Today's GENERAL COUNSEL
SPRING 2019 VOLUME 16/NUMBER 1 TODAYSGENERALCOUNSEL.COM

Protecting Software in the Face of an Ever-Changing Workforce

By Mark P. Kesslen

The average person changes jobs 10 to 15 times during his or her career, which means many people spend five years or less with any one employer. Do you know what employees and others are bringing with them when they join your company, or what they are taking when they leave? Either can create financial and litigation risks for your organization.

Take the notorious case of Anthony Levandowski. When he left Google's Waymo division to form his own company, which was ultimately bought by Uber, he took with him 14,000 technical files related to laser-ranging LIDAR and other self-driving technologies. Waymo employees who followed Levandowski downloaded other sensitive information, including manufacturing details and supplier lists.

In early 2018 — a week into trial — Google and Uber settled, with Uber agreeing to ensure it would not use the Waymo technology and giving Waymo a 0.34 percent ownership stake in Uber. The case demonstrates that it has never been easier for employees to take trade secret and proprietary information with them from job to job. Making these situations even more precarious, companies are increasingly using consultants and contractors to handle their development work.

So what can organizations do to prevent proprietary software from going AWOL and unwanted outside technology from walking through the door uninvited? How do you know whether your new employee or contractor is introducing a prior employer's information or other third-party code into your products and services? Does your current intellectual property (IP) portfolio provide the necessary safeguards?

These risks, coupled with increasing cyber thefts, mean you need to develop new strategies to protect your IP. Tried-and-true methods may no longer be adequate.

To counter these risks, it's time to reevaluate and update existing employment agreements and trade secret policies, develop a copyright registration process (which is an evolving best practice), and reassess patent filing strategies to address the challenges created by the mobile and ever-changing workforce. This also provides you an opportunity to introduce an open source code policy to ensure that wrongly introduced code does not virally impact the value of your source code.

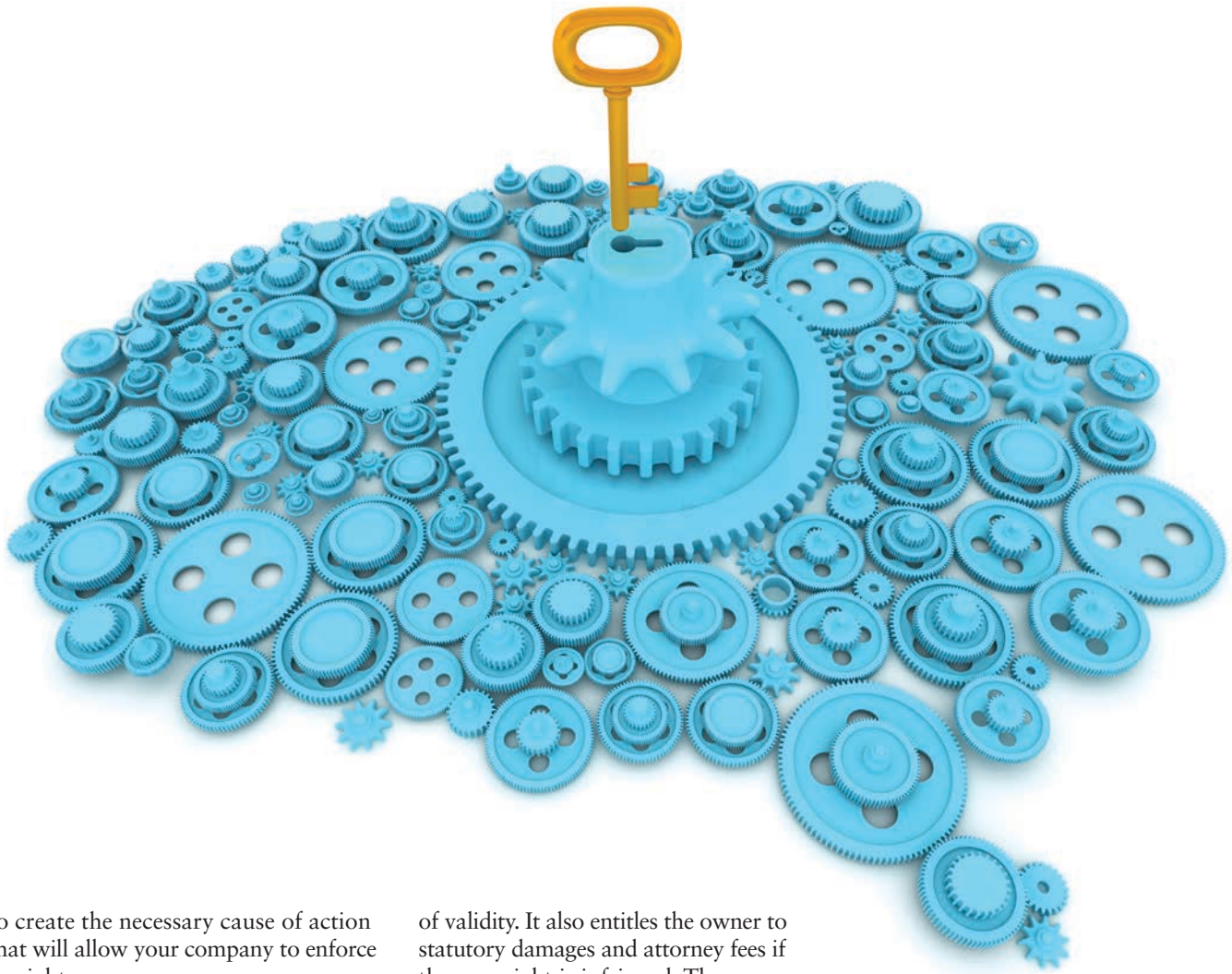
It has never been easier for employees to take trade secret and proprietary information with them from job to job.

THE NDIAA AGREEMENT

The first step occurs when a new employee joins the company or a new contractor is engaged. Many organizations overlook the simple step of using a robust non-disclosure and invention assignment agreement (NDIAA), which addresses critical expectations of the new relationship. First, it ensures that ownership of all developed work product, including associated intellectual property rights, is assigned to the company. This assignment is critical to the copyright and patent strategy described below. Second, it protects the company's confidential and trade secret information and data.

The NDIAA includes a provision that prohibits new employees or contractors from introducing a prior employer's proprietary and confidential information into the company, and requires them to confirm they are not bound by any agreement or arrangement that would conflict with their new position. It includes a provision requiring them to confirm in writing that they have purged or returned all proprietary and confidential information and removed it from all personal devices upon leaving the company. These provisions provide clear causes of action for breach if employees or contractors behave as Mr. Levandowski did.

An NDIAA works well for employees and certain contractors, but there is another security aspect to be considered. What are you doing to protect your trade secrets and code with supply chain partners who are also provided access to the company's proprietary and confidential information? Trade secret policy must address how the company contractually addresses the care and handling of this information, including from a cybersecurity perspective. It has to address the use, storage and transfer of electronic files. These protections must be in transactional documents with third parties in order



to create the necessary cause of action that will allow your company to enforce its rights.

In addition to the claim of breach of the NDIAA and requirements under the trade secret policy, a properly defined IP strategy relating to copyrights and patents will provide more leverage against the former employee or contractor. A best practice being adopted at many tech companies: File for copyright registration for developed code.

COPYRIGHT FOR ADDITIONAL PROTECTION

Although a copyright automatically exists upon creation of the code in some tangible medium, it is now prudent to file for registration with the United States Copyright Office to obtain additional benefits. This grants the owner the ability to immediately seek injunctive relief in federal court. The registration creates a record of ownership and evidence of validity. It also entitles the owner to statutory damages and attorney fees if the copyright is infringed. The copyright protects the literal and nonliteral elements of the code against an exact copy and works that are substantially similar. Therefore, when a former employee or contractor takes code and reuses it, there should be a relatively clear path to establishing copyright infringement.

Since this will likely be a new strategy for the company, internal procedures and processes should be established, depending on the software development schedule of the organization. The focus should be on new releases and material changes to existing products including source code (which is preferable to object code); graphical elements; application program interfaces; and the structure, sequence and organization of the software, including file structures, design, organization and data input formats.

Filing the application is relatively straightforward, but the Copyright Office requires the deposit of the first and last 25 pages of the software's source code unless trade secret information is incorporated. In that case, the confidential information can be redacted from the filing. The cost is the time to fill out the registration application and a filing fee, currently $55.

QUALITY, NOT QUANTITY, FOR PATENT PROTECTION

If a former employee or contractor takes core intellectual property and implements it at another organization, a claim for patent infringement may be an aggressive, necessary but expensive course of action. Much has been written about the demise

of software patents since the 2014 *Alice Corp. v. CLS Bank International* decision. However, software patents continue to be filed and issued. The key is to be smart — it's not a game of quantity, but rather of quality.

In the context of the ever-changing workforce, the question is how to build the proper portfolio to protect against ideas being stolen and then implemented in the new organization. This is not to suggest that companies should abandon their existing patent strategy. Instead, we are recommending that companies consider a change in their philosophical approach to filing software patent applications to ensure the patent portfolio is used as an efficient and effective tool to enforce their rights.

The first factor to consider in filing for patent protection is whether the technology will be incorporated into a company product. That is, does the technology represent a differentiator that provides a competitive advantage? The second factor is whether competitors want or need to use or copy the technology. If either is present, then in the context of this strategy, the detectability of the software must be assessed to determine in which of three categories the code falls. Those categories are:

- ***inherently strong detectability*** (i.e., no reverse engineering), such as code that requires unique input (configuration files, command line interface parameters, graphical user interface input), or produces unique graphical output attributable to implementing the invention, or that is described in product literature;
- ***medium detectability*** (i.e., some reverse engineering), such as code that generates network traffic or other detectable output, including some "fingerprint" features attributable to implementing the invention, which becomes weak if traffic can be end-to-end encrypted; and
- ***weak detectability*** (i.e., significant reverse engineering using a debugger), such as executable code utilizing known central processing unit (CPU) registers and system data structures, or executable code that includes "fingerprint" features only attributable to implementing the invention, modifying known system data structures or CPU registers.

If the software falls within the first or second categories, then a patent application should be pursued. This strategy focuses on core products and services that provide a competitive advantage. The detectability will enable you to more readily ascertain whether the former employee or contractor appropriated your company's valuable IP. This is not to say that patents directed to emerging and less detectable innovations should not be filed; rather, this outlines how to use patents as tools against the theft of ideas by employees and contractors. By following this approach, a company will be in a better position to associate a third party's adoption of its technology with the hiring of a former employee or contractor.

Why is open source part of this discussion? Many NDIAAs include specific guidance about the proper use and introduction of open source code, and many companies include open source code policies addressing the same points. With that said, with a mobile workforce, a rogue employee or contractor could introduce open source into a company's code base and do grave harm to the organization.

There are generally two types of open source licenses: permissive and copyleft. A permissive license imposes minimal requirements on the user of the open source, such as the obligation to include a copyright notice and various disclaimers relating to its use. The copyleft license, however, requires the code user to distribute under the same license. Therefore, a company's code base integrated with code under a copyleft license will require release of that code in source code and at no charge, which could extinguish the entire enterprise value of the code.

Some of the copyleft licenses that could cause concern include GPL, LGPL, and AGPL. Therefore, having the proper policy in place protects your intellectual property against potential bad behavior created by the mobility of the current workforce.

A rogue employee or contractor could introduce open source into a company's code base and do grave harm to the organization.

Most of the actions above, other than implementing a copyright process, are likely small or incremental changes to your organization's overall IP strategy. However, they are critical to monitoring and enforcing your rights against a mobile workforce and to helping ensure that valuable IP is not leaving your company. ■

Mark Kesslen is a partner at Lowenstein Sandler. He chairs the Intellectual Property Section of The Tech Group, and focuses his practice on advising innovators as they create businesses, launch new products, and conduct M&A and venture capital transactions. He counsels his clients on intellectual property issues, such as litigation assessments, patent scope, open source, trademarks, privacy and ownership risks.
mkesslen@lowenstein.com

Lowenstein Sandler

Mark P. Kesslen
mkesslen@lowenstein.com
T: +1 646.414.6793