**.US Overview**

The .US top level domain (usTLD) is the country code-top level domain for the United States of America. It is operated by the United States Department of Commerce and managed by Neustar, Inc. Today, there are over 1.7 million .US domains under management. Registrants include individuals, organizations, corporations, and localities that have crafted their domain names to emphasize US-origins, geo-target content by bringing US consumers directly to the domestic sites or product offerings of international corporations, represent the word "us," or combine both the string to the left and right of the "." to spell out a word ending in the letters u and s. It is an online home for the people, organizations, and corporations that make up the United States and for foreign and multi-nationals providing services to the US market.

***Issue***

A legitimate privacy service lists alternative, reliable contact information in WHOIS, while keeping the domain name registered to its beneficial user as the registrant. A proxy service registers the domain name itself and licenses use of the domain name to its customer.[1] In both cases the contact information of the service provider is displayed rather than the customer's contact information. The proxy service provider maintains all rights as a registrant and assumes all responsibility for the domain name and its manner of use. Under the current policy, registrants are barred from using privacy and proxy services. These services are often available in other TLDs. This policy reflects the historic needs of law enforcement, rights holders, and others, for easily accessible and accurate contact information. On the other hand, the inability to use privacy and proxy services ("P/P services") is a frequent complaint from registrants who desire to use these services to protect their online identities and from some registrars whose registrants may be deterred from choosing .US, due to the inability to choose to keep their contact information private.

The inability to use P/P services may also disproportionately affect certain categories of registrants, thereby inadvertently shifting the registrant composition of the usTLD. Sixty percent of .US websites are registered to state governments, public school districts, county libraries, and colleges, but forty percent of .us domain websites belong to other entities such as international corporations, global media publications, global nonprofit organizations, churches, sports teams, small businesses, blogs, home businesses, retail stores, social media messaging sites, gaming sites and video/music streaming sites. This later grouping encompasses the demographic of registrants who are most likely to be affected by the existing prohibition on P/P services.

[1] "ICANN WHOIS." Privacy and Proxy Services. ICANN, 2015. Web

***Objective***

The Stakeholder Council is considering whether the existing ban on privacy and proxy services remains appropriate for the usTLD, whether exceptions should be made for certain categories of users and/or specific types of registrations, or whether the ban should be lifted altogether. The purpose of this paper is to explain the P/P services restriction by defining its goals and origins, show how the restriction is implemented and enforced, explore both the risks and benefits of privacy protection services, outline the range of P/P service options for registrars, and outline options that might foster productive growth within the usTLD.

**Background**

***Privacy/Proxy Policy - Goals and Origins***

The usTLD policies require every domain name registration to be associated with valid contact information- typically this includes a name, address, email address, and phone number. This information is then hosted in a database called WHOIS, where it can be searched by anyone with access to the Internet. Historically speaking, the WHOIS database was the "telephone directory of the Internet." It was used so that registrars and registrants could communicate directly with one another. However, in recent years, just as the needs and concerns of individuals posting in the phone book have changed, so too have those operating web domains.

P/P services were created in the gTLD space and for some ccTLDs, to accommodate people and organizations who wish to keep certain information about them from being published in public WHOIS information. A legitimate privacy service lists alternative, reliable contact information in WHOIS, while keeping the domain name registered to its beneficial user as the registrant. A proxy service registers the domain name itself and licenses use of the domain name to its customer. In both cases the contact information of the service provider is displayed rather than the customer's contact information. The proxy service provider maintains all rights as a registrant and assumes all responsibility for the domain name and its manner of use. In this case, the service provider maintains all rights as a registrant (such as managing, renewing, transferring and deleting the domain name,) and assumes all legal responsibility for the domain name and its manner of use.

The prohibition on P/P services is the result of an effort to provide complete and accurate WHOIS information for all .US domain names. Maintaining an accurate WHOIS database for .US registrants is an important responsibility of the .US registry. The WHOIS database is an important tool for law enforcement investigations. While there is a legitimate role for proxy registration in limited circumstances, privacy protected registrations make it difficult to identify

or contact those responsible for abusive domain name registrations. As a result, P/P services have been barred in an effort to promote complete openness and transparency within the .US name space.

***Implementation and Enforcement***

The policy restriction is implemented by .US registrars. Neustar does not directly enter into agreements with registrants. Language in the .US Registry-Registrar and Registrar Accreditation Agreement states that:

> "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."

This policy is passed through to registrants by way of registration agreements that a registrar must enter into for all of the .US registrations that it sponsors. Some examples of how this policy is relayed in .US Registration Agreements are found below.

> GoDaddy: "…You acknowledge and agree that you are not permitted to purchase private or proxy .US registrations. You shall register for any and all .US registration using your personal information, which information you represent and warrant is current, accurate and complete."

> Google Domains: "Registrant is not permitted to purchase private or proxy .us registrations. Registrant will register for any and all .us domain name registrations using Registrants personal information as the registered Name Holder, which information Registrant represents and warrants is current, accurate, and complete. Registrant certifies that to the best of Registrant's knowledge."

Neustar enforces the restriction through a number of mechanisms. Neustar currently operates a WHOIS Accuracy Reporting Tool where users can report false or incomplete WHOIS records for .US domain names. All domains reported through this tool are investigated by Neustar. If a record is found to contain false or inaccurate WHOIS information or to use a proxy service, the registrant is given ten (10) days to remedy the deficiency by providing complete and accurate WHOIS information. If the deficiency is not remedied it may be deleted from the Registry database.

Additionally, Neustar performs random spot checks on .US registrations to affirm that WHOIS information is being accurately provided. If, as part of these checks, registrants are found to be using P/P services, they are given thirty (30) days to remedy the deficiency by providing

complete and accurate WHOIS information. If the P/P service in question is found to be provided by a .US registrar or reseller, Neustar will also work directly with that party to ensure that the entity ceases to sell these services and that other affected registrations are updated.

Neustar also runs an automated query to attempt to identify Privacy/Protection registrations in .US. Where registrations are identified, Neustar works with the sponsoring registrars to ensure that the provision of such services is ceased and that WHOIS records are updated for the registrations in question. The results of such queries are reported in the Annual WHOIS Accuracy Report to the Department of Commerce.

**Discussion and Analysis**

***The Pros and Cons of Restricting Privacy Protection Services***

***Pros***

One reason to restrict P/P services is that having accurate WHOIS information publicly accessible is meant to foster accountability. When P/P services are not in use, complainants are able to directly interact with the registrant, without depending on the registrar or other third party P/P service providers to regulate the flow of information. This is beneficial for law enforcement and in cases of intellectual property infringement because the ability to deal directly with the registrant can avoid costly delays.

Another advantage of restricting P/P services is that it may reduce the presence of illegal or harmful Internet activities. *The 2013 Study of WHOIS P/P Service Abuse* found clear evidence that a significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via privacy or proxy services to obscure the perpetrator's identity. It also concluded that it is often true that the percentage of domain names used to conduct illegal or harmful Internet activities that are registered via privacy or proxy services is significantly greater than the percentage of domain names used for lawful Internet activities that employ privacy and proxy services.[2] In this study, harmful activity is categorized as phishing, money laundering, unlicensed pharmacies, typosquatting, child sexual abuse image websites, domains appearing in email spam (SUBURL domains), domains associated with malware, and domains subject to the Uniform Domain Name Dispute Resolution Policy (UDRP) process. Therefore, a restriction deterring this type of activity serves a variety of important purposes and helps maintain the integrity of the .US name space.

Another reason to restrict P/P services is that they give online consumers some of the same information normally available offline in the brick and mortar world. A study by FWD Strategies

[2] Clayton, Richard. *A Study of Whois Privacy and Proxy Service Abuse* (2013): Pg. 58. Sept. 2013. PDF.

International and LegitScript entitled *Commercial Use of Domain Names: An Analysis of Multiple Jurisdictions* argues that consumers want to know who they are doing business with. The usTLD is host to various commercial businesses and the current policy allows consumers to identify the individual(s) with whom they transact business. This is a foundational principle in consumer protection law. The study goes on to argue that consumerism in the online world should mimic consumerism in the offline world, where participants gain information through the physical appearance of storefronts, consumer reviews and publicly available business information. In the offline world consumers are able to visibly inspect the company, meet the staff and review business licenses or corporate registration information. This transparency protects consumers by giving them a way to validate the legitimacy of the person or entity with which they are conducting business. It also provides both parties a means of recourse as each party can identify and locate the other should the transaction go wrong. This transparency is carried over to shoppers online to the extent the WHOIS database is updated and contains accurate information listings.

According to the study mentioned above, WHOIS registration data plays a vital role in combating sources of consumer fraud, spam and denial of service attacks, preventing or detecting sources of security attacks, supporting UDRP proceedings, investigating legal violations (piracy, product counterfeiting and trademark violations, pornography, illegal drug sales, financial crimes), and facilitating and validating the legitimacy of a website for commercial transactions. In order for online consumerism to continue developing within .US, consumers have to feel safe providing their credit card information to multiple vendors and they need to trust that the vendors they're dealing with are legitimate and reliable. Those who support the usTLD ban on P/P services reason that this policy can help grow the demographic of online retailers. By ensuring that transactions will be protected due to the openness produced by the P/P restriction and the accuracy guaranteed within the WHOIS database, the logic is that more commercial entities will be attracted to .US.

***Cons***

A consequence of barring privacy services may be that registrants engaged in entirely legitimate activities, like bloggers, home businesses, startups, and nonprofits, etc., will provide false or inaccurate information to protect their privacy. The FWD/Legit Script study, mentioned above, also demonstrates that although many domains registered for entirely lawful Internet activities have viable telephone contact information recorded within the WHOIS system, a great percentage of them do not. The reason could be that registrants have significant privacy concerns about publishing otherwise unlisted phone numbers. In general this reluctance is consistent with growing privacy awareness demonstrated by the steady increase of unlisted telephone numbers, particularly among wireless users.

In the gTLD setting, ICANN's *Initial Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process* states that the WHOIS accuracy tools and reviews have generally found violations in which a P/P service is used to be very low. WHOIS accuracy checks, on the other hand, reveal a high number of registrations, in all TLDs, in which false WHOIS data is provided. While the registrations identified may be ultimately corrected or deleted from the registry database, the overall trend suggests that the unavailability of P/P services may push registrants toward other forms of WHOIS abuse and make the registrant altogether un-contactable; an externality that undermines the primary objective of the usTLD prohibition.

Moreover, public comments in response to ICANN's *Initial Report* reflect legitimate concerns for the safety of Internet users who abide by the rules of the restriction and provide accurate WHOIS data. Another con of restricting P/P services is that with personally identifiable information now publicly available, it is easier to "dox" and "swat" people online. Doxing refers to the practice of uncovering personal information about someone online for malicious intentions. Swatting refers to the practice of using personal information to place hoax calls with law enforcement with the intention of sending out squads of armed police to specific locations.[3] The most prevalent instances of doxing occur for extortion, coercion, harassment, public shaming, and/or vigilante justice purposes. Swatting, which is not as prevalent as doxing, is more common within gaming communities and with young children looking to prank their friends and celebrities, or young hackers targeting security journalists for show.

In January 2008, anonymous hackers doxed the top-level religious members of Scientology, revealing their personal information as well as internal memos that had been circulating within the inner circle of the Church.[4] In 2011, the hacker group Anonymous doxed the technology firm HBGary Federal and exposed detailed information on 7,000 members of law enforcement officials.[5] In 2014, a group of women were doxed by male gamers trying to intimidate them into keeping silent about sexism within the gaming community.[6] And later that year, in November 2014, Anonymous began publicly releasing the identities of members of the Ku Klux Klan in Ferguson, Missouri.[7]

Randi Harper, founder of the Online Abuse Prevention Initiative, was swatted based on information obtained from the WHOIS record for her domain. And Brian Krebs, an online security journalist, was also swatted as a prank by young hackers. The FBI estimates that based

[3] "Doxxing, Swatting and the New Trends in Online Harassment." *The Conversation*. The Conversation, April 2015.

[4] Barkham, Patrick. "Hackers Declare War on Scientologists amid Claims of Heavy-handed Cruise Control." *The Guardian*. N.p., 4 Feb. 2008. Web.

[5] Bright, Peter. "Anonymous Speaks: The inside Story of the HBGary Hack." *ARS Technica*. Conde Nast, 15 Feb. 2011. Web.

[6] Barkham, Patrick. "Hackers Declare War on Scientologists amid Claims of Heavy-handed Cruise Control." *The Guardian*. N.p., 4 Feb. 2008. Web.

[7] Blue, Violet. "Anonymous Seizes Ku Klux Klan Twitter Account over Ferguson Threats | ZDNet." *ZDNet*. Zero Day, 16 Nov. 2014. Web

on local law enforcement calls, received about once a month, interviews of individuals arrested, and a review of social media, where perpetrators brag about these instances, there are around 400 swatting attacks per year. Doxing, on the other hand, occurs more frequently and is not always investigated by the police.[3]

Another con is that prospective registrants, specifically those who operate home businesses, might be dissuaded from registering in .US based on the unavailability of P/P services. Even though there is professional contact information on the registrant's website, the registrant is still required to list home address and an associated phone number on the domain registration, which could result in unwanted home visits or phone calls. Another example could be that a registrant operates a blog and decides to use that blog platform to speak out against a controversial political matter. If a reader takes offense to this act of free speech, they could access the registrant's contact information and publish it to their social media pages, which could lead to multiple forms of harassment. Additionally, these legitimate concerns about privacy could inhibit the success of the usTLD in reaching out to nonprofit networks (e.g. girl or boy scouts troops, local community groups, and others not engaged in online commerce.)

It is relevant to note that other than the incidence involving Randi Harper, there is no evidence that the above instances are the result of information found through the WHOIS database. There are cases of individuals that understand the ban on P/P services, provide accurate information and take measures to protect themselves despite the ban. This includes purchasing a new phone with a new telephone number, creating a brand new email, and/or establishing a PO Box and using that as an address for registration purposes. Nonetheless, these instances suggest that barring privacy protection services for the purpose of openness and transparency may come at the cost of potentially deterring registrants, fostering other forms of WHOIS abuse and exposing personal information that may put some registrants at risk.

***Other Activity***

**ICANN** has been considering issues related to the use of P/P services in the gTLD space. On May 5, 2015, the Privacy/Proxy Services Accreditation Issues (PPSAI) Working Group (of the Generic Names Supporting Organization) published its Initial Report. It was put out for public comment and thousands of responses have been received. These comments are now under review.

In the Initial Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process the Working Group stated that there are specific topics on which there is no consensus.

> Although the WG agreed that the mere fact that a domain name is registered by a commercial entity or by anyone conducting commercial activity should not preclude the use of P/P services, there was disagreement over whether domain names that are actively used for commercial transactions (e.g. the sale or exchange of goods or services) should be prohibited from using P/P services. While most WG members did not

> believe such a prohibition is necessary or practical, some members believed that registrants of such domain names should not be able to use or continue using P/P services.[8]

Meanwhile, **Nominet,** a .UK registry, plans to enforce an updated WHOIS policy in September 2015. This new policy will allow non-trading, non-commercial, entities to "opt out" of the public WHOIS database. According to this policy, individuals who are not using their domain name for trading, commercial, purposes will be able to opt-out of publishing their contact information in the public WHOIS database. However, domain names that choose this opt out policy and use P/P services cannot transact with customers, primarily advertise or promote goods, services, or facilities. The P/P service providers will act as an address for service for the registrant, respond to or pass on abuse complaints from third parties to the registrant, and provide the contact details of their privacy service, which will be validated by Nominet and published in the WHOIS database.[9]

***Registrar Options for Privacy Protection***

Should the Council elect to undertake policy development on this issues it is important to note that the availability of P/P services in the usTLD need not be an all or nothing proposition. There are a range privacy protection options and many registrars implement carve outs that best fit the goals of their specific domain space. The goal of .US is to produce growth while ensuring the accuracy of the WHOIS database listings within the .US registry. This means serving the needs of major corporations and commercial businesses without deterring bloggers, home businesses, and nonprofits, etc. The range of privacy protection options and their descriptions are listed below.

- *Complete P/P restriction*

This involves retaining the current policy.

- *No P/P restriction at all*

This would involve allowing the unregulated use of P/P services within the usTLD.

- *P/P restricted to accredited services.*

[8] ICANN. *Initial Report on the Privacy and Proxy Services Accreditation Issues Policy Development Process* (2015): Pgs 15-16. 5 May 2015. PDF

[9] Neylon, Michele. "Nominet Announces WHOIS Policy Changes." *Domain Name Industry News*. 23 July 2015. Web.

In this case a registrar could choose to offer an accredited (by .US) P/P service as part of the domain registration contract. For example, the top five gTLDs, .com, .net. .org, .info, and .biz all use a WHOIS privacy or proxy service for those registrants that want to protect themselves.[10]

- *Allow P/P services for non-commercial entities*

This would permit the use of P/P services for non-commercial entities, but would keep the prohibition in place for commercial use.

- *P/P self-services provided by accredited organizations*

These services would restrict the use of P/P services for registrants who are associated with community groups and nonprofit organizations that would serve directly as the P/P service provider. For example, Girl Scouts of America could provide P/P services for its affiliated Girl Scout troops, members, and volunteers, etc.

**Approaches to Consider**

***.US Stakeholder Council Recommendations and Observations***

-Retain policy as is.

-Introduce carve-outs whereby certain categories of users could be exempt from the privacy and proxy requirement.

- Are there categories of users for whom the restriction on privacy/proxy registrations should be waived?
- If so, what would these categories of users be?
- How would these users be verified?
- What parties should have access to information that is behind the gate? For what purposes and under what conditions?
- Could carve outs be implemented in a way that parties were appropriately verified and key parties retained access to information behind the gate?

Lift the privacy and proxy restrictions for .US registrants but require that the full data be retained by Neustar and accessible to the Department of Commerce.

- Is lifting the policy across-the board appropriate? In what cases should the use of privacy and proxy be restricted?

[10] ICANN. "ICANN Study on the Prevalence of Domain Names Registered Using a Privacy or Proxy Service among the Top 5 GTLDs." *ICANN Study on the Prevalence of Domain Names Registered Using a Privacy or Proxy Service among the Top 5 GTLDs Executive Summary* (n.d.): n. pag. Web. <ICANN Study on the Prevalence of Domain Names Registered using a Privacy or Proxy Service among the top 5 gTLDs>.

- What parties should have access to the full data? For what purpose and under what conditions?
- How could this be implemented such that eligible parties can still access the full data?
- What would be the costs to Neustar to implement and the time required to implement?
- Would the cost/time tradeoffs be justified by the benefits?
- How could the existing third party WHOIS Accuracy tool be substituted for in cases where privacy was being used?
    - Is this tool necessary?
    - What benefits has it provided in terms of WHOIS accuracy enforcement?
    - What other tools and mechanism could achieve similar benefits?

Allow membership organizations representing key target registrant demographics (presumably those that would be specifically deterred by privacy/proxy) to sponsor registrations on behalf of users.

- What are the registrant categories that we want to cover?
- What membership organization would cover some or all of these groups?
- How do these organizations verify members? Are these verification procedures sufficient for our purposes?
- What additional information, if any, would organizations be required to retain for this purposes?
- What would be the costs for implementation for relevant organizations? Would this be worth it given the size of the potential registrant networks?

What other impacts could come about as a result of this?

- User impacts?
- Policy interrelations?
- Registrar impacts?
- Impacts on LEA?