

WHERE CAN BRAND OWNERS FIND THE UNDISCOVERED LEAK OF THEIR TRADE SECRETS? IT'S ACADEMIC

John H. Zacharia*

Kebharu Smith*

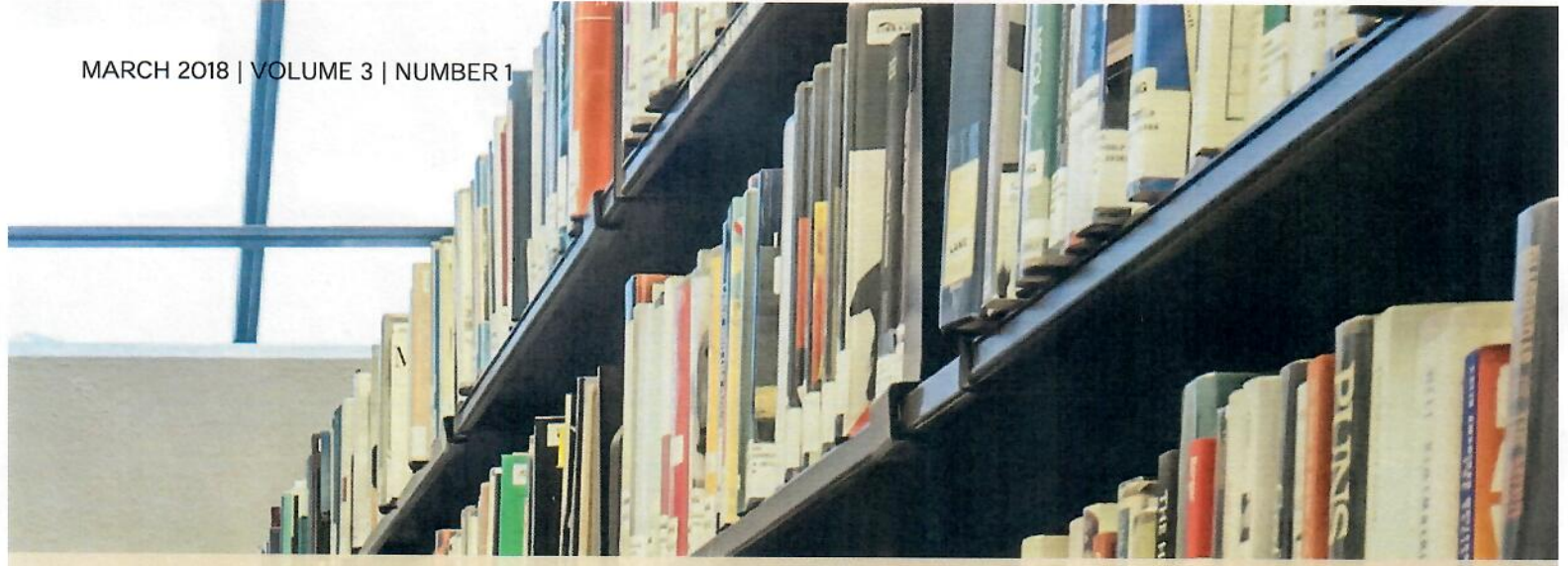
Intellectual property is among a brand owner's most valuable assets. Brand owners invest a great deal of time and resources developing their trademarks, copyrights, patents, and trade secrets. Although brand owners typically rely on their own employees to develop the original works, products, and inventions that they sell in commerce to maximize their intellectual property's value, they also rely on partnerships with universities to develop their intellectual property. This has become especially true in the development of trade secrets. Companies and universities enter research arrangements that allow company employees and academic researchers to work side-by-side in developing trade secrets. While these partnerships introduce new opportunities for companies to develop and protect trade secrets, they also introduce new ways in which trade secrets can be leaked.

Recognizing the significant threat that trade secret theft poses to brand owners and the national economy, Congress passed the Economic Espionage Act (EEA) in 1996. This authorizes the Department of Justice to investigate and prosecute trade secret theft as a federal crime. Trade secrets are the only form of intellectual property whose value derives principally from being *kept* secret from the public. Preventing the leak of trade secrets requires brand owners to take reasonable measures with their employees to keep proprietary information secret—and extend these measures to their university partners.

Here we explore (1) what reasonable measures brand owners can take to ensure protection of their trade secrets under the EEA, (2) examples of how university partnerships can lead to trade secret leaks, and (3) what reasonable measures brand owners and universities can take to ensure trade secrets they develop are protected under federal law.

THE ECONOMIC ESPIONAGE ACT

The EEA criminalizes the theft of trade secrets in two provisions. First, the EEA punishes anyone who *knowingly misappropriates* (or attempts or conspires to misappropriate) a trade secret with *the intent or knowledge* that such theft will benefit a foreign government, instrumentality, or agent (see 18 U.S.C. section 1831 (a)). Second, the EEA prohibits trade secret theft by anyone who knowingly misappropriates (or attempts or conspires to misappropriate) a trade secret for "the economic benefit of anyone other than" the trade secret owner, with the intent that the misappropriation would injure that owner, and "with the intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce" (see 18 U.S.C. section 1832 (a)).



Not all of a brand owner's proprietary information constitutes a "trade secret" under the EEA. Proprietary information is only a "trade secret" where (1) "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public" and (2) the brand owner takes "reasonable measures" to ensure that information's secrecy (see [18 U.S.C. section 1839 \(3\)](#)).

A critical consideration for brand owners who partner with universities is the EEA's requirement of *reasonable protection measures*. This requirement compels brand owners to invest in security measures to protect their trade secrets from theft. Brand owners should consider physical security measures, network and other digital security measures, employment and contractual protections, and other potential reasonable protection measures of their trade secrets. A brand owner need not take every conceivable step to protect their trade secrets. In fact, they need not even employ the best available security measures. The question of whether particular protection measures are reasonable is limited to the measures actually taken by the brand owner to protect their trade secrets, not on the other universe of measures that could have been taken.


IN PRACTICE

Before determining how to extend "reasonable measures" to their university partners, brand owners seeking to protect trade secrets should implement protection measures in locations that they exclusively control. Do they have entry checkpoints at all facilities housing the trade secret? Is there an alarm system? Are there security personnel limiting entry? Are there physical barriers preventing anyone from viewing the trade secret from outside the rooms where it is kept? Are the rooms locked? Is entry limited to employees with a key who need to know the trade secret? Does the brand owner track the entry and exit of employees into such facilities?

Having a written security policy specifically for trade secrets is helpful. Are the brand owners' employees advised of such a policy and required to sign a written acknowledgement of it? Does the company require its employees to enter into non-disclosure or confidentiality agreements regarding its trade secrets? If the trade secret is stored on a computer network, is network access limited to employees who "need to know"?

THE UNIVERSITY RISK

Brand owners who work with universities to develop trade secrets face more risks of a leak. Universities will typically be beyond the reach of security measures brand owners implement at their own facilities and computer networks. Universities also present risks that may not be addressed easily by the brand owner. Possible sources of these risks come from professional students (i.e., a company's employee who is also a student at a partner university), foreign national students, and research presentations to peer researchers. We review each of these on the next page.



PROFESSIONAL STUDENTS

In line with their business models and in the interest of maintaining an educated and competitive workforce, companies often encourage their employees to pursue an undergraduate or advanced degree. Such professional students are in a unique position of risk: they possess insider knowledge not readily available to university colleagues. Though they may understand their professional duties of confidentiality as it relates to information gleaned from their work, that is free of conflicts and owned by their employer, there may be questions about the status of those obligations when working in a communal and collaborative university setting. Universities and companies must contemplate the potential for spillage and protect themselves. Professional students and university counsel should understand that the EEA does not provide a defense for students who take the proprietary, trade secret protected information from work to the university classroom or research lab. This also applies to students who are “moonlighting” or interning for a company and leak protected university research. Both the university and the company should be vigilant and ensure that students understand their obligations as they move between the two.

CROSS-BORDER INFORMATION FLOW

The cross-border information flow of trade secrets makes them more prone to leaks and misappropriation than they have ever been. This cross-border flow does not distinguish universities from corporations. The consequences from a malicious or accidental disclosure apply equally. Once a trade secret crosses the U.S. border and is out of the university’s control, there may be no protective order or injunction to protect it. To avoid this possibility, universities could: account for their diverse student and employee population when developing their protection programs, consider the risk of border searches when faculty and students are entering foreign countries for presentations and conferences, use table-top exercises to address the ease with which devices storing trade secrets can be copied or imaged surreptitiously while traveling abroad, and calculate the risks associated with visiting professors from foreign countries. These are just a few things that trade secret owners and universities should think through as they endeavor to protect their trade secrets from leaks and misappropriation in an increasingly international academic environment.

RESEARCH PRESENTATIONS TO PEERS

Universities encourage their professors and students to present their research findings to peers. These presentations can be through webinars, live presentations, published journals, or still other formats. Universities promote research presentations for many reasons. These include highlighting advancements, receiving scientific critiques through peer review, satisfying grant obligations, or simply publishing to indicate they were first to the “scientific” finish-line. Skilled presenters who desire to protect their work and the university’s intellectual property have learned not to provide information that could result in reverse engineering or pilfering. Such threats are real and identifiable. It is not uncommon to see smart-phone users take photos of a presenter’s slides. Researchers and universities should be thoughtful in how they share their work, scrubbing data as necessary. Premature dissemination in journals or elsewhere could result in a determination that reasonable measures were not used to protect the trade secret.

Just as brand owners should take reasonable measures to protect the secrecy of their trade secrets “at home,” they also should take reasonable measures in developing trade secrets with universities. This is easier said than done. Brand owners do not have the same control over university faculty and students that they have over their own employees.

Just as brand owners should anticipate and develop “reasonable measures” to prevent leaks the theft of trade secrets from their own facilities, they should also require their partner universities to stop leaks as well. Brand owners should require universities to list names of faculty and students who will have access to jointly developed trade secrets and share that list. As they do with their own employees, they should demand that universities track when faculty or students access trade secret materials. If those materials are stored on a jointly accessible server, network access should also be limited to faculty or students who “need to know” and who log each time they access the network. Finally, brand owners should ensure that universities require individuals who work with brand owners on trade secrets to sign non-disclosure agreements regarding them.

If brand owners and universities work as cooperatively on implementing “reasonable measures” to protect trade secrets as they do to develop them, they not only maximize the value of those trade secrets, they also maximize their ability to protect them under the EEA.

* John H. Zacharia is the former Assistant Deputy Chief for Litigation of the Computer Crime and Intellectual Property Section of the United States Department of Justice’s Criminal Division. He is a graduate of the University of Virginia College of Arts and Sciences and the University of Virginia School of Law.

* Kebharu Smith is a Senior Counsel at the Computer Crime and Intellectual Property Section of the United States Department of Justice’s Criminal Division. He is a graduate of the University of North Texas and the Thurgood Marshall School of Law.

The views expressed in this article are exclusively those of the authors and do not necessarily represent the views of the U.S. Department of Justice, its components, or the United States.

The authors would like to thank Lorryn Young for her invaluable research support.