Secure Domain Foundation Response for GNSO Privacy & Proxy Services Accreditation Issues Working Group Initial Report Question 23

23. The WG's illustrative Disclosure Framework currently applies only to IP (i.e. trademark or copyright) rights-holders. Please provide your views on the applicability of a similar framework or policy to other types of requesters. In particular, please provide your views on the following specific questions:

(1) Should it be mandatory for accredited P/P service providers to comply with express requests from LEA in the provider's jurisdiction not to notify a customer?

YES, with a caveat. Providers should be required to comply with LEA requests not to notify a customer only in cases in which the LEA request for information has already been deemed valid.

(2) Should there be mandatory Publication for certain types of activity e.g. malware/viruses or violation of terms of service relating to illegal activity?

YES. Publication of domain abusers' WHOIS information is critical for proactive anti-abuse. Without it, a registrant can engage in blatant domain name abuse (such as phishing, malware hosting, command and control of botnets, and high volume SPAM) but hide behind the protection of a P/P service. Withholding publication in the face of such behavior would not only defeat the purpose of anti-abuse criteria; it would enable and further embolden cybercriminals. Furthermore, withholding publication when such violations occur would be a disservice to those seeking P/P services for legitimate reasons, victims from around the globe harmed by cybercriminals, and the integrity of the entire DNS system.

P/P services are just that, services that provide WHOIS privacy and/or proxy protection for a customer pursuant to terms of use. Removing publication consequences for those who engage in domain name abuse (such as phishing, malware hosting, command and control of botnets, and high volume SPAM) will cause great harm to the DNS. A recent ICANN-sponsored study concluded that privacy and proxy services are one method used by cybercriminals in their perpetration of domain name abuse (http://gnso.icann.org/en/issues/whois/pp-abuse-study-20sep13-en.pdf). Merely taking down a domain name but allowing for P/P protection to remain or only disclosing such information to a complaining party will enable cybercriminals to be repeat offenders. Accordingly, this will stifle

proactive anti-abuse efforts by preventing a registrar or another P/P service from knowing that a domain name abuser is registering with them.

WHOIS privacy is offered as a service subject to a P/P's terms of service. The obligation of a P/P provider to provide WHOIS privacy is therefore extinguished upon the breach of such terms. Accordingly, a registrant engaged in phishing, malware hosting, botnet command and control, malware, or high volume spam on a domain name protected by P/P should lose their WHOIS privacy protection. It should be noted that the termination of P/P service is wholly distinct from the due process rights afforded to one accused of a crime by a sovereign government.

(3) What (if any) should the remedies be for unwarranted Publication?

It depends upon whether or not such publication was due to negligence, harmless error, or malicious motivation. At their core, P/P services are provided by contract. Accordingly, contract law remedies should be available for a registrant if a P/P provider does in fact breach the contract and cause harm. Incentives for P/P operators to exercise caution when publishing WHOIS information should be implemented through the ICANN accreditation and compliance process. If and when unwarranted publication occurs then complaints should be lodged with ICANN. ICANN itself can threaten to withdraw accreditation if a P/P provider conducts unwarranted publication due to negligence or malicious intent and there is demonstrable harm on behalf of the aggrieved party.

Proper auditing and publication of errors made by P/P providers will enhance the ability of registrants to choose a P/P provider with a strong reputation for fulfilling their P/P contract services. A P/P system without remedies for unwarranted publication could enable P/P providers to cave to pressure and publish WHOIS information for reasons unrelated to domain name abuse and/or a breach of terms of service. This would harm accountability efforts and call into question the purpose of an accreditation regime.

(4) Should a similar framework and/or considerations apply to requests made by third parties other than LEA and intellectual property rights-holders?

(Section 1.3.2, Section 7.1 Category F)

Yes, interested and aggrieved third parties do not always fall into the category of LEA or intellectual property rights holders. Domain name abuse affects the entire Internet ecosystem. As a result, many NGOs and public benefit entities seek to stop cybercriminals and should be able to seek publication of WHOIS information for registrants that breach the terms of P/P services.

About the Secure Domain Foundation

The Secure Domain Foundation (SDF) is a Canadian incorporated not-for-profit organization dedicated to the vision of an open and secure Internet. We are a public benefit community driven organization.

Our primary mission is to provide Domain Name Registrars, registries (ccTLD & gTLD), hosting providers, DNS operators, and other Internet infrastructure providers with the tools they need to combat abuse of their services and a forum for sharing intelligence on bad actors.

For more information, please visit www.securedomain.org