Coalition for Online Accountability

www.onlineaccountability.net

April 5, 2021

Dear .us Stakeholder Council and Secretariat and Registry Services LLC:

The Coalition for Online Accountability ("COA") consists of seven leading copyright industry companies, trade associations and member organizations of copyright owners. COA's goal is to enhance and strengthen online transparency and accountability, with a particular focus on the domain name system ("DNS"). COA represents copyright interests in ICANN's multistakeholder community and actively participates in its processes and meetings.

While COA itself is a small organization, its members: Broadcast Music, Inc., the Entertainment Software Association, the Motion Picture Association, the Recording Industry Association of America, NBCUniversal Media, The Walt Disney Comany and WarnerMedia represent and/or employ hundreds of thousands of creators whose copyrighted works are made available legally online as well as subject to damaging online infringement and piracy.

The members of COA appreciate the opportunity to express our views on the .US TLDs call for privacy services to be allowed for .us domain name registrants, and offer the following high level comments for your consideration.

THE NEED TO BALANCE PRIVACY AND PUBLIC SAFETY AND SECURITY

We appreciate the concerns set out in the usTLD Recommendation for Privacy Policies dated February 21, 2021 ("Recommendation") and the goal, as stated in the Recommendation, of providing *"greater choice and protection for American Internet users."* However, we believe allowing the use of Privacy or Proxy services to mask the identity of registrants of .us domain names will not further—and frankly will undermine—the stated goal. This is because the privacy of domain name registrants must be balanced with the imperatives of protecting the rights and safety of internet users, including the privacy of such users. Unfortunately, over the past several years, experience and evidence have both proven that the use of Privacy or Proxy services along with the redaction of domain registrant data ("WHOIS data") have contributed to increasing levels of cyberattacks and a broad range of illegal activity online that threaten the safety of American Internet users.

We are thus concerned that the availability of these services for .us domains would attract bad actors resulting in greater abuse of internet users, increases in online illegal activity and abuse associated with the .us TLD and consequently a greatly diminished reputation for the .us TLD that would reflect poorly on the United States.

THE GROWTH IN ONLINE ABUSE AND ILLEGAL ACTIVITY

Governments as well as leading private organizations around the world have noted with alarm the increase in cyberattacks and online illegal activity that have coincided with the COVID-19 pandemic. The FBI's Internet Crime Complaint Center reported that as of June 2020, daily cybersecurity complaints had spiked from 1,000 to 4,000 and that cyberattacks on financial institutions had increased by nearly 240%[1] Neustar, a leading U.S. domain name registry and the parent company that administered the .us TLD since 2002 until Neustar was acquired by GoDaddy last year reported *"we're seeing a dramatic upturn in attacks using virtually every metric that we measure. We have observed an increase in the overall number of attacks as well as in attack severity . . . ."*[2] The Public Safety Working Group of the Governmental Advisory Committee ("GAC") to ICANN noted that global reports of ransomware attacks in 2020 increased by over 700%.[3]

Unfortunately, it is not just the COVID-19 pandemic that has led to these very concerning increases in online abuse and illegal activity. In response to the European General Data Protection Regulation, ICANN enacted policies in May 2018 that permitted domain name registries and registrars to redact most of the WHOIS data of domain name registrants (whether natural persons/individuals or legal persons/organizations), thus virtually eliminating third-party access to much of this data. This has made it much more difficult for law enforcement agencies around the world to fight online crime and for private organizations and companies to protect their rights. Even the European Union, which enacted the General Data Protection Regulation, has stated the following:

"The EU and its Member States stress that the current situation where access to non-public WHOIS data for public policy objectives is left at the discretion of registries and registrars affects the Member States authorities' ability to obtain legitimate access to non-public WHOIS data necessary to enforce the law online, including in relation to the fight against cybercrime. . .The EU and its Member States note the concerns raised by law enforcement authorities, cybersecurity organisations and intellectual property rights holders about the negative impact of limitations of access to WHOIS data on their work."[4]

---

[1] See: https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic

[2] https://www.home.neustar/resources/whitepapers/covid-19-online-traffic-and-attack-data-report

[3] See page 27 of presentation slide deck available for download here: https://69.schedule.icann.org/meetings/w8wuCYSW5rvL4Yzf3#/?limit=10&sortByFields[0]=isPinned&sortByFields[1]=lastActivityAt&sortByOrders[0]=-1&sortByOrders[1]=-1&uid=a6ijir8iemBHYWRru

[4] See: https://data.consilium.europa.eu/doc/document/ST-13443-2018-INIT/en/pdf

A number of U.S. federal agencies have also unequivocally stated that the lack of access to WHOIS data interferes with their critical investigative work of online criminal behavior. For example, in a letter dated July 16, 2020 to Congressman Latta, Homeland Security Investigations ("HSI") stated:

"HSI views WHOIS information, and the accessibility to it, as critical information required to advance HSI criminal investigations, including COVID-19 fraud. Since the implementation of GDPR, HSI has recognized the lack of availability to complete WHOIS data as a significant issue that will continue to grow. If HSI had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the investigative process[.]"[5]

Allowing registrants to use Privacy or Proxy services to mask their WHOIS data at worst obstructs investigations of online criminal behavior and at best impedes the timeliness of such investigations, which can result in serious public harm, including the loss of life. As noted by the Federal Drug Administration ("FDA"):

"Unlike some other federal law enforcement agencies, FDA's Office of Criminal Investigations (OCI) does not have authority to issue an administrative subpoena for basic WHOIS data ***or WHOIS data shielded by a privacy/proxy service.*** *Because FDA cannot access basic WHOIS data without a Grand Jury subpoena, which requires coordination with the Department of Justice, many investigative leads have not been sufficiently addressed or significantly hindered."*[6] (emphasis added)

In this same letter the FDA noted how important ready and immediate access to WHOIS data for investigations of the sale of counterfeit medications and substandard personal protective equipment that seriously threaten public safety and welfare:

"Access to WHOIS information has been a critical aspect of FDA's mission to protect public health. Implementation of the E.U. General Data Protection Regulation (GDPR) has had a detrimental impact on FDA's ability to pursue advisory and enforcement actions as well as civil and criminal relief in our efforts to protect consumers and patients. WHOIS data has also been widely used in FDA's criminal investigations to identify individuals and organizations selling online a variety of unapproved/uncleared/unauthorized products such as opioids, counterfeit or adulterated drugs as well as purported dietary supplements containing deleterious or undeclared ingredients. Most recently, lack of WHOIS transparency significantly hindered FDA's ability to identify sellers of fraudulent and unproven treatments for COVID-19 as well as illegitimate test kits and counterfeit or substandard personal protective equipment."[7]

While the .us TLD is not subject to the EU General Data Protection Regulation ("GDPR"), allowing registrants of .us domain names to use Privacy or Proxy services would result in the same masking of WHOIS data. Government agencies and private parties with legitimate and pressing needs for such data to investigate crimes, enforce laws, and vindicate legal rights, would be forced to file requests for access to such data with no assurances as to how timely access would be granted or whether access would be

---

[5] https://secureandtransparent.org/wp-content/uploads/2020/09/20-02497-ICEs-Signed-Response-to-Representative-Latta.pdf

[6] https://secureandtransparent.org/wp-content/uploads/2020/09/2020-2860-RESPONSE.pdf

[7] Ibid

granted at all. Moreover, while certainly not all uses of Privacy or Proxy services are illegitimate, the unfortunate reality is that these services are frequently used by bad actors to mask their abusive and illegal online activities. For example, the Public Safety Working Group of the GAC has found during the COVID-19 pandemic that *"the majority of domains involved in pandemic-related fraud, phishing, or malware have employed Privacy/Proxy Services to hide the identity of the registrant."*[8] According to one Public Safety Working Group government investigator, **65% of domains referred for investigation for likely abuse used a Privacy or Proxy service, typically one affiliated with the registrar of the domain name.**[9]

For the above reasons alone, we strongly recommend the retention of the current prohibition concerning the use of Privacy or Proxy services with respect to the .us TLD. and maintain that the Recommendation is misguided. In terms of the two specific questions asked for Public Comment:

1. Do you support the implementation of a policy to allow for privacy services for .us domain name registrants?
2. Do you support the implementation of privacy services to all domain holders regardless of commercial status?

COA's response to both questions is "No."

THE .US TLD SHOULD FOLLOW THE EXAMPLE OF OTHER CCTLDS THAT PROHIBIT THE USE OF PRIVACY/PROXY SERVICES AND MAINTAIN PUBLICLY ACCESSIBLE WHOIS DATA

In Europe, Denmark has determined that the public interest in accessible WHOIS data for its .dk country-code top level domain ("ccTLD") merits that such information be publicly available, even when the registrant is a natural person.[10] Denmark enacted legislation to require that the name, postal address and phone number of all .dk registrants, with narrow exceptions, be publicly accessible.[11] This is consistent with, and allowed, under the GDPR because EU Member States can determine via legislation or regulation when the public interest in personal data outweighs the privacy interest. All of this was clearly explained in recent correspondence between Denmark and ICANN. In fact, Denmark's letter states that in weighing the privacy interests against other interests that *"[t]he purpose of this provision by the Danish legislators was to establish a high-quality domain with as much transparency as possible. Anyone should be able to find out the identity of a registrant, and thus who is the person behind a specific domain name. The provision should, among other things, help to limit illegal websites as well as harassment on websites, etc., since registrants were not, as a rule, anonymous."*[12] (emphasis added)

---

[8] See: https://gac.icann.org/presentations/icann68-session-8-dns-abuse-slides.pdf and in particular page 14

[9] See page 8 of transcript available at: https://68.schedule.icann.org/meetings/qXuruznZZieKZ52yn#/?limit=10&sortByFields[0]=isPinned&sortByFields[1]=lastActivityAt&sortByOrders[0]=-1&sortByOrders[1]=-1&uid=iAz4vQpCkwvHcRSjc

[10] Of course, when the registrant is a corporation or other legal person, nothing in GDPR requires redaction of the Whois data related to that registration, and thus any justification to allowing such redaction by permitting such registrants to employ a privacy/proxy service for .us registrations is correspondingly diminished.

[11] See Section 18 of the Danish Domain Names Act

[12] See: https://www.icann.org/en/system/files/correspondence/vignal-schjoth-to-plexida-28may20-en.pdf

In addition, DK Hostmaster, which is the registry operator for .dk, undertakes efforts to verify the WHOIS data of its domain name registrants. As a result of these policies that emphasize transparency and accountability over domain registrant privacy, the levels of abuse on .dk are among the lowest of any TLD (whether ccTLD or generic TLD "gTLD"). According to the Spamhaus Project, the .dk is 0.1% bad (score 0.00). In contrast, the TLD that Spamhaus identifies as the #1 Most Abused Top Level Domain is .asia with 42.3% bad (score 3.25). The largest gTLD, .com, has 3.2% bad (score 0.38). And currently for .us the Spamhaus analysis is 9.8% bad (score 0.82).[13]

When analyzing just ccTLDs, Spamhaus ranks .us as the second worst "Spam Countries" in between China as #1 and Russia as #3 per the partial screen shot below.[14]

We believe this should be a cause of great concern not only to the .us Stakeholder Council ("Council"), but to the United States government as well.

As the top level domain that represents the United States of America, a primary goal of .us should be to reduce the amount of illegal and abusive behavior on the domain. Therefore, NTIA should be requiring that the Registry for .us adopt policies and practices to reduce the current levels of abuse on .us. Given the .us score of 9.8% bad as compared with, for example, the .dk score of 0.1% bad, and the .us ranking of second worst ccTLD for spam, substantial steps should be undertaken towards this

[13] All of these scores and percentages are available from Spamhaus at the following website: https://www.spamhaus.org/statistics/tlds/ (last visited April 1, 2021)

[14] See full webpage here: https://www.spamhaus.org/statistics/countries/

goal. Allowing the use of Privacy or Proxy services will move in the opposite direction by increasing the risk of even higher levels of abuse on .us, and therefore should be firmly rejected.

In addition to the foregoing, we note that the United States is party to several international free trade agreements whose provisions may limit the ability of .us to stop providing full public access to WHOIS data.[15] Any proposal to relax the long-standing ban on privacy/proxy registrations in .us must be carefully vetted for compliance with these international obligations that the U.S. government has taken on. To the extent that the obligations in a few of these agreements make reference to compliance with applicable national privacy laws, it would be incumbent on the Council to specify which U.S. privacy law requires giving .us registrants the option to hide their WHOIS data.[16]

We appreciate the opportunity to provide these comments and we hope the Council will take account of this input. We would welcome the opportunity to discuss and engage with the Council further on these issues.

Sincerely,

Dean S. Marks
Executive Director and Legal Counsel
Coalition for Online Accountability ("COA")
E-mail: ed4coa@gmail.com

[15] See Australia-US Free Trade Agreement, sec. 17.3.2 ("Each Party shall require that the management of its ccTLD provide online public access to a reliable and accurate database of contact information for domain-name registrants."); Korea-US Free Trade Agreement sec. 18.3.2 (same); U.S.-Colombia Trade Promotion Agreement sec. 16.4.2. (same). Texts of all Free Trade Agreements can be accessed at this link: https://ustr.gov/trade-agreements/free-trade-agreements.

[16] See U.S.-Chile Free Trade Agreement sec. 17.3.2 ("Each Party shall, in addition, require that the management of its respective ccTLD provide online public access to a reliable and accurate database of contact information for domain-name registrants, in accordance with each Party's law regarding protection of personal data.")