New Jersey Law Journal

VOL. 201 NO. 5 AUGUST 2, 2010 ESTABLISHED 1878

White Collar Crime

Defending the Muffin Man and Protecting Your Client From Intellectual Property Crimes

By Ernest E. Badway

Unfortunately, this article may not claim credit for the "Muffin Man" reference in the context of intellectual property crimes.

Newspaper sources used this term to describe a former food executive, who knew the process to make Thomas' English muffins "nooks and crannies" and was then barred by a judge from working for a competitor. More on his plight below, but his civil setback provides an opportunity to discuss the value — some say worth over $5 trillion — of IP rights in today's economy and the problems associated with IP protection. Further, various government agencies, including the Department of Justice ("DOJ"), have accelerated their investigations and prosecutions of these crimes.

As described above, the Muffin Man was banned from working with a competitor because he possessed trade secrets, proprietary and/or confidential information to create Thomas' English muffins despite not being subject to any contractual restrictive covenant. This court order is on appeal and a decision is expected soon. Although he is not under criminal investigation (at least, no reports), his plight highlights the criminal consequences of misappropriating another's IP rights. This article's purpose is to prepare one for the potential criminal liability, and the breadth of the government's approach to preventing and prosecuting these IP crimes.

Badway is a partner with and co-chair of both the white collar and securities industry groups at Fox Rothschild in Roseland. He is also a former SEC Enforcement attorney, and an adjunct assistant professor of law at Brooklyn Law School.

The Government's Decision-Making Process and Statutory Tools

In addition to its usual cadre of weapons, government investigators and prosecutors rely upon IP- specific criminal statutes to prosecute potential criminal defendants. Essentially, the statutory framework falls within three categories of criminal activities: (1) theft of trade secrets; (2) counterfeiting or the misappropriation of another's IP; and (3) economic espionage. Statutes include, among others, Criminal Copyright Infringement, 17 U.S.C. § 506 and 18 U.S.C. § 2319; Counterfeit and Illicit Labels, 18 U.S.C. § 2318; Bootleg Recordings, 18 U.S.C. § 2319A; Camcording of Motion Pictures, 18 U.S.C. § 2319B; Trafficking in Counterfeit Goods, 18 U.S.C. § 2320; Economic Espionage, 18 U.S.C. § 1831; and Theft of Trade Secrets, 18 U.S.C. § 1832.

However, not every IP theft results in an investigation or prosecution since several statutes have a civil component, and, potentially, a government investigator or prosecutor may defer an investigation or criminal prosecution, preferring that the matter be resolved civilly. Government investigators and prosecutors consider several factors, among others: (1) is the actor in question a repeat offender; (2) is the conduct egregious where the public health and safety are at risk; and (3) is the information concerning the questioned activity and the actor's intent timely and adequate. If these factors or a combination are present, a criminal investigation and possibly a prosecution is more likely.

Regarding trade secret thefts, sentences include imprisonment of up to 10 years, and, for an organization, a fine of up to $5 million if the individual or organization, among other things, converted or without authorization appropriated some trade secret of another. Trade secrets are

broadly viewed under the criminal statute, and cover conduct where an alleged defendant without authorization copies, duplicates or even destroys the information in question.

Similarly, substantial penalties for counterfeiting or misappropriating another's IP may include imprisonment for 3 to 20 years and fines reaching $15 million. These crimes, generally, include copyright infringement; counterfeiting products; mislabeling a product (e.g., phony Coach bags sold on Newark streets); or copying music or movies (DVD warnings). Government investigators have also found that India and China have become havens for these counterfeiters, and pharmaceutical products are increasingly targeted. Criminal investigators also noticed various counterfeit prescription and generic drugs entering the American marketplace and potentially harming consumers.

Another threat to IP rights is economic espionage, since numerous foreign interests covet American IP owned by both for profit and non-profit organizations, such as universities and research centers. New Jersey's for profit and nonprofit organizations are a prime target for attack given their importance in the pharmaceutical, defense and high-tech industries. The government perceives economic espionage as a grave national security threat, and its response includes the dedication of more resources to its prevention.

Foreign interests use many avenues to obtain American IP, and, not surprisingly, individuals and organizations, who participate in such a scheme, risk imprisonment of 15 years, or, for an organization, fines totaling $10 million. Prosecutors are particularly interested in those foreign agents who attempt to acquire classified information, non-classified defense information and network communications data. These foreign agents test Internet and computer systems to obtain this material, and are relentless in their activities according to the government.

Although potential criminal liability is enormous, individuals and organizations accused of such conduct are not without defenses. For example, those targeted may argue that the information was not protected with, among other things, a valid copyright or other protective status. Further, criminal charges are weakened if the IP was not maintained with proper care, protected from theft or treated as a valuable resource by the IP holder. That is, if the IP owner did not protect the IP from unauthorized use, government investigators, prosecutors, and, most importantly, juries will share that same feeling, and not investigate, prosecute or convict a defendant.

Cybercrime and IP Crimes

At a recent conference hosted by the NJ United States Attorney, prosecutorial and investigative representatives — DOJ, NJ Attorney General, FBI, Secret Service and ICE — stated that there is a connection between computer-Internet use and IP crimes. Many IP crimes involve unlawful access to computers and software to steal IP data and the value associated with it. Criminal prosecutors, thus, may charge both IP and cybercrimes. For example, government investigators found that many alleged IP criminal defendants engaged in identity theft, using stolen identities as the importer or exporter front to ship counterfeit goods.

For the criminal practitioner, defending these accusations has become increasingly difficult given the advances in computer technology. However, government investigators quickly point out much activity arises outside of the United States, and these actors often use many methods to disguise their conduct.

That returns us to the Muffin Man, who was accused of downloading confidential information from his former employer's computer. This activity may be a crime, especially if the computer material was damaged or destroyed, provided the other indicia discussed above were present. No one is suggesting that the Muffin Man be prosecuted since the information does not appear to have been used for profit, damaged or destroyed, but one should certainly expect that a future "Muffin Man" may not be so fortunate.

New DOJ Initiatives

N.J. United States Attorney Paul J. Fishman and his team of veteran and tech-savvy prosecutors and other government investigators are leading a rejuvenated effort to investigate and prosecute IP crimes. The N.J. United States Attorney has also reached out to lawyers, for profit and nonprofit organizations to establish a partnership so that, with early intervention, information sharing and preventative measures, IP crimes may be avoided. However, the N.J. United States Attorney is also hedging by seeking lengthy prison sentences to deter IP crimes.

Compliance and Precautionary Programs

For profit and nonprofit organizations should also establish compliance and response programs to monitor and protect IP.

The organization must first identify the "crown jewels of its operation," that is, the organization should identify its critical IP. A defense lawyer may, however, point out an organization's failure to identify critical IP if the client faces an IP theft prosecution.

The organization must also establish written procedures outlining its IP protections and response to threats. Although there are different security measures, the organization must adapt to changing events, where, for example, card access and secure rooms may work for some IP types while password encryption or nondisclosure contracts may work for others. Further, special computer systems procedures to prevent unauthorized use are imperative.

Additionally, these IP theft response procedures should focus on containment, assessing damage and preserving the evidence of the alleged crime. Such evidence must exist if the organization wishes to prosecute or to learn from the events causing the breach or theft.

Any set of procedures should also contain a system of "checks and balances" to avoid providing one individual or group with "God Access," unless, of course, the access is critical to the organization. However, such situations are rare in modern organizations, and coordination with direct communication between various groups in the organization, including IT, is a better practice.

In sum, the government is devoting significant resources to investigate and prosecute IP crimes to protect the American economy and national security. Individuals, for profit and nonprofit organizations should expect this trend to continue, and, thus, prepare protective measures to either avoid or ameliorate potential criminal activity. ■