

**MARKMONITOR COMMENT IN RESPONSE TO A REQUEST FOR SUBMISSIONS FROM THE  
OFFICE OF THE U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR (IPEC)  
RELATED TO FORMULATION OF A NEW 3-YEAR, JOINT STRATEGIC PLAN**

**Introduction**

MarkMonitor, part of Clarivate Analytics, appreciates the opportunity to provide comments and offer input to the Office of the U.S. Intellectual Property Enforcement Coordinator (IPEC) as IPEC prepares to develop its new 3-year Joint Strategic Plan on Intellectual Property Enforcement (the “Joint Strategic Plan”).

Since its founding in 1999, MarkMonitor has offered domain name management and brand protection services to hundreds of the leading and most recognized companies and consumer brands in the world. Last year, MarkMonitor sent 46,000 email enforcements to website owners who were infringing its clients’ trademarks or counterfeiting their brands. MarkMonitor also reported more than 800 counterfeit listings to e-commerce marketplaces. For its anti-fraud work, MarkMonitor sent 184,000 enforcement notices to website hosts and domain name registrars and registries requesting suspension of phishing and other fraud schemes. MarkMonitor scans and detects hundreds of counterfeit websites each week. Suspending websites that sell counterfeit goods and pirated content helps erode funding for organized crime, terrorism, distribution of illegal medications, and sex trafficking, as well as enhancing consumers’ overall trust and safety in the Internet.

**Recent Survey on the Brand Protection Problem**

Recently, MarkMonitor commissioned an independent survey of 600 marketing decision makers from a cross section of industries in the U.S., U.K., Germany, France and Italy and asked them about their experience and opinions regarding the future of brand protection. A copy of those survey results are included with this comment, and MarkMonitor encourages IPEC to read and consider the content in that report.

The survey reveals that respondents believe counterfeit infringement has increased more than 60% over the last year based upon the number of enforcement actions now being required. Many also believe brand protection threats have new sources and are emerging from social media platforms, online marketplaces, the dark web, and mobile apps. IPEC should encourage social media platforms and mobile apps, in particular, to implement better processes for receiving and acting on reports of infringement in order to combat the increasing threats. MarkMonitor urges IPEC to collaborate with brand protection service companies, like MarkMonitor, to use their data and information to understand better the nature of these new

forms of abuse and to help inform trade representatives, law enforcement, and other government officials of where to focus resources that will help protect brand owners and consumers.

### **The Importance of Continued Public and Private Sector Cooperation**

For the last several years, MarkMonitor has been an active participant in public/private sector partnerships that aim to curb intellectual property infringement in the United States and abroad. For example, in 2018 MarkMonitor participated in [Operation “Pangea,”](#) a partnership with European law enforcement aimed at suspending domain names used by rogue and illegal online pharmacies. MarkMonitor provided Interpol with more than 800 websites it had identified as being distributors of illegal pharmaceuticals, which were suspended en masse, sending a message to pharmaceutical counterfeiters around the globe. This year MarkMonitor also participated in [Operation “In-Our-Sites,”](#) a partnership with Europol targeting websites that sell counterfeit goods and pirated copyrighted content. Once again MarkMonitor provided an extensive list of counterfeit websites to Europol which resulted in hundreds of domain name suspensions. Similar public/private sector law enforcement initiatives must be supported and encouraged, if not led, by IPEC and other federal agencies in the U.S., which would be readily supported by industry trade groups such as the Automotive Anti-Counterfeiting Council ([A2C2](#)) and the International Anti-Counterfeiting Coalition ([IACC](#)) whose vital work with law enforcement agencies already helps reduce the number of dangerous counterfeited products in today’s marketplaces. These groups, as well as others, benefit from IPEC’s continued support and inclusion in the Joint Strategic Plan.

Finally, MarkMonitor wishes to draw IPEC’s attention to the resources and talents of academic institutions and scholars who are doing research into the future of intellectual property protection. One example is Michigan State University’s Center for Anti-Counterfeiting and Product ([A-CAPP](#)). This research and scholastic program provides valuable research data and information that can help shape the Joint Strategic Plan. MarkMonitor recently partnered with A-CAPP to research where the proceeds of counterfeit purchases go, and we hope to share the results of this research with IPEC and the public in the coming months ahead.

### **Improvement of Data and Information Sharing**

While private sector partnerships with federal law enforcement has resulted in the successful removal of infringing websites and counterfeit goods, more data and information from law enforcement is needed in further strengthening these efforts. For example, in many of the operations identified above, brand owners and brand protection companies are not given any

data on the number of websites shutdown, domain names suspended or delisted, or pirated content removed. Because this important data is not shared with private sector partners, it's difficult to know the effectiveness and impact these operations are having on the infringement problem. If federal law enforcement agencies would share more details and data related to the success of their operations, more cooperation and collaboration could be fostered. As called for in the FY 2017-2019 Joint Strategic Plan, MarkMonitor urges IPEC to encourage U.S. federal agencies to contribute more data and information to its private sector partners in order to strengthen these partnerships and make an even greater impact.

### **GDPR, WHOIS, and the Impact on Brand Protection**

When the European General Data Protection Regulation (GDPR) became effective, many domain name registries and registrars moved to redact domain ownership information from their public WHOIS record. Historically, domain name registrant information in WHOIS has been used by intellectual property owners, cybersecurity experts, brand protection service providers, and law enforcement to identify, contact, and prosecute individuals who publish websites that sell counterfeit goods and pirate copyrighted movies, TV shows, photographs, and music. MarkMonitor has been tracking the impact of redacted WHOIS on our anti-counterfeit, anti-piracy, and anti-fraud services since GDPR went into effect on May 25th, and the impacts have been significant.

From the data we have collected over the previous four months since GDPR went into effect, only 9% of WHOIS records searched have un-redacted registrant information publicly available after GDPR. Most registrars, however, have denied or ignored requests for registrant information. Of more than 350 requests made to more than 70 registrars, registrars have responded with WHOIS data only 26% of the time. 74% of the requests to identify the alleged bad actor were either ignored (no response to the request was acknowledged) or denied.

With access to domain name ownership information severely inhibited, brand owners have had to adjust their enforcement strategies and processes to adapt to a post-GDPR world. Since GDPR went into effect, MarkMonitor has witnessed a 19% loss of operational efficiency when it comes to performing brand enforcement activities. Without reliable access to WHOIS data, it takes more time for IP owners and their brand protection companies to find reliable contact data to enable sending takedown notices to website owners.

MarkMonitor urges IPEC to stay informed about ICANN's Expedited Policy Development Process (EPDP) that will establish the future policy for registrant data publication and, most importantly, ongoing multistakeholder efforts to develop a unified accreditation and access policy for WHOIS data. Such a policy will allow intellectual property owners and their brand protection advisors, law enforcement, and other parties with a legitimate interest in accessing

the registrant data the ability to do so in order to carry out enforcement activities. MarkMonitor commends the U.S. government for the good work already done and ongoing as a leading voice in ICANN's Governmental Advisory Committee (GAC), and regular contact and exchange of information with David Redl at the National Telecommunications and Information Administration of the Department of Commerce should be a critical part of the Joint Strategic Plan going forward.

## **Conclusion**

Protection of intellectual property is essential for maintaining consumer trust and safety and also the credibility of marketplaces on the Internet. IPEC and its counterpart agencies around the globe play a critical role in preserving this consumer confidence and safety. The Joint Strategic Plan is an expression of the United States' commitment to protecting consumers from dangerous counterfeit goods and illicit pharmaceuticals and also for protecting inventors, artists, filmmakers, and musicians from exploitation by criminal organizations that seek to profit from the valuable artistic expressions these individuals contribute to a global society. MarkMonitor looks forward to supporting and contributing to IPEC and the objectives it seeks to achieve in its forthcoming new Joint Strategic Plan.

Respectfully submitted,



A. Statton Hammock, Jr.  
Vice-President, Global Policy & Industry Development  
MarkMonitor, Inc.

November 13, 2018