



STATE OF NEW YORK
OFFICE OF THE ATTORNEY GENERAL
www.oag.state.ny.us

ANDREW M. CUOMO
ATTORNEY GENERAL

DIVISION OF PUBLIC ADVOCACY
INTERNET BUREAU

**New York State Office of the Attorney General
Internet Bureau
Comment on the Preliminary GNSO Whois Task Force Report on Whois Services
January 12, 2007**

Transparency of online businesses is key to building consumer trust in the electronic marketplace and for maintaining legitimate and robust use of the Internet.¹ Whether intended or not, the Whois service, as it exists today, serves as an essential line of defense to a secure and legitimate online market. When registering a domain name, name holders must submit to Whois their name and contact information as well as the names and contact information for persons responsible for administrative, billing, and technical issues related to the website.² This information, which is publicly accessible in real-time, ties domain name holders to the websites they operate. Even in the absence of any specific law requiring merchants to reveal their identities directly to their consumers or to the countries, states, and provinces in which they do business, merchants cannot function online without submitting this information to Whois.

As a result, access to Whois information has become critical to both law enforcement and the public. For nearly a decade the New York State Office of the Attorney General (“NYOAG”) and, in particular, the Internet Bureau of the NYOAG (the “Internet Bureau” or the “Bureau”)³ has used the Whois database as a first step in its investigations of online fraud and illegality. The information accessible via Whois enables us to, among other things, identify potential wrongdoers or witnesses, identify the scope of fraudulent or illegal activity, initiate fact finding by the sending of informal

¹ See Directorate for Science, Technology and Industry Committee on Consumer Policy, Organization for Economic Cooperation and Development (“OECD”), *Consumer Policy Consideration on the Importance of Accurate and Available Whois Data*, dated June 2, 2003 (“OECD Report”) at 4, a report issued by the OECD at the request of the Government Advisory Committee (“GAC”) to the Internet Corporation for Assigned Names and Numbers (“ICANN”).

² Registrars require domain name holders to submit this information for publication in Whois pursuant to the Registrar Accreditation Agreement between them and ICANN available at www.icann.org/registrars/ra-agreement-17may01.htm.

³ The Internet Bureau enforces a range of laws as they apply to Internet transactions, including New York state and federal consumer protection laws, to ensure that New York’s on-line consumers, businesses, and children are adequately protected by state and federal statutes. To this end, we have resolved cases on behalf of New York state consumers involving privacy, data security, adware/spyware, deceptive advertising, auction fraud, spam, online gambling, terms of service, protection of children, and website accessibility.

requests for information or subpoenas, initiate litigation, and resolve jurisdictional questions. Consumers also use the information available in Whois to determine the validity of online and offline transactions and to resolve complaints with website operators without legal intervention.

In its Report on Whois Services (the “Report”), the Generic Names Supporting Organization (“GNSO”) Whois Taskforce (the “Taskforce”) has offered two proposals regarding information that is publicly accessible via Whois. In the “Operational Point of Contact” proposal, the Taskforce suggests eliminating from Whois the names and contact information for the domain name holder and the personnel responsible for administrative, billing, or technical issues related to the website. In place of this information, the Taskforce proposes that domain name registrants submit the name, address, telephone number and email address for an “Operational Point of Contact” (referred to as the “OPoC”). This proposal, however, threatens to leave a serious void in accountability. Under this proposal, a domain name holder can designate an OPoC that is wholly independent from both the name holder and the website.⁴ Although OPoCs would be obligated to resolve – on their own – issues relating to the technical aspects of the domain name or to “reliably pass on data” to resolve such technical issues,⁵ OPoCs have no obligation to forward important communications or notices to domain name holders or to resolve any other issues with the domain name, such as consumer complaints or a site’s failure to comply with applicable laws. Likewise, domain name holders have no incentive to require their OPoCs to fulfill any other role than the technical one outlined in the Report.⁶ Meanwhile, the only information about the domain name holder that would be published in Whois is the holder’s name, country and state/province.⁷

The second proposal, the “Special Circumstances” proposal, would maintain the current Whois database and continue identifying the domain name holder and designated administrative, billing and technical contacts. However, it would enable individual, non-commercial domain name holders to shield their contact information from the public upon demonstrating that such publication would “jeopardize a concrete and real interest in personal safety or security that cannot be protected other than by suppressing that public access.”⁸ Here, the Report describes an unwieldy and seemingly expensive process for determining a domain name holder’s request for anonymity.⁹

⁴ See Preliminary Generic Names Supporting Organization (“GNSO”) Whois Task Force Report on Whois Services (the “Report”), at 13, 18-20.

⁵ Report at 18-19, 20.

⁶ Report at 18-19.

⁷ Report at 20.

⁸ Report at 16, 43.

⁹ For example, the “Special Circumstances” proposal suggests that ICANN choose one to five independent third-party vendors to receive, process and decide upon requests to curtail public access to contact information, see Report at 43, that the third-party vendor(s) be responsible for spot-checking Internet resources tied to the domain name to ensure that the use remained non-commercial during the designation, see Report at 45, and that the vendor(s) report

Moreover, it is devoid of many important details. For example, it does not define specific criteria for adjudicating a domain name holder's request for anonymity in Whois.¹⁰ It also does not define a procedure through which law enforcement can obtain non-public domain name registrant information.

We appreciate the opportunity to offer our comments on these proposals. In so doing, we are sensitive to conflicts that could exist between obligations to make contact information for a domain name holder publicly available via Whois and certain privacy laws, regulations, or directives. We are also sensitive to the privacy interests of individuals who wish to use a domain name for non-commercial purposes, such as speech; especially those who wish to do so anonymously. However, as set forth below, we believe that maintaining a publicly available database of contact information for registrants of commercial websites does not violate any privacy law, rule, directive, or individual privacy interest.

1. *Holders of commercial domain names should continue to be required to submit contact information for themselves and for an administrative, billing, and technical contact for public access via Whois.*

If the OPoC proposal is adopted, domain name holders would no longer be required to publish contact information for themselves or for other personnel responsible for issues related to a website. Removing this information from Whois destroys the only assured connection between a domain name and its holder. Without this information, law enforcement agencies such as the NYOAG, would not be able to identify the people behind websites that are being used to perpetrate fraud and engage in other illegal conduct. We could not send inquiries or subpoenas to these website operators to determine whether or not fraud or unlawful conduct is taking place. And we would have no anonymous way of determining at the outset of an investigation whether or not we should exercise jurisdiction over the website. Similarly, without this contact information, consumers would have no way to resolve complaints about the goods and services offered through a website. In short, the OPoC proposal allows online merchants to hide behind their OPoCs and to avoid detection by law enforcement and aggrieved consumers. It provides the perfect environment for Internet fraud and illegal conduct to proliferate unchecked.

The proposed requirement that an OPoC's contact information be publicly available on Whois does not remedy these problems. Under the proposal, the OPoC may be wholly independent from the domain name holder and is not obligated to forward communications from law enforcement or consumer complaints to the domain name holder.¹¹ Furthermore, the proposal creates no

on the operation of the "special circumstances" mechanism, see Report at 46.

¹⁰ Report at 43-44, 46.

¹¹ Report at 13, 18-20.

incentives for requiring OPoCs to forward such communications to the name holders.¹²

Given these realities, the Report's proposals that touch upon how law enforcement agencies (like the NYOAG) and consumers can obtain contact information for a domain name holder¹³ are inadequate. These proposals do not adequately distinguish between requests for information by the public and those by law enforcement. The proposals also fail to provide clear criteria or finite timetables for handling third-party requests for information and do not guarantee that requests for information made by law enforcement will be kept confidential to protect the integrity of an undercover investigation.

Accordingly, we are opposed to the OPoC proposal and believe it is imperative that law enforcement and the public have real-time access to a commercial website's administrative, billing, technical, and domain name holder contact information.

2. *Continuing publication of the contact information for domain name holders of commercial websites in the Whois database does not violate individual privacy interests.*

To the extent privacy concerns have fueled the Taskforce's proposal for eliminating the publication of direct contact information for domain name holders and for websites' administrative, billing and technical personnel in Whois,¹⁴ such concerns do not apply to commercial websites. The domain name holder of a commercial website has no more of an expectation of privacy in his/her professional contact information than the operator of a store front has in his business address. If a domain name holder chooses to take advantage of the opportunities available in an online market, he cannot avoid the corresponding responsibilities to his customers by hiding his or her identity. Such reasoning creates a safe haven for perpetrators of online fraud and turns the concept of privacy rights on its head.

Indeed, the written opinions ICANN has received regarding the current Whois system's violation of certain international and national data protection laws reflect a concern for individual's privacy rights and thus support treating private individuals and businesses differently.¹⁵ Therefore,

¹² Report at 18-19.

¹³ Report at 23-27 (describing five proposals regarding how the public could request and possibly obtain domain name holder contact information).

¹⁴ *See Final task force report on a policy recommendation and advice on a procedure for handling conflicts between a registrar/registry's legal obligations under privacy law and their contractual obligations to ICANN* at 17, found at gns0.icann.org/issues/tf-final-rpt-25oct05.htm.

¹⁵ *See Letter from the Working Party on the Protection of Individuals with regard to the Processing of Personal Data ("Article 29 WP") to ICANN*, dated June 22, 2006 at 2 (noting the different legal issues raised by the registration of domain names by individuals as opposed to the registration of domain names by companies or other legal persons); European Commission Internal Market DG, *Contribution of the European Commission to the general discussion on the Whois database raised by the Reports produced by the ICANN Whois Taskforce*, dated May 12,

the public should continue to have access to the contact information of holders of commercial domain names.

3. *Even if only OPoC information is published for registrants of non-commercial websites as a means of protecting individual privacy interests, procedures must be maintained for guaranteeing law enforcement access to the direct contact information of the domain name holder when appropriate and for requiring registrars to investigate and take appropriate action to halt the improper or inaccurate use of OPoC information.*

Publishing OPoC information for registrants of non-commercial websites makes sense provided that law enforcement is able to receive direct domain name holder contact information when necessary and that websites are not permitted to abuse their designation as non-commercial or provide inaccurate OPoC information. Registrants of non-commercial websites should thus be required to submit direct domain name holder contact information to registrars even if it is not published in Whois. Registrars should also be required to make the domain name holder's direct contact information available to law enforcement upon legally valid request and should be required to keep these requests confidential. This protects the individual's privacy interest in their personal information, promotes the non-commercial use of the Internet, and allows for the resolution of technical issues with an individual's website.

In addition, domain name holders should not be able to avoid disclosing their identity by misrepresenting that they are registering a non-commercial website or by providing other misinformation. As the Organization for Economic Cooperation and Development noted in its June 2, 2003 report to ICANN domain name holders intent on defrauding the consuming public may take advantage of the non-commercial distinction by claiming to be non-commercial for registration purposes and then using their sites for commercial purposes.¹⁶ This situation can be remedied by following existing procedures for correcting inaccurate Whois data as modified by the Taskforce's proposal. At present, ICANN's Registrar Accreditation Agreement requires registrars to investigate claims of inaccurate Whois data brought to their attention by any person and, if necessary, to have that information corrected.¹⁷ The Taskforce proposes, and we support, further empowering registrars in this regard by requiring them to place a domain name on hold or revoke a domain name's registration in the event that inaccurate Whois data is not corrected.¹⁸ Therefore, if a registrar learns

2003, at footnote 4 (referring to threats to individual privacy rights by publication of contact information via Whois); International Working Group on Data Protection in Telecommunications, *Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet*, adopted May 4/5, 2000 (prefacing its position on the observation that "more and more private persons are starting to register their own domain names[.]") (emphasis supplied).

¹⁶ See OECD Report at 5.

¹⁷ See Registrar Accreditation Agreement at 3.7.8.

¹⁸ Report at 28.

that a domain name holder for a commercial website has listed an OPoC's contact information in Whois instead of his own direct contact information, the registrar can treat that listing as inaccurate Whois data and require the domain name holder to either list his direct contact information or lose the website's registration.

Some Internet users have expressed fear that using registration data for anything other than strictly technical purposes would place ICANN in a role of policing the content of the Internet.¹⁹ However, requiring a registrar to vet notices that a website designated as non-commercial for registration purposes is actually a commercial site does not call for ICANN or the registrars to police Internet content. Rather, it focuses on the accuracy of Whois data, which is a stated goal of the Taskforce.

4. *In the event that only OPoC information is submitted for publication in Whois, registrars, the OPoC and/or the domain name holder should be obligated to address requests for contact information of the domain name holder and complaints about a commercial website.*

While we urge the Taskforce not to change the contact information currently provided in Whois for commercial websites, we note that the Taskforce has not reached consensus as to how the public, including law enforcement, can access a domain name holder's contact information if only OPoC information is publicly available.²⁰ Nor has it reached consensus as to the OPoC's obligations regarding third party requests for this information.²¹ Accordingly, the Report does not set forth a definitive procedure for ensuring timely and confidential responses to requests for information made by law enforcement or consumers.

If the Taskforce does decide to stop publishing direct contact information for all domain name holders, in order to prevent the Internet from becoming a safe haven for fraud and crime and to enable consumers to resolve issues they have with the goods and services offered through a website, the Taskforce must require that the OPoC, registrars, and/or the domain name holder have protocols in place to address, within a set period of time, requests for information not published in Whois and to resolve complaints made to the OPoC about the operation of a commercial domain name. Otherwise consumer complaints, requests for information, letters of inquiry, subpoenas and other legal process may languish in the hands of the OPoC and allow the domain name holder to avoid legitimate consumer and law enforcement inquiries and demands for compliance with the law. In addition, registrars must be directed to keep requests made by law enforcement confidential in

¹⁹ See European Commission Internal Market DG, *Contribution of the European Commission to the general discussion on the Whois database raised by the Reports produced by the ICANN Whois Taskforce*, dated May 12, 2003.

²⁰ Report at 23-27 (describing five proposals regarding how the public could request and possibly obtain domain name holder contact information).

²¹ Report at 20.

order to preserve the integrity of undercover investigations.

5. *The accuracy of Whois data.*

The Taskforce has proposed that a registrar and either the domain name holder or his OPoC work together to address complaints and notices of inaccurate Whois data.²² Specifically, the registrar must notify the OPoC or domain name holder of a “notice of alleged inaccuracy” and the inaccuracy must be corrected. If the inaccurate data is not corrected, the registrar must take action in “a timely manner.”²³ While we support the Taskforce’s proposals for the improvement of the accuracy of Whois data in general, specific procedures and timetables for correcting Whois data must be adopted.

6. *The purpose of Whois.*

On April 12, 2006 the GNSO passed a resolution recommending that ICANN adopt a new definition of the purpose of Whois; a definition which the Taskforce used in drafting the proposals in the Report. This new definition states:

The purpose of the gTLD WHOIS service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS name server.²⁴

Based in part upon the importance of law enforcement access to the Whois database as it exists today, the Federal Trade Commission (“FTC”) requested that the GNSO reconsider its resolution recommending the adoption of this new definition.²⁵ The GNSO is currently re-evaluating its decision.²⁶ Because of the importance of the current Whois database to law enforcement and to consumers, we similarly encourage the GNSO to re-evaluate its revision of the definition of the purpose of Whois. We also encourage it to define the purpose of Whois according to the needs it has served thus far, including promoting the technical stability of the Internet at large, assisting law enforcement investigations and the enforcement of laws and

²² Report at 28-29.

²³ Report at 28-29.

²⁴ Report at 4.

²⁵ See FTC, *Prepared Statement of the Federal Trade Commission Before the Subcommittee on financial Institutions and Consumer Credit of the House Committee on Financial Services on Public Access to Whois Database*, July 18, 2006 (the “FTC Prepared Statement”) at 3-4.

²⁶ See FTC Prepared Statement at 3-4.

regulations, especially those that involve misuse of the Internet, and building user confidence in online commerce.²⁷

7. *ICANN's Draft Procedure for Handling Whois Conflicts with Privacy Law.*

On December 3, 2006, ICANN published a draft procedure outlining how registrars should handle conflicts between privacy laws and their current obligations under the Registrar Accreditation Agreements with ICANN to publish domain name holder contact information in Whois.²⁸ The draft procedure has five steps: (1) registrars notify ICANN of any "investigation, litigation, regulatory proceeding or other government or civil action" that "might" affect their contractual Whois publication obligations (hereinafter the "inquiry"); (2) registrars consult with ICANN about the inquiry with a view towards resolving it in a manner that preserves the publication of domain name holder information in Whois; (3) if the inquiry demands that registrars modify their Whois publication obligations, ICANN will prepare a public report and recommendation for the ICANN Board and the public; (4) the Board will pass a resolution; and (5) the resolution will be made public.²⁹ The draft procedure also recognizes that a registrar might be compelled to violate its contractual publication obligations prior to the completion of this five step process.³⁰ In this situation, ICANN may opt to refrain from enforcing the agreement against that registrar.³¹

ICANN's draft procedure provides a promising framework for addressing legitimate individual privacy concerns and compliance with applicable privacy laws while maintaining publicly available contact information for domain name holders. It describes a narrowly tailored yet flexible mechanism for addressing a practical problem with registrars' contractual obligations to publish individual contact information in Whois. That said, the draft procedure is vague on many critical points which would make its implementation problematic. For example, the draft does not make clear whether or not domain name holder contact information will be made available to the public while the registrars and ICANN are working through their review of potential privacy conflicts, it does not provide concrete time limits for any of the procedure's steps, and it does not describe means for law enforcement to obtain domain name holder contact information in the event it is removed from Whois while the review procedure is pending. The draft procedure therefore enables registrars to remove potentially large amounts of domain name

²⁷ See Governmental Advisory Committee, *GAC Principles Regarding Whois Data, Draft, V.3*, December 6, 2006 at 3.1; Whois Taskforce 1, *Restricting Access of Whois for marketing Purposes, Preliminary Report*, at Part II (discussing the principles for the use of Whois data).

²⁸ See ICANN, *DRAFT ICANN Procedure for Handling Whois Conflicts with Privacy Law*, December 3, 2006 ("Draft ICANN Procedure").

²⁹ See Draft ICANN Procedure, 3.1-5.2 (Steps 3, 4 and 5).

³⁰ See Draft ICANN Procedure, 2.3.

³¹ See Draft ICANN Procedure, 3.1.

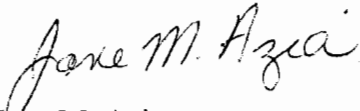
holder information from Whois for indefinite periods of time and leaves the public, including law enforcement, with no way to obtain it during that time.

8. *Tiered Access.*

Although not addressed in the Report, we are aware that “tiered access” has been discussed as a solution to providing third-party access to the direct contact information of a domain name holder in the event that this information is removed from the Whois database. Tiered access envisions different levels of access to Whois data depending on the identity of the data user.³² For example, the public could have real-time access to limited domain name information such as the registrar, name server, and the creation and expiration dates.³³ Law enforcement, meanwhile, would have password protected access to all Whois data, including the domain name holder’s contact information.³⁴ Absent any specific proposal outlining various levels of accessibility, we cannot comment further on this topic. Were such a proposal made, public discussion would be necessary. In addition, even if some form of tiered-access was adopted, we believe the public should continue to have real-time access to the complete registration information of a commercial website.

We thank you for the opportunity to submit these comments.

Submitted by,



Jane M. Azia
Assistant Attorney General In Charge, Internet Bureau
New York State Office of the Attorney General

³² See Governmental Advisory Committee, GAC Whois Working Group Discussion Paper, posted June 22, 2003, at point 4. See also Comparison of Whois Task Force 1 and 2 reports recommendations regarding tiered access and notification of data access to registrants.

³³ See Governmental Advisory Committee, GAC Whois Working Group Discussion Paper, posted June 22, 2003 at point 4.

³⁴ See Governmental Advisory Committee, GAC Whois Working Group Discussion Paper, posted June 22, 2003, at point 4.