Effective Data-Use Policies Can Have "Far-Reaching" Benefits in Cracking Down on Employee Cyber Theft

Karen H Bromberg, Partner

In a decision that could make it easier for U.S. companies to enforce claims against employees who commit cyber theft from remote locations, including from beyond U.S. borders, the Second Circuit breathed life into a Connecticut lawsuit accusing a former Canada-based employee of using her home computer to steal trade secrets from her employer's Connecticut server.

Plaintiff, a Connecticut-based chemical company, employed defendant as an account representative in Canada. When the employee became aware of her impending termination, she downloaded and forwarded to her personal email account certain data files that the company alleged were confidential and proprietary. The company then sued the employee "alleging unauthorized access and misuse of a computer system and misappropriation of trade secrets." The terminated employee moved to dismiss the complaint for lack of personal jurisdiction. Although the district court held that there was no personal jurisdiction over the Canadian employee because she had not used a computer in Connecticut, the Court of Appeals disagreed. It held that jurisdiction over the defendant employee (in a state she had never visited) was established by her purposeful remote access to the Connecticut servers in retrieving and emailing confidential files.

Pivotal to the decision was the fact that the company had a clear written policy that both identified the location of its servers that stored the company's proprietary and confidential electronic data and made it a condition of employment that employees acknowledge in writing that they were not authorized to transfer such information to their personal email accounts. As the Court observed, "[m]ost Internet users, perhaps, have no idea of the location of the servers through which they send their emails. Here, however, [the company] has alleged that [the employee] knew that the email servers she used and the confidential files she misappropriated were both located in Connecticut." The Court found persuasive "that employees of [the company] and its subsidiaries are, as a condition of employment, made aware of the housing of the companies' email system and their confidential and proprietary information in Waterbury" and that the employee "agreed in writing to safeguard and to properly use [the company's] confidential information and that she was not authorized to transfer such information to a personal email account."

It is, of course, essential for companies to make sure that their employee handbooks clearly articulate an acceptable use policy for sensitive information, with clearly defined restrictions on use and warnings about the improper downloading of information from company servers (along with an acknowledgement

that employees have read and agree to the policy). However, this case makes it clear that companies with employees in distant locations may wish to go further and explicitly disclose not just the existence, but also the *location* of the servers that store confidential information, so that an employee who disregards the warnings and improperly downloads confidential information can be sued in the company's home jurisdiction – with the company, rather than the employee, enjoying the often substantial cost savings and other benefits that accompany "home field" advantage in litigation.

The case is *MacDermid, Inc. v. Deiter*, No. 11-5388-cv (2nd Cir. Dec. 26, 2012).

About the Author

Ms. Bromberg is the head of the firm's Intellectual Property and Licensing Group. She handles all aspects of intellectual property and technology law, including license agreements, technology transfer and vendor agreements, joint development and co-branding agreements, privacy policies, website terms of service, and management of IP litigation (including patent, trademark, copyright, and trade secret litigation). She was named as a New York *Super Lawyer* for Intellectual Property in 2010, 2011, and 2012.

About Cohen & Gresser

Cohen & Gresser is a boutique law firm with offices in New York and Seoul. We represent clients in complex litigation and corporate transactions throughout the world. Founded in 2002, the Firm has grown to over fifty lawyers in four practice groups: Litigation and Arbitration; Corporate Law; Intellectual Property and Licensing; and White Collar Defense, Regulatory Enforcement and Internal Investigations. Our attorneys are graduates of the nation's best law schools and have exceptional credentials. We are committed to providing the efficiency and personal service of a boutique firm and the superb quality and attention to detail that are hallmarks of the top firms where we received our training.

NEW YORK | SEOUL

www.cohengresser.com info@cohengresser.com PH: +1 212 957 7600