usTLD Recommendation for Privacy Policies

February 26th 2021

On behalf of the usTLD Stakeholder Council ("Council"), the usTLD Security Subcommittee ("Subcommittee") was formed to review, analyze, and provide recommendations on the current policies in place for the .US namespace through the lens of their security implications for the namespace, including for registrants and users that rely on .US.

Within this scope, the Subcommittee reviewed the current ***usTLD Privacy Services Policy*** and the previous recommendations on the ***.US Registry Based Privacy Service Plan.*** Based on the Subcommittee's review, the Council formally recommends that the NTIA adopt a policy that allows for privacy services for .US domain name registrants***.***

This document submitted by the usTLD Stakeholder Council includes three sections:

1. Background on usTLD Privacy Services Policy
2. Rationale of Support for allowing Privacy Services
3. Recommendations

1. Background on usTLD Privacy Services Policy

There is currently a prohibition in place on privacy services for domain registrations. The current policy stated in Section 3.6.13. of the usTLD Registrar Accreditation and Registry-Registrar Agreement reads as follows:

"Neither Registrar nor any of its resellers, affiliates, partners, and/or contractors shall be permitted to offer anonymous proxy domain name registration services which prevent the Registry from having and displaying the true and accurate data elements contained in Section 3.3 for any Registered Name."

The National Telecommunications and Information Administration (NTIA), awarded the contract to manage the usTLD registry to Neustar in 2001. That contract and the subsequent renewal contracts require domain name registrants to provide contact information for inclusion

in the WHOIS database. In 2005, the NTIA issued a letter to Neustar clarifying its policy that privacy or proxy services were inconsistent with registrars' obligations under the usTLD Registrar Accreditation and Registry-Registrar Agreement to provide complete and accurate contact information for the WHOIS database,and instructed Neustar to direct all .US registrars to cease offering these services.

At the 2015 usTLD Stakeholder Town Hall, stakeholders identified the lack of privacy services as a key issue suppressing domain name registration in the .US TLD. Subsequently, the Council developed recommendations for the ***.US Registry Based Privacy Service Plan***. This work concluded in 2017 and submitted to the NTIA.

In 2019, the usTLD Administrator contract was again awarded to Registry Services, LLC, a Neustar company. Within the response, now incorporated as contracts, a registry privacy service plan was proposed to be developed and deployed.

2. Rationale of Support for allowing Privacy Services

The usTLD Stakeholder Council believes that implementing a policy to allow for privacy services for .US domain name holders is fully consistent with, and indeed advances, the U.S. Department of Commerce's goals for management and coordination of the domain.

In its decision to outsource operation of .US, the U.S Department of Commerce intended for the domain to grow and adapt to the evolving needs of United States Internet users. In fact, it specifically stated its desire to promote "… a stable, flexible, and balanced environment within the usTLD that is conducive to innovation and that will meet the future demands of potential registrants."

We believe that allowing a privacy service plan would better meet the needs of today's Internet users and the realities of today's Internet environment, which have evolved considerably in the

nearly 20 years since the current .US registration data provisions were established. Furthermore, the previous proposal for a privacy service plan outlined a framework to satisfy the legitimate needs of a range of .US stakeholders, including consumers, registrants, registrars, law enforcement, and intellectual property holders (among others), consistent with the notion of promoting a stable and balanced environment within the TLD.

Overall, we believe the adoption of a policy to allow for privacy services will lead to greater use and innovation in the domain, greater choice and protection for American Internet users and registrants, and a domain environment that meets the needs of a range of stakeholders, consistent with U.S. policy objectives.

The Council also believes that privacy services can be implemented in a way that addresses the concerns of law enforcement and other relevant parties that rely on access to accurate WHOIS information, through the provision of an authoritative, accurate, real-time private WHOIS database that is quickly and easily accessible in response to lawful requests.

There are legitimate concerns about the implications for digital and physical safety when individuals' personal information is published and publicly accessible, including name, physical address, phone number, email address, and more. These concerns relate to the ability of .US registrants to safely use the namespace to engage in business, life events, express themselves, and ultimately exercise their constitutional rights.

The Stakeholder Council believes that the implementation of a mechanism to protect privacy of registrants is long overdue amid a WHOIS landscape that has shifted significantly during the time in which the prohibition on privacy and proxy registrations have been in place.
Examples of Privacy concerns with implications for safety and security include:

- Shifting landscape - registrants of nearly all top-level domains have their registration information redacted from the public whois. This has potentially made registrants of .US a more vulnerable target as the pool of publicly available information from other TLDs diminished.
- All registrants expose themselves to identify theft, spamming , spoofing, scammers, and more.
- Activists, bloggers, and others seeking to exercise their constitutional rights on a .US domain name are at heightened risk of exposing themselves to doxing, swatting, online harassment, threats, as well as targeted physical harm.
- Registrants promoting physical events, such as their own wedding, are effectively announcing what day(s) their home will be vacant, while their physical address is published publicly.
- Email address and phone number are often two key identifiers linked to our online accounts. This has long been an issue, but during a time in which nearly every aspect of our lives are online, it is as critical as ever to protect people's security online.

3. Recommendations

The Council continues its longstanding support for privacy services by formally recommending that the NTIA adopt a policy that allows for a usTLD ***privacy plan.***

Building on current and previous recommendations, the Council believes it is important to highlight the difficulty that would be presented by a carve out for commercial entities. The Council recommends that to reduce confusion in the application and enforcement of the policy, to protect legitimate concerns of home-based businesses, and to maintain a low cost of administration, privacy service should be made available to all domain holders regardless of commercial status.