



AT&T Comments on Defensive Registrations for New gTLDs February 27, 2012

AT&T Inc. (AT&T), on behalf of its affiliated companies, appreciates the opportunity to submit comments on the issue of defensive registrations for new gTLDs. Defensive registrations continue to be a significant problem for AT&T and many other companies, in terms of both cost and consumer confusion. We continue to believe that additional safeguards are needed to mitigate the risk that the new gTLD program will greatly expand the universe of defensive registrations.

The concern about defensive registrations is not a new issue in this proceeding. AT&T has been a consistent participant in the public comment process for the new gTLD program over the past four years. We have provided a fact-based perspective and offered constructive proposals to address that concerns that we have raised. This includes real-world data about the problem of defensive registrations in the current environment of limited gTLDs.

We are re-submitting a copy of an economic report – “Assessment of ICANN Preliminary Reports on Competition and Pricing” (Economic Assessment) – that was prepared by Michael Kende, an economist who heads the regulatory practice of Analysys Mason. AT&T originally filed this economic report with ICANN on April 17, 2009. It was supported by industry data submissions and analysis of actual domain name registrations provided by MarkMonitor.

The Economic Analysis analyzed a sampling of portfolio domain name registration data for five multi-national corporations from different economic sectors. For purposes of the analysis, a “core registration” was defined as a registration that is used as a company’s main website or to complement the main website in some way. A “defensive registration” was defined as a registration that is not unique, does not resolve, redirects traffic back to a core registration, or does not contain unique content.

The consistent results for the five companies were that their portfolios consisted of thousands of domain names (ranging from 1,892 to 8,654) and the percentage of defensive registrations was extremely high (ranging from 88.01% to 99.95%). While a significant portion of defensive registrations were in the .com domain, there were also sizable numbers of domain registrations in other gTLDs. AT&T’s experience with defensive registrations has not improved over the intervening three years. We still maintain thousands of defensive registrations and defensive registrations still comprise the vast majority of the registrations in our portfolio.

AT&T is forced to incur substantial costs protecting its trademark by maintaining defensive registrations and pursuing remedies against infringing uses through the UDRP process and other legal claims. But our concerns extend beyond trademark protections. AT&T is forced to resort to defensive registrations in order to prevent domain name abuse which has a range of harmful impacts on our business and our customers. There are numerous examples of egregious domain name infringements involving sites with sexually explicit content and competitive commercial



content linked to AT&T's brand. Even worse, there are websites that are designed to confuse consumers for phishing, fraud or other harmful purpose.

AT&T's firsthand experience with defensive registrations has shaped our perspective of the new gTLD program. The reality is that globally recognized brands are a common target for domain registration abuse because infringing sites can be used to generate traffic (and associated advertising revenues) or to confuse consumers. The most effective safeguards to avoid defensive registrations and the underlying problem of domain name abuse are those which keep infringing and confusing domain names out of the system in the first place. Accordingly, we have long supported common sense protections that are designed to keep established global brands from being registered by third parties at the top level and the second level. We also have supported proposals to streamline post-delegation remedies and increase their effectiveness.

We recognize that ICANN has made progress establishing mechanisms that are designed to mitigate the need for defensive registrations and to generally address the rampant problem of domain name abuse. Based on our experience and the magnitude of the problems that may arise in connection with the new gTLD program, however, we believe additional safeguards are needed. We also agree with other commenters that, while there are concerns about defensive registrations at the top level, such concerns are magnified at the second level.

Consistent with AT&T's prior comments, the following are additional safeguards that ICANN should implement to address these concerns:

- *Controlled Introduction of New gTLDs.* AT&T supports the controlled introduction of new gTLDs in a manner that allows ICANN to manage the risks and potential impacts of new gTLDs, while also prioritizing the introduction of Internationalized Domain Names (IDNs). ICANN is already developing a mechanism for processing new gTLD applications in batches, which means it will have to address the issues of how to reasonably manage the process and to prioritize certain applications. ICANN should go a step further and establish a more controlled introduction process so it has the opportunity to test the process and ensure that any unforeseen problems are addressed.
- *Do Not Register List.* AT&T supports a Do Not Register List as an effective way to provide stronger protections and to at least reduce the need for companies to file defensive registrations and rely on post-delegation remedies to address domain name abuse. The existing new gTLD program provides only limited protections designed to keep infringing domain name registrations out of the system in the first place. At the top level, a company must resort to a defensive registration or the filing of a legal rights objection process. At the second level, a company can register with the Trademark Clearinghouse, but this offers only limited and temporary protection. By contrast, a Do Not Register list would provide more a more effective and persistent mechanism for preventing the registration of infringing domains. The protections that we are seeking are



similar to the protections that ICANN has afforded itself and other globally recognized organizations that have been placed on a Reserve List.

- *Strengthen and Streamline Post-Delegation Remedies.* AT&T supports making changes to strengthen and streamline post-delegation remedies. For example, the Uniform Rapid Suspension (URS) process should be modified so it is both rapid and cost effective. In order to be a viable option for companies, the URS process should be streamlined and a “loser pays” structure should be imposed in order to provide cost recovery for parties that successfully utilize the process.

AT&T is an active participant in ICANN and a strong supporter of the multi-stakeholder Internet governance process. However, we have ongoing concerns that ICANN’s work is unfinished when it comes to providing effective safeguards to address the potential costs and negative externalities of introducing large numbers of new gTLD. We urge ICANN to continue analyzing how existing problems, such as defensive registrations and the underlying issue of domain name abuse, may be exacerbated by the new gTLD program as it is currently structured. It is not too late to strengthen the safeguards that will help to prevent and remediate these problems, particularly at the second level. ICANN also should establish a robust structure for gathering data about defensive registrations and other indicia of domain name abuse, which will inform its decision-making process and contractual compliance activities.