.

This issue was analyzed by the United States Court of Appeals for the Second Circuit in its opinion in *MacDermid, Inc. v. Deiter*, 2012 WL 6684580 (2nd Cir. Dec. 26, 2012). MacDermid is a company located in Connecticut. Deiter was an employee of MacDermid who worked remotely from Canada. Deiter learned she was about to be terminated but, before she was actually terminated, she used her MacDermid email account to forward to her personal email account MacDermid's confidential and proprietary data files from its computer servers. The computer servers were located in Waterbury, Connecticut. Deiter was fully aware of the location of the computer servers and this fact proved to be important in the court's rationale for its decision.

MacDermid sued Deiter in the United States District Court for the District of Connecticut for a state law claims of misuse of a computer and misappropriation of trade secrets. MacDermid did not sue under the Computer Fraud and Abuse Act. Jurisdiction was based on diversity of citizenship and the Connecticut long-arm statute. Deiter filed a 12(b)(6) Motion to Dismiss claiming Connecticut did not have personal jurisdiction over her. The District Court agreed and dismissed the case. On appeal, the Second Circuit determined there was personal jurisdiction over Deiter in Connecticut based on its long-arm statute and the fact that Deiter knew MacDermid's computer servers — which she knowingly accessed — were located in Connecticut.

THE LONG-ARM STATUTE

The Connecticut long-arm statute permits the exercise of jurisdiction over anyone who uses a computer or a computer network located within the state. While Deiter was not present in Connecticut when she sent the offending emails, the way the computer system operated, in order to use her MacDermid email account and obtain the confidential and proprietary data, she had to access computer servers located in MacDermid's offices in Connecticut. The computer servers are encompassed within the definition of computers under the long-arm statute, thus, her access and use of those computers by remote means constituted a use of the computer within the state.

DUE PROCESS

After determining the long-arm statute encompassed Deiter's activities, the court next examined whether the exercise of jurisdiction over Deiter would comport with due process. This required looking at Deiter's minimum contacts with Connecticut to determine whether the maintenance of the suit would offend traditional notions of fair play and substantial justice. This step is satisfied if the defendant purposefully directed her activities at residents of the forum state and the arising injuries relate to those activities. Where a defendant knows computer servers are located in a forum state and intentionally commits computer fraud against those servers, the defendant meets this purposeful availment requirement: "Deiter purposefully availed herself of the privilege of conducting activities within Connecticut because she was aware 'of the centralization and housing of the companies' e-mail system and the storage of confidential, proprietary information and trade secrets' in Waterbury, Connecticut, and she used that email system and its Connecticut servers in retrieving and emailing confidential files." The court's rationale made it clear that Deiter's knowledge of the location of the computer servers was the linchpin of this decision.

REASONABLENESS OF EXERCISING JURISDICTION

Satisfied that due process permitted the exercise of jurisdiction, the court then looked to whether the exercise of jurisdiction was reasonable. It looked to the five Asahi Metal Factors and determined that under those factors it was reasonable, primarily because the burden for Deiter to travel there was not too great and both Connecticut and MacDermid had significant interests in resolving the matter in Connecticut. "Further, efficiency and social policies against computer-based theft are generally best served by adjudication in the state from which computer files have been misappropriated." I agree.

The rule of this case is that the proper jurisdiction for suing someone for computer fraud from a foreign country, directed at companies in the United States, is the place where the wrongfully accessed computer server is located if the person knows the location of the computer server. But, what is the takeaway?

Takeaway: If your company has people accessing its computer system from international locations, make sure they know and understand where the computer server is located. So, how about you just put this information in your company's computer use policy!

If you have any questions about computer fraud or policies for protecting your company's proprietary data, please feel free to contact me to discuss.

Shawn E. Tuma
direct: 469.635.1335
stuma@brittontuma.com