The Anti-Phishing Working Group

Position Statement to ICANN Regarding WHOIS Data Access Policy Proposals

The Anti-Phishing Working Group tenders this document as the statement of the organization in consultation with its executives, steering committee, research partners and its members regarding proposals to modify and restrict WHOIS data that has been, to date, publicly available information, specifically the so-called 'Operational Point of Contact' and 'Special Circumstances' proposals. Please accept this as the petition of an organization with a membership that cuts across all of the stakeholding cohorts that are burdened by the costs and consequences of phishing and other forms of electronic crime that exploit the domain name registration system.

The APWG, a 501(c) 6 non-profit corporation founded in 2003, has evolved to become the federating nexus for the larger dialogue among counter-e.crime stakeholders worldwide. Functionally, the APWG is a broad industry, government and law enforcement coalition that has brought together counter-phishing stakeholders from across the globe, now numbering some 2680 active members from 1639 technology companies, financial services firms, ecommerce concerns, ISPs, law enforcement agencies, government agencies as well as vertical trade associations and non-profit groups serving constituencies who are injured otherwise burdened by phishing and electronic crime.

During the week of January 7, the APWG Steering Committee considered and voted on a recommendation articulated by MarkMonitor, one of the APWG Steering Committee members, that was published at http://www.markmonitor.com/openwhois/. The Steering Committee voted unanimously to support the measure. We republish that language here:

Introduction

Billions of Internet users benefit from the protection enabled by current WHOIS policy, which requires free, unrestricted and immediate access. If ICANN policy creates new obstacles or delays for those seeking to protect consumers from illegal activity involving domain names, Internet users will suffer. Thwarting the current and successful process will profoundly increase the number innocent consumers made victims by Internet criminals.

The undersigned ask the WHOIS Task Force to recognize that brand owners are most often first to respond to online illegal activity and that they rely almost exclusively on WHOIS to identify and stop the persons behind such illegal conduct. Identification is critical-it helps parties communicate and speed dispute resolution without legal action, and when such action is necessary, enables service of process, without which the legitimate rule of law cannot provide a safe environment for consumers and businesses on the Internet.

While many legitimate and important privacy concerns exist over access to WHOIS data (for example, registration data of a battered women's shelter site) many others seek anonymity as a cover for nefarious intent like cyber squatting, phishing and other for

profit illegitimate behavior. While those with ill-intent profit from anonymity, consumers and legitimate online commerce suffer, often unknowingly. We request that ICANN evaluate models that offer protection from those who seek to abuse the system while making decisions related to blocking access to WHOIS data.

We therefore ask that ICANN and the WHOIS Task Force act on the behalf of Internet users and consumers to preserve the collective trust instilled in the Internet. We request that any new policies be examined by the WHOIS Task Force in light of their impact on consumers and those seeking to maintain and protect the safety and reliability of electronic commerce.

To preserve order and maintain a sense of security and accountability for Internet users, we recommend the adoption of the Special Circumstances proposal.

Evaluation of Proposals

I. The Operational Point of Contact (OPOC) Proposal

The OPOC proposal is troubling for a number of reasons. First, it reduces the amount of information available in investigating instances of online abuse. Brand owners often rely on the various fields in WHOIS to track down cybersquatters and fraudsters. Reducing the amount of such information will likely cause delays for brand owners in identifying and commencing action against registrants who engage in illegal conduct.

The OPOC proposal does not specify the qualifications, responsibilities, and standards to be applicable to the OPOC. For example, it is unclear whether the OPOC would be able to accept service of process for legal actions involving domain names, such as the UDRP. Under the proposal, the OPOC could be a party with _no relationship to the actual registrant_. Since the OPOC can be a third party (such as a proxy service or even a registrar), there is no assurance that important communications will be promptly forwarded to the registrant. Thus, cease & desist letters, domain transfer approvals, notices of inaccurate WHOIS information, phishing take-down notices, UDRP complaints and other similar communications may not be received and processed in a prompt manner.

In addition, the OPOC proposal does not address the privacy concerns that have been raised as the primary reason for changing WHOIS policy. Without such improvements in privacy, it is difficult to justify the adoption of OPOC over the status quo.

II. Special Circumstances Proposal

The Special Circumstances proposal is preferable to the OPOC proposal because it provides a workable solution to the privacy concerns without significantly changing WHOIS for the vast majority of Internet users.

The impact to brand owners should be minimal under the Special Circumstances proposal because registrants who misuse domain names to conduct illegal online activities should not qualify for the "special circumstances designation" and therefore would continue to have their contact information displayed in the same manner as currently available today. The Special Circumstance proposal includes a practical mechanism that allows the WHOIS information to be revealed in the event the privacy designation is abused, or the domain name is used for commercial purposes.

Thus, under the Special Circumstances proposal, brand owners would not need to significantly alter their current processes and procedures for monitoring, tracking and taking action against those illegally targeting their businesses and consumers.

Epilogue

The APWG is proud to count ICANN as one of its collaborators in the contest with electronic crime and recently has agreed to develop a problem statement and policy draft on registrar and registry practices that are exploited by phishers and electronic crime gangs. The APWG will broach the issues discussed in these two proposals in that project in a more comprehensive context, with a broader brief to tender analysis and advice to the ICANN. The APWG looks forward to the process and to the fruits of that collaboration. We have been working since November to organize an appropriate working committee and supervisors for that project and will soon initialize the project.