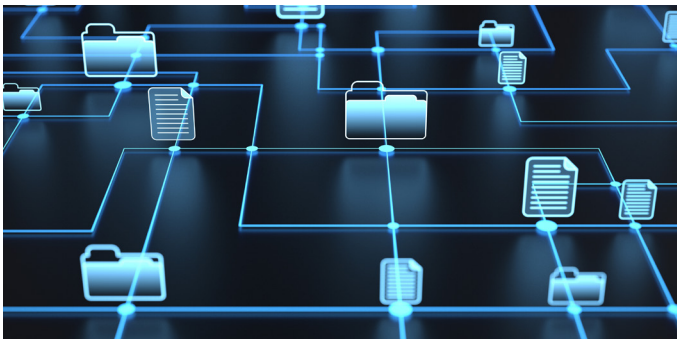
Code Nicking Cases on the Rise?

A Brief Intro

Cases involving “code nicking” — a British term for stealing—seem to be on the rise. You may not have heard much about them because these cases are often litigated in confidential arbitration proceedings. A quintessential case involves a company hiring a computer programmer from a competitor, with allegations that the programmer took confidential information upon their departure. Sometimes the programmers bring source code with them to the new employer. Other times the programmers leave with nothing tangible but their technical knowledge.

When the original employer believes its confidential information has been stolen, it may file suit asserting misappropriation of trade secrets, copyright infringement, and breach of nondisclosure agreements (NDAs), among other things. A number of questions frequently arise: What was stolen? How is the stolen data being used by the programmer with his or her new employer? Is the stolen information proprietary or just generic knowledge? What are the underlying contractual obligations of the parties? What kind of damages can be shown? Every case is unique and fact dependent. Below are some considerations.



By far the biggest issues is what information was taken (exfil) and how that information was then used (infil). Hence, conducting a proper forensic investigation is important. Once a company becomes aware that its trade secrets may be at risk, it should start an investigation and begin collecting and preserving evidence. Typically, this will include a forensic collection of data from laptops as well as mobile devices of the departing programmers. The company will also want to investigate its source code repositories, network logs, servers, and the like for unusual activity. Often, there will be evidence of exfiltration, such as, programmers emailing code to themselves, copying files onto USB devices, or FTP transfers. Discoveries of encrypted or hidden communications may indicate programmers taking efforts to conceal an exfil.

The programmers' new employer might not even hear of a potential problem until it is contacted or sued. In such instances, the respondent company will want to conduct its own forensic investigation. This may include a review of emails and communications of the suspect programmers, projects they worked on, and the potential scope of infiltration of any protected information. In the event that source code is found to have been infiltrated, it is important for the company to evaluate the nature of any code that it received. For example, is the code proprietary or open source, or is it generic with little economic value? Has the information been disclosed at trade shows or conferences? In cases involving no code exfiltration, the new employer should also investigate whether any proprietary system designs and architecture may have been brought over in a programmer's memory and could have been misappropriately used by the programmer in building new systems for the company. The new employer will benefit if it has a story showing a "normal" systems development lifecycle unaided by any misappropriation of trade secrets.

Assuming an action is filed, discovery is important. The claimant is usually required to provide a description of its trade secrets. Care must be given to that the disclosure has sufficient detail to describe the trade secret. An overly high-level description of the trade secret may be shown to be generic and publicly known, thus losing trade secret protection. This disclosure is also important to shape the scope of discovery.

The parties will also want to give consideration to damages issues. The claimant will want to show the amount of time and money it invested in developing the trade secrets and moneys derived from at-issue systems. On the other hand, the respondent may seek to show that any infiltration saved them little to no time and money.

In sum, it is important to start with knowing the facts and then establishing a good plan of attack early in the case. Early case investigation is key.

Originally published in the January 2025 issue of DBA Headnotes.

JASPAL HARE
Director
+1 214.397.1617
jaspal.hare@fticonsulting.com

01312025 | VN03992-v01