Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

Philippa Lawson, Executive Director
(613) 562-5800 (2556)
plawson@uottawa.ca

June 17, 2004

Internet Corporation for Assigned Names and Numbers (ICANN)
Attention: Whois Task Force
4676 Admiralty Way, Suite 330
Marina del Rey, CA
90292-6601
USA

whois-tf1-report-comments@gnso.icann.org

Whois Task Force:

Re: Commentary on the Whois Preliminary Reports

We write to you to regarding your recent call for commentary on the preliminary reports concerning the Whois database and corresponding privacy issues.

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) is a legal clinic that educates and advocates on public interest matters involving the intersection of law and technology, in areas such as consumer protection in e-commerce, personal information protection, and privacy.[1]

The Whois database is a directory service which catalogs contact information (including the name, telephone number, and mailing and email addresses) for domain name Registrants. Although the Whois was initially developed to facilitate communication between network administrators and to aid in the resolution of technical problems, it has evolved with the development and popularity of the Internet, and is now used for a variety of purposes by businesses, network administrators, law enforcement agencies, and the general public.

Despite its utility, the availability of Registrants' personal information to the general public through the Whois database has raised numerous concerns. In October 2003, ICANN formed three Task Forces to the analyze privacy issues surrounding the Whois database.[2] On 28 May 2004, the Task Forces published preliminary reports and requested public comment on their findings and recommendations.[3] In an attempt to avoid repetition and for reader convenience we have consolidated our commentary on the three reports into a single document.

I. Whois Task Force 1: Restricting Access of Whois for Marketing Purposes

Problem: Registrant information is being harvested from the Whois database by marketers for marketing purposes.

We agree with the Whois Task Force 1 (WTF1) that current techniques to prevent the collection of personal information, or "data mining", from the Whois database are inadequate. CAPTCHA programmes and speed bumping techniques, while effective at limiting unsophisticated users, are easily circumvented by those experienced in online data collection.[4]

Contrary to statements by the Commercial and Business User Constituency that the use of Whois data for spamming purposes is "small", there have been numerous documented incidents of personal information being harvested from the Whois database for the purposes of sending unsolicited mailings.[5] For example, the Canadian Competition Bureau recently laid charges against the Internet Registry of Canada for sending misleading mail solicitations regarding the re-registration and transfer of domain names to Registrants whose domain names were about to expire.[6] While full details of the Canadian Competition Bureau's investigation into the Internet Registry of Canada are not known at this time, it is logical to assume that the domain expiry date and mailing addresses of the Registrants were obtained through the Whois database.

We support the WTF1's conclusion that the treatment of Registrant personal information, or "sensitive data", such as the Registrant's name, address, email address, and telephone number, should differ from the treatment of "non-sensitive data", such as the Registrar name and technical information. As pointed out in a letter to ICANN regarding the Whois database, to which CIPPIC was a signatory, a sensible Whois policy would improve contact-ability and data accuracy for network administrators, while restricting third party access to personal information.[7] It is our opinion that a two-tiered system should be implemented which provides public access to non-sensitive technical and operational information and restricted access to personal information.

Technical and operational data available to the public should be limited to the name of the Registrar, the renewal and registration date, and the primary server. Other information required for administrative and billing purposes (sensitive data) should be accessible only by the Registrar and Registry and used only for those purposes. In general, sensitive data should not be made available to third parties except where required by judicial order, or where the Registrant has expressly requested that specific data be disclosed (see section II for further discussion of consent to disclosure).

The Whois database was developed to assist network administrators in resolving technical problems; it was never intended to assist law enforcement agencies and intellectual property right holders in investigations. As discussed by the Non-Commercial Users Constituency (NCUC), while the desire to obtain information by law enforcement agencies and intellectual property rights holders may be legitimate, both have significant powers to command such information through due process procedures.

Further, we propose that Registrants should be notified immediately if a third party is granted access to their personal information. It is not enough that information regarding third party access is held by the Registrar and made available to the Registrant upon request as suggested by the At-Large Advisory Committee (ALAC). While we understand that there will be certain occasions where Registrars will be prohibited by Court order from communicating this information to Registrants, Registrars should generally be required to inform Registrants immediately of third party access to their personal information.

II. Whois Task Force 2: Review of Data Collected and Displayed

Problem: Registrant personal information is freely available to the general public through the Whois database, contrary to the desires and privacy rights of many registrants.

We agree with the Whois Task Force 2 (WTF2) that Registries and Registrars should not be forced to violate national laws in order to comply with ICANN regulations. Registrars are currently required through their agreements with ICANN to provide public access to Registrant data, including the Registrant's name, telephone number, and email and mailing address, in violation of many countries' privacy laws.[8] ICANN regulations should apply only to the extent that they do not conflict with applicable national laws regarding privacy or telecommunications.

We further agree with the WFT2 that (a) disclosure of personal information through the Whois system should be voluntary, and (b) that Registrars should obtain consent to the disclosure of data through the Whois directory separately from consent to other terms of service. Moreover, consent to the publishing of personal information through the Whois database should be obtained on an opt-in basis to ensure that consent has been intentionally provided. While Registrants who do business with the public may wish to publish their contact information so that consumers can verify the organization with whom they are dealing, Registrant personal information should, in general, not be accessible except by the Registrar and Registry for the technical, operational and administrative purposes outlined in their privacy policies.[9]

To make Registrant consent meaningful, the purposes of the collection, use, and disclosure must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.[10] We believe that there should be more conspicuous notice provided by Registrars regarding their privacy policies and, specifically, the collection, use, and disclosure of Registrant personal information. Registrars should be required to implement a system that ensures that Registrants have read and understood how their information will be collected, used, and disclosed before consenting to its public disclosure. Registrars should also be required to designate an individual within their organization for Registrants to contact should they have questions regarding their personal privacy.

One of the proposals put forward by the Commercial and Business User Constituency was the creation of a "White List" which would give access to Registrant personal information to certain organizations for certain purposes. As can be inferred from our above recommendations, we are opposed to the creation of a White List in any form.

The creation, implementation, and supervision of a White List would amount to an immense administrative and operational burden. There are no doubt hundreds of thousands of businesses and organizations which would seek access to the Whois database for purposes such as academic research or the creation of third party value-added services.[11] It would be nearly impossible to create a set of criteria outlining who should receive access and for what purposes. It would be even more difficult to ensure that organizations who are allowed access to personal information are limiting their use to the purposes for which access was granted.

It has also been suggested that law enforcement agencies and intellectual property rights holders be granted access to Registrant personal information for the purposes of law enforcement and the protection of intellectual property rights. As mentioned briefly above, the purpose of the Whois database is not to provide law enforcement and intellectual property right holders a mechanism through which to obtain contact information, but rather to assist network administrators in resolving technical problems.

Police and law enforcement agencies have considerable powers to obtain information through due process procedures. Similar to having to obtain a warrant in order to search an individual's home or car, law enforcement agencies should be restricted in their access to Registrants' personal information to situations where they can demonstrate to a judge the necessity for access.

Similarly, intellectual property right holders and other groups wishing to commence legal action against a domain name Registrant may apply to the courts for access to Registrant information held by Registrars in the same manner they do now for access to subscriber information held by Internet Service Providers (ISPs) in Canada. As pointed out by NCUC, the availability of Registrant contact information through the Whois directory has led to "flagrant" abuses by many intellectual property attorneys, including the sending of letters which threaten litigation and/or heavy fines if the Registrant does not comply with their demands.[12] Third parties should not be granted access to personal data merely upon allegations of intellectual property right infringement, defamation, or other civil wrongs.

III. Whois Task Force 3: Improve the Accuracy of Data Collected from Registrants

Problem: Registrants often provide Registrars with inaccurate information.

The Whois Task Force 3 (WTF3) was charged with developing mechanisms to improve the quality of Registrant contact information collected by Registrars. WFT3 did not provide any specific recommendations, and is still developing a proposed statement of best practices aimed at improving the accuracy of Registrant contact information to be included in the final report.

We agree, in large part, with the recommendations of the Whois Task Force III At-Large Advisory Committee (ALAC). ALAC suggested that Registrants whose data is inaccurate could be roughly divided into four categories:[13]

1. Those who purposely provide inaccurate data for fraudulent reasons.
2. Those who purposely provide inaccurate data to protect their privacy.
3. Those who mistakenly provide inaccurate data.

4. Those who provide accurate data at registration, but then fail to keep them up to date so that the information becomes inaccurate.

As pointed out by the ALAC, it is a waste of both time and effort to attempt to get accurate information from those who do not wish to provide it; those engaged in fraudulent activities are unlikely to provide accurate information voluntarily. WTF3 should instead concentrate on mechanisms to improve the accuracy of contact information for those Registrants falling into the other three categories.

We agree with the statements made by the NCUC that the best manner in which to improve the accuracy of Registrant contact information is to ensure the protection of Registrant personal information. Registrants concerned about their personal privacy will be more likely to provide accurate and up-to-date information if they can be ensured that third parties will not have unfettered access to this information.

In regard to those Registrants falling into the third category, we believe that Registrants who have mistakenly provided inaccurate data should be given the opportunity to correct the errors without penalty prior to the suspension of their domain name. Failure to properly correct errors within a reasonable amount of time (e.g. 30-45 days) should result in the suspension of the domain name registration. If the Registrant corrects the information during the suspension period, the Registrar should be required to reactivate the domain name. While we agree that the Registrar should be able to charge a fee for re-connection, we believe that this fee should be limited to recovery by the Registrar of the costs of re-registration. Failure to correct errors in contact information after suspension should result in the cancellation of the domain name registration after a reasonable amount of time (e.g. 10-15 days).

Finally, in dealing with the last category of Registrants, the ALAC properly pointed out that one of the primary reasons that Registrants fail to keep their data up to date is the inconvenient, difficult, and often complicated steps which must be undertaken in order to amend contact information. We suggest that all Registrars be required to provide an online mechanism which allows Registrants to access their personal information and make changes as necessary. Similar to above, Registrants who are found to have inaccurate data should be given the opportunity to correct the errors without penalty prior to the suspension of their domain name. Failure to properly correct errors in contact information should result in the suspension and, if not attended to, termination, of the Registrant's domain name.

IV. Summation

It is our primary belief that the Whois database should be limited in use to facilitating communication between network administrators and aiding in the resolution of technical and operational problems. Registrants have a legitimate and reasonable expectation of privacy and have legitimate reasons for concealing their personal information.

Whois data should not be openly available to law enforcement agencies, intellectual property rights holders, or the general public. It is well established that broad access to personal

information leads to spam, fraud and identity theft, and can be used for such purposes as stalking, harassment, and other violations of personal privacy.

We have suggested the implementation of a two-tiered system. Public access would be permitted to non-sensitive technical and operational information such as the name of the Registrar, the renewal and registration date, and domain name's primary server. Access to Registrant personal information would be limited to Registrars and Registries for solely administrative purposes and for the management of the Domain Name System and resolution technical problems except where expressly consented to by the Registrant. To make such consent meaningful, the consent to disclose personal information through the Whois database should be obtained separately, should outline what information will be disclosed, and should clearly explain that the Registrar will not be able to control the manner in which the information will be used by the public.

If you have any questions or concerns regarding this document, please feel free to contact us at (613) 562-5800 ext. 2553, or by email at cippic@uottawa.ca.

Sincerely,

Philippa Lawson
Executive Director
CIPPIC

Matthew Kindree
Research Fellow
CIPPIC

cc: Whois Task Force 2 <whois-tf2-report-comments@gnso.icann.org>
Whois Task Force 3 <whois-tf3-report-comments@gnso.icann.org>

---

[1] More information about the Canadian Internet Policy and Public Interest Clinic (CIPPIC) including our mission statement, our current project and cases, and the law and technology program at the University of Ottawa is available online at: www.cippic.ca.

[2] The descriptions of work for each of the Whois Task Forces are available at: http://gnso.icann.org/issues/whois-privacy/index.shtml.

[3] The full reports are available online at: http://gnso.icann.org.

[4] A CAPTCHA (an acronym for "completely automated public Turing test to tell computers and humans apart") is a type of challenge-response test used to determine whether or not the user is human. A common CAPTCHA requires that the user enter text displayed in a distorted .gif image. While originally very effective, programmers have been able to develop complex algorithms which allow computers to pass these tests with great accuracy. For more information on CAPTCHA visit the CAPTCHA project at: http://www.captcha.net.
Speed Bumping is a process that limits the amount of enquires that can be made by IP address during a given period of time. However, more sophisticated users can gain access and make queries from a number of different IP address.

[5] The recommendations and comments of the Commercial and Business Users Constituency is attached as an appendix to WTF1 Report on Restricting Access of Whois for Marketing Purposes available at the address noted above.

[6] For more information concerning this please visit the Competition Bureau's website at: http://competition.ic.gc.ca/epic/internet/incb-bc.nsf/en/ct02442e.html.
Two other prominent incidents of the abuse of Whois data are the cases of *Register.com v. Verio, Inc.* [*Register.com*] and *Federal Trade Commission v. Domain Registry of America, Inc.* [*DROA*]. In *Register.com* Verio was found to be 'mining' the personal information of Register.com customers for the purpose of email and direct mail solicitation. Similarly, in *DROA*, the Federal Trade Commission sought and received and an injunction which prohibited the DROA from harvesting Whois information and sending misleading mailings to consumers regarding the re-registration and/or transfer of their domain name registration.

[7] A copy of the letter is available at: http://www.thepublicvoice.org/news/whoisletter.html.

[8] For example, Canada's *Personal Information Protection and Electronic Documents Act (PIPEDA)* requires that an individual be supplied with a service even he or she refuses to consent to the disclosure of personal information (so long as the disclosure is not essential to the transaction). If a Registrant requests that their information not be disclosed through the Whois directory the Registrar will either be in violation of their agreement with ICANN if they comply with the request or in violation of Canadian law if they do not.

[9] See WTF2's preliminary report, footnote 20.

[10] This is one of the principles set out in Canada's privacy legislation, the *Personal Information Protection and Electronic Documents Act (PIPEDA)*. Under the Act, organizations collecting personal information are required to have personal information policies that are clear and understandable so that an individual has a clear understanding of why the information is being collected, how it will be used, and to whom it will be disclosed.

[11] The Commercial and Business User Constituency suggests in their recommendations to the WTF that the creation of third party value-added services is a legitimate use for which they should be granted access to Registrant personal information. What constitutes third party value-added services is not elaborated upon.

[12] Kathryn Kleiman, Esq., Co-Founder of NCUC and Internet Law and Policy Attorney states that: "as a telecommunications and intellectual property attorney in the mid-1990s, I was amazed to see the horrible letters sent to domain name registrants at their homes. These letters often were (and sometimes still are) outside the bounds of professional conduct. Taking advantage of the big vs. little discrepancy, and sensing the vulnerability of a domain name registrant for a small organization reached at his/her home, these letters threatened ongoing harassment, litigation, triple damages and even jail. Generally, the more threatening the letter, the less substantiated the claims, and some were downright reverse domain name hijacking. But people feel very scared by these letters.

[13] The full text of the At-Large Advisory Committee on the Whois Task Force III is available as an appendix to the preliminary report.