An ALM Publication
CORPORATE COUNSEL
The Business Magazine for In-House Counsel
corpcounsel.com | May 2015

CYBERSECURITY'S WEAPON OF CHOICE

Companies are advised to use their IP rights to counter cyberthreats.

BY CLARK W. LACKERT

BRUCE MACPHERSON

ALMOST EVERY DAY WE HEAR MEDIA stories on cybersecurity: from North Korea, to credit card database breaches, to counterfeit goods sold in online autions, to fraudulent copycat websites. We also hear about the weapons used to attack such threats, including improved software and infrastructure, increased monitoring, better training and tighter oversight. What has not been explored are the existing remedies that intellectual property rights—particularly trademarks and copyrights—can provide to improve overall corporate cybersecurity.

WHY INTELLECTUAL PROPERTY?

Many forms of cyberthreats are perpetrated through various guises, including misleading domain names and email addresses (including "phishing"—an email fraud scam in which the criminal sends out a fake email in order to obtain personal information from the recipient). There are also online auction sales of counterfeit or infringing merchandise, copycat websites and distribution of malware and viruses through misleading email. All of these threats involve IP infringement. Intellectual property rights, most importantly trademarks and copyrights, exist in the online world as they do in the brick and mortar world. In fact, most U.S. Customs seizures come from IP infringements as opposed to narcotics or weapons or other illegal products commonly smuggled across borders.

Conversely, there are many ways to use IP to fight cybercrime and cyberthreats. The three most efficient and cost-effective are: (1) online domain name arbitration under the ICANN Uniform Dispute Resolution Policy (UDRP); (2) website take-down procedures under the Digital Millennium Copyright Act (DMCA) in the U.S., or similar procedures in other countries; and (3) IP infringement policies that permit swift removal of infringing online auctions (e.g., the Verified Rights Objection (VeRO) in the eBay platform, and many others internationally). If these infringements involve criminal violations, government authorities may become involved to investigate these IP cybercrimes.

DOMAIN NAMES

One of the most potent threats to cybersecurity is pirated domain names. These names are commonly used to sell counterfeit or infringing merchandise, to go on a "phishing" expedition to collect sensitive personal information and to infect computers with malware or viruses. Commercial watch services are available to provide periodic reports on domain names that may be pirated, which are then reviewed by IP attorneys. For example, your company may have registered its brand in the ".com" registry, but not in the ".org" registry, and not in country code registries such as ".de," or in any of the new registries such as ".direct."

All of these open registries may be subject to a pirated registration of your brand, or variations on your brand name. If they have been pirated, a private investigation would be warranted in the interests of examining the nature, length and scope of the infringement. Thereafter, a cease and desist letter may be sent.

Additionally, arbitration forums such as the Uniform Dispute Resolution Policy for generic top-level domains or local equivalents (like the policy maintained by the Chinese Internet Network Information Centre for the ".cn" and Chinese provincial abbreviation extensions) provide cost-effective options for resolution. However, such options may be appropriate only for severe cases of domain name infringement. If both parties have legal rights in the underlying trademark for the domain name, court action may be necessary.

Stronger legal action may be more appropriate for instances involving counterfeit goods and monetary gain. In such cases it is advisable to seek remedies through civil or criminal authorities without written notice to the counterfeiter. Many countries have statutes pertaining to online infringement, such as the U.S. Anticybersquatting Consumer Protection Act, which incorporate injunctions, fines and imprisonment. Other countries have recognized the need for a scope of protection for registered trademarks that includes virtually any form of the registered mark on the Internet, including domain names, keywords or websites.

Accordingly, many pirated domain names may be the subject of some form of fast-track arbitration if the infringing name constitutes cybersquatting. The usual remedies are cancellation or transfer of the infringing domain name. If the domain name becomes involved in other counterfeiting or infringing activity, other remedies (e.g., injunctions or damages) may be sought.


CLARK W. LACKERT

Companies have focused on software and infrastructure to counter attacks. Sometimes their best weapons are **COPYRIGHTS AND TRADEMARKS.**

WEBSITES

Apart from pirated domain names, copycat websites are a serious threat to cybersecurity. These websites can disseminate false information, collect private information from participants for use by the infringer elsewhere and spread malware once contacted. As with domain names, websites in the U.S. and abroad can be policed through various local and international legal vehicles.

Two avenues of defense are available: the trademark route and the copyright route (both can be used together). Trademark jurisdiction and venue against infringers are properly found in those countries where there is some "commercial effect," and an enforcement option is available in many. For example, the Chinese State Administration for Industry and Commerce enacted Interim Measures for the Trading of Commodities and Services through the Internet for the purpose of regulating online commerce.

Apart from trademark actions, copyright is also a powerful weapon. If a copyrighted package or website is copied, the trademark owner may claim infringement of copyright, and many countries provide notice and takedown vehicles. In fact, copyright protection can be stronger than trademark protection in certain cases. For example, in the United States the DMCA provides an efficient notice and takedown provision. Essentially, the copyright owner serves notice on the infringer to remove the infringing content. The notice must be accompanied by specifics regarding the content and the complainant's statement that the notice is being sent in good faith. Other jurisdictions such as the European Union maintain similar procedures.

ONLINE AUCTION PLATFORMS

Perhaps the most attention has been paid to online auction platforms, since online sales of counterfeit goods undermines the legitimate product quality, funds illegal activity and may be used by infringers to obtain confidential corporate and personal information to help them infiltrate corporate firewalls. The question most commonly raised is whether such platforms operate as innocent intermediaries, merely providing platforms for sales of merchandise, or whether such entities are contributory infringers that should be responsible for monitoring the nature of transactions conducted using their websites. There is no clear consensus.

In *Tiffany v. eBay*, the U.S. Court of Appeals for the Second Circuit applied an analysis to establish the extent to which an online platform has actual or constructive knowledge of infringements or is operating under the guise of "willful blindness." The appeals court decided that eBay should not be held liable for infringing activity, since it had undertaken reasonable safeguards to protect the brand owner's rights, including an infringement notification and takedown program. It was determined that such procedures placed the burden of policing on the trademark owner, and that specific knowledge of infringing activity would be necessary in order to hold eBay liable. Similar approaches have been taken in other countries.

Aside from litigation, many auction platforms maintain notice and takedown procedures: e.g., eBay's Verified Rights Owner (VeRO) program and Alibaba's IP Protection System (AIPPS) program. Although these procedures can be cumbersome, they can prove effective and inexpensive tools for fighting online sales of counterfeits and infringements. As a general principle, online platforms may be liable to the extent that they participate in the activity.

Moreover, if activity such as online fraud is involved, criminal authorities may take action. Consideration of these other IP rights is important because they may strengthen defensive measures.

THE BOTTOM LINE

Intellectual property rights are overlooked weapons for companies and individuals trying to enhance cybersecurity. An effective use of patents and trademarks, launched on a global basis, can make internal and external digital platforms more secure in a cost-effective and efficient manner. Thus, they can be seen as having two functions, namely, the basic IP function of protecting valuable intangible corporate assets, and, at the same time, protecting the corporation or individual against several of the most effective cyberattacks.

Clark W. Lackert is a partner in the New York office of Reed Smith. He specializes in U.S. and international intellectual property law as it relates to the Internet, ICANN domain names, anticounterfeiting and enforcement. He can be reached at clackert@reedsmith.com.

Reprinted with permission from the May 2015 edition of CORPORATE COUNSEL © 2015 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 016-04-15-05