Bloomberg BNA

Electronic Commerce & Law Report™

DOMAIN NAMES

The authors recount the recent spate of domain name seizures by governments seeking to enforce laws on pharmaceutical sales, online gambling, and intellectual property. They offer suggestions for how online businesses might respond to domain name seizures, and they discuss the prospect of federal legislation—which is still in the drafting stage—that might give domain name registrants notice and an opportunity to be heard prior to a domain name seizure.

Domain Name Seizures: A Primer on the Government's Hot New Weapon Against Internet Businesses

By David B. Deitch and Timothy B. Hyland

You are sitting at your desk early on a Monday morning with a fresh cup of coffee when the phone rings. You pick it up to hear a frantic client, the president of an internet-based business headquartered outside of the United States, telling you that she has just learned that U.S. law enforcement authorities have seized the company's domain names based on the allegation that the company's business transactions have violated U.S. law. The client is panicked because all of her business's interaction with customers takes place online, and none of it can happen with the domain names seized.

David B. Deitch is a member of Ifrah Law PLLC in Washington, D.C. A highly experienced litigator, he represents people charged with a wide variety of business crimes. As a prosecutor, he tried well over 100 felony cases to juries. He also has a broad practice in commercial litigation. Timothy B. Hyland, a member of Ifrah Law PLLC, frequently represents companies in domain name disputes. He handled Network Solutions Inc. v. Umbro International, one of the first cases to be litigated. his work in technology law includes disputes concerning cybersquatting, the Digital Millennium Copyright act, and data piracy.

More and more attorneys in the United States with business clients are receiving phone calls like this one. An ever-increasing number of businesses execute more and more of their transactions online, and an ever-increasing number of businesses have no traditional brick and mortar locations—existing, at least with respect to customer interaction, solely in the form of an internet website. For those businesses in particular, the safety, security and continued reliable operation of that website, and the ability of customers to access it, are critical to their continued existence.

For internet-based businesses, the rapidly growing law enforcement use of domain name seizures is an alarming phenomenon. In an increasingly broad spectrum of contexts, the seizure of domain names at the time when an indictment or complaint is filed (or unsealed) has become as common as the execution of search warrants or the seizure of bank accounts.

The purpose of this paper is to provide practitioners who represent internet businesses with an understanding of the basis on which the government seizes domain names, the bases on which it does so, and the responses by counsel that may ultimately save the internet business from failure during the pendency of criminal charges or civil enforcement proceedings. To that end, we first review some of the recent uses of domain seizures by law enforcement, then consider the technical background relating to domain names as it relates to such seizures, and finally describe some approaches

 ISSN 1098-5190

that counsel may put to use in response to a domain name seizure.

Recent History of Domain Name Seizures

The use of domain name seizures by law enforcement has become increasingly common. In pursuing domain names, government regulators and prosecutors rely not only on general principles of criminal and forfeiture law, but also on more narrowly focused laws of recent vintage that specifically authorize the government to do so.

Internet Gambling

In the area of internet gambling, the most prominent domain name seizure occurred on April 15, 2011—a date to which people in that industry refer as ''Black Friday.'' On that date, the United States government seized the internet domain names for Full Tilt Poker, Poker Stars and Absolute Poker – at that point, the largest online poker websites in the world.[1] The seizure of those domain names, which the government based upon both the general criminal forfeiture statute (18 U.S.C. § 981) and the Illegal Gambling Business Act (''IGBA'') (18 U.S.C. § 1955(d)), effectively and instantly shuttered these multi-million dollar businesses, creating enormous leverage against the affected parties. Because the operation of these websites outside of the United States did not violate U.S. law, counsel for these companies were able to negotiate within a short time with U.S. prosecutors an agreement that permitted the domain names to be redirected to their websites to resume operation with technological restrictions that barred consumers in the United States from accessing the website.

While most domain name seizures have been executed by the federal government, the Commonwealth of Kentucky has been in litigation for well over 3 years relating to its seizure of over a hundred domain names—including the Full Tilt Poker and Poker Stars websites—on the asserted ground that the domain names constituted ''gambling devices'' under Kentucky law.

Online Pharmaceutical Sales

The seizure of domain names is by no means limited to law enforcement against illegal gambling. Another area in which U.S. federal agencies have used domain name seizures is in enforcement efforts relating to pharmaceutical products sold from outside the United States.

For example, in early October of this year, the U.S. Food and Drug Administration sought to shut down more than 3,700 web addresses owned by Canada Drugs, an online business that has been selling prescription drugs for a decade. The domain name seizure arose from allegations that Canada Drugs had knowingly distributed a counterfeit version of a cancer-fighting drug as well as foreign versions of erectile dysfunction medicines. Notwithstanding the fact that the seizures were based on conduct that the government alleged to constitute violations of law, the government has not yet filed any complaint or other case arising from that conduct. These domain name seizures were part of a law enforcement initiative dubbed, ''Operation Bitter Pill,'' but that program was part of a global effort against online pharmaceutical companies called ''Operation Pangea V'' that included numerous law enforcement agencies.

Online Piracy and Copyright Violations

Yet another area in which domain name seizures have been effected is in cases involving copyright violations and online piracy. One unique feature of these seizures is that they have proceeded pursuant to specific legislative authorization in the form of the PRO-IP Act of 2008. That statute (formally, the ''Prioritizing Resources and Organization for Intellectual Property Act) increased both civil and criminal penalties for trademark, patent and copyright infringement, and also provided for *ex parte* seizure of domain names by the government based on claims of copyright or trademark infringement.

There was significant publicity in June 2012, when, based on this specific authorization, federal prosecutors seized the domain name registered by Megaupload as part of a criminal prosecution of the company and some of its personnel for copyright violations. But the Megaupload seizure was actually just one of many hundreds of domain name seizures effected by the government as part of several stages of ''Operation In Our Sites''—a program of enforcement against website operators alleged to be committing criminal copyright violations. Some of these operators were alleged to be distributing movies and television programs; others, including a number seized by the government in recent action in the District of Maryland, were claimed to be involved in the distribution of counterfeit brand name products.

Seizures associated with claims of criminal copyright and trademark violations have met with mixed success—some of which is driven by the fact that the United States's decision to criminalize copyright violations distinguishes it from most other countries. In part for this reason, the enforcement proceedings related to Megaupload have stalled because of a wide variety of obstacles to the extradition of Megaupload's principal, Kim Dotcom, and there has been significant criticism that the government should not be permitted to continue its domain name seizure when it is unable to go forward with the associated enforcement proceedings. There have other misfirings that received less publicity. For example, in November 2010, the government seized the domain name <dajaz1.com>, which blogged about music and hosted some downloads. After holding the domain name for a full year – during which there were press reports that many of the songs on the site had been provided to the operator by music industry executives – the government vacated its seizure. Likewise, <rojadirecta.com> and other Spanish websites seized in January 2011 were returned in August 2012.

In another instance in February 2011, federal law enforcement seized 10 domain names that it alleged were being used for distribution of child pornography, but in the process it mistakenly blocked 84,000 websites not accused of any such conduct. Visitors to those websites, many of which were personal sites or sites of small businesses, were greeted with a banner stating that the domain name had been seized based on allegations of child pornography. Obviously, this accusation was ex-

[1] A copy of the warrant issued for the seizure of the Full Tilt Poker domain names is available at http://pub.bna.com/eclr/pokerstars_warrant.pdf.

  ECLR ISSN 1098-5190

tremely embarrassing for the innocent domain name users whose sites were blocked in error.

Technical Aspects of Domain Name Seizures

The theory upon which the government relies to seize a domain name is that the domain name is an asset that the subject company has used (or is using) to violate the law. In this sense, domain name seizures are not that different from the seizure of a car, boat or apartment used to sell drugs, though some courts have called into question whether domain names are, in fact, property that may be seized. *See*, *e.g.*, *Network Solutions, Inc. v. Umbro Int'l, Inc.*, 529 S.E.2d 80 (Sup. Ct. Va. Apr. 21, 2000) (finding that, while domain name is an intangible asset, that asset is limited to contract rights held under the contract between the domain name holder and the registrar, which are not assets subject to seizure under Virginia's statutory garnishment procedure). *See also e.g.*, *Dorer v. Arel*, 60 F. Supp. 2d 558 (E.D. Va. 1999) (denying plaintiff's request to dispose of domain name by sheriff's sale, and suggesting in dicta that a domain name is not personal property subject to judicial lien but instead represents trademark and contract rights); *Zurakov v. Register.com, Inc.*, 760 N.Y.S.2d 13 (N.Y. App. Div. 2003) (a domain name is merely a contract right, not a tangible asset).

Even assuming that domain names are assets, the seizure of such assets is also different from the seizure of a car, boat or apartment in that the control of the assets lies in the hands of other parties. It is this circumstance that forms part of the reason why the government has become enamored with domain name seizures. An understanding of how this makes it easy for the government to seize a domain name requires an explanation of some of the technical aspects of how domain names work – particularly, the role of registries and registrars.

A registry—run by companies such as VeriSign, Affilias, Neustar and Public Interest Registry—is essentially a database of all domain names within a given top-level domain (such as .com, .net, or .mobi). A registry contains certain information associated with each domain name. In the case of what is called a ''thick registry,'' the registry includes the Internet Protocol (IP) address associated with the domain name. In the case of a ''thin registry,'' the only information held by the registry is the identity of the registrar through whom the domain name was registered; the associated IP address is recorded only by the registrar. A registrar, on the other hand, is one of the thousands of companies which facilitate the registration of second-level domain names, such as <brand.com>.

Nearly all of the current top-level domains have U.S.-based registries.[2] For example, the registries for the .com top level domain (which is, by far, the most populous one) and the .net top level domain are operated by VeriSign, located in Reston, Virginia. Public Interest Registry, which operates the .org top level domain, is also located in Reston, Virginia. The non-country code registries that are located outside of the United States are largely limited to little-used top level domains, such as .asia (located in Hong Kong), .cat (located in Spain), .info and .mobi (both located in Ireland), .post (located in Switzerland) and .tel (located in England). Even in the case of so-called ''country code'' top level domains (such as .ca for Canada or .au for Australia), a number of country code top level domains contract with U.S.-based companies to operate their registry.[3]

Many of the most popular registrars—such as Godaddy, Network Solutions, Register.com—for domain names are also located here in the United States. But there is a growing number of domain name registrars in other countries.

The geographic location of the registry and registrar associated with a domain name is key to the ability of the U.S. government to seize a domain name. A government agency that obtains a seizure warrant may seize a domain name through either the registry or registrar as long as one is based in the United States. Thus, the only circumstance in which the government may be unable to seize a domain name is the rare situation in which both the registry and the registrar are located overseas (and even that is no guarantee against seizure).

In addition, legislation relating to online copyright protection—particularly, Title II of the Digital Millennium Copyright Act, known as the Online Copyright Infringement Liability Limitation Act (OCILLA)—gives companies that operate registries or act as registrars little or no incentive to fight a government seizure of a customer's domain name. The DCMA created a specific safe harbor for service providers, codified at Title 17, United States Code section 512(c), granting them (and ISPs) immunity for copyright violations as long as they have no actual knowledge of the allegedly infringing content, and as long as they act promptly to remove that content when they are notified of the alleged infringement. Thus, in most cases, the safer course for these companies, to ensure that they are not exposed to liability for contributory copyright infringement, is to comply with government requests to shut down websites under their control. What this means, however, is that a company's domain name is an asset that is vulnerable to government seizure because it is in the control of one or more companies with little or no incentive to fight the government's seizure.

Responses to Domain Name Seizures

Given the ease with which law enforcement can seize domain names, the likelihood in cases involving internet businesses is that internet-based businesses charged with crimes will also face potentially disastrous website shut-downs. There are somewhat limited options for dealing with these situations, and, from a business perspective, time may be of the essence. It may be difficult for a company that conducts most of its business on the internet to move its traffic to a website resolving from a different domain name without giving up the accumulated good will and brand recognition that sustain its success. Moreover, the ability of a putative defendant to challenge a domain name seizure through litigation is largely untested, and is ultimately likely to be time-consuming. Thus, part of the triage for such

[2] A full listing of top level domain registries may be found on the website for the Internet Corporation for Assigned Names and Numbers (ICANN) at www.icann.org/en/resources/registries/listing .

[3] The current process creating numerous new top-level domains is likely to result in a much larger number of top level domains whose registries are outside of the United States. *See* http://archive.icann.org/en/topics/new-gtlds/factsheet-new-gtld-program-oct09-en.pdf.

businesses will involve creative approaches to keep websites open.

The key issue in this regard is the extent to which the business in question has website operations that are not implicated by the underlying allegations of infringement. For example, after the file-swapping service, Napster, was preliminarily enjoined from its operations after being sued by music recording businesses, it was permitted to resume its operations that did not implicate the conduct that formed the basis for the allegations leveled against it in the litigation. In Napster's case, that victory was a Pyrrhic one: From a business perspective, Napster was unable to operate successfully on that limited basis.

In many cases, however, the conduct that forms the basis for law enforcement or other litigation activity is only a portion of the business, and the business could operate successfully based solely on that non-violative conduct. The recent criminal and civil cases against Full Tilt Poker, PokerStars and Absolute Poker are a good example. At the same time that enforcement authorities unsealed indictments and seized massive amounts of money, they also seized domain names for these internet-based businesses. The result of the seizure of the domain names was closure of these websites not only for U.S.-based customers, but also for customers from all around the world. It was indisputable that the interactions between these websites and users outside of the United States was beyond the control or jurisdiction of U.S. law. Yet, the seizure of the domain names of these poker companies would, if no action were taken, deprive the companies of income from overseas during the pendency of the criminal and forfeiture proceedings. Put simply, <fulltiltpoker.com> resolved to the same website whether the user was in the United Kingdom or the United States. In the case of Full Tilt and PokerStars, counsel were able to negotiate an agreement with government attorneys that permitted the use of the domain names and the corresponding websites after only four days. In that case, the solution was to institute ''geo-blocking''—technology that barred users from U.S.-based IP addresses from accessing the play for money parts of the websites, but leaving the company able to continue to offer real money poker to users from outside the United States. The companies also agreed to place a banner on the websites that would appear to U.S. users stating that the domain names had been seized, and to appoint a monitor to confirm compliance with the agreement. The companies were required to waive their challenges to the seizure during the pendency of the agreement, but the result of the agreement was the preservation of the ability of the companies to continue conducting non-U.S.-facing business.

One can easily conceive of similar situations in which there are portions of the activity conducted on a website that are unquestionably outside the scope of alleged wrongdoing that formed the basis for the government's domain name seizure. In such situations, as long as there is a feasible method to ensure that the allegedly violative conduct is excluded, the government should be amenable to permitting use of the domain name while the parties litigate the underlying claims.

Of course, in some cases—either because of the nature of the website's business or intransigence on the part of the government—there may be no opportunity to negotiate an arrangement permitting the use of the previously seized domain name. In those circumstances, the options are somewhat limited and are likely time-consuming

Assuming the domain names have been seized in anticipation of a civil forfeiture proceeding, the assertion of a claim in such a proceeding and all that follows would likely track according to the rules applicable to forfeiture proceedings involving assets other than domain names. In this regard, the available defenses would likely include the assertion that no crime ever occurred, that the government lacked probable cause, or that the property is not closely enough connected to the alleged crime to be considered an instrumentality or proceeds. In addition, a domain registrant may argue that the domain name is merely a contract right not subject to forfeiture.

The historical trend has been toward the use of civil forfeiture rather than criminal forfeiture. If, nonetheless, the government seeks to forfeit a domain name as part of a criminal proceeding, the ultimate question of forfeiture would almost unquestionably be deferred until after the resolution of the underlying criminal charges. There do not appear to be any reported cases testing the application of Rule 41 of the Federal Rules of Criminal Procedure but, if a domain name were seized during an investigation and no charges were filed, it may be that a domain name registrant could seek return of the domain name through a motion for return of property pursuant to Rule 41(g). On the one hand, the government is likely to oppose such a motion vigorously if it believes that the putative defendant is using the domain name to continue to violate U.S. law. On the other hand, the hardship that seizure of the domain name may pose to an internet business fits squarely with cases in which courts have required the return of property—usually things like documents, files and computer equipment—where the continued withholding of those items cause an extreme hardship to a business not formally charged with any crime. The intangible quality of the domain name makes such a motion seem odd, but if the domain name is an asset subject to seizure, it certain follows that it should also be subject to release. Because of the nature of most cases involving domain name seizures—usually arising from the claim that the website corresponding to the domain name was continuing to conduct illegal activity—there is little or no case law on these issues.

The Future of Domain Name Seizures

The seizure of domain names—particularly in the context of alleged copyright violations—has met with significant criticism. Much of that criticism proceeds from the assertion that the *ex parte* seizure of domain names, which results in the silencing of the speech on the related websites, is a violation of the First Amendment guarantee of free speech in that it occurs without any of the safeguards that are usually required for such restrictive action by the government.

In part for this reason, one recent reaction to the proliferation of domain name seizures has been increased interest on Capitol Hill in reigning in the ability of federal law enforcement to effect domain name seizures. Rep. Zoe Lofgren has been the most prominent critic of the way in which particularly U.S. Immigration and Customs Enforcement (ICE) has executed its authorization to make such seizures. Media reports suggest that

  ECLR ISSN 1098-5190

Rep. Lofgren is drafting legislation that would require notice and an opportunity to be heard before domain names could be seized.

If such legislation were to be enacted, it would clearly present a more favorable situation for registrants whose domain names are seized by the government. Rather than being force to seek the return of domain names in the government's hands—and to seek the reopening of the associated websites—registrants will be entitled to an adversarial hearing on whether the government has an adequate basis for seizure. Given the stakes for internet businesses, such a pre-seizure hearing better meets the dictates of fairness and justice than the government's current program of *ex parte* seizures.