Canadian Journal of Law and Technology

Volume 4 | Number 1 Article 5

1-1-2005

Whazup with the WHOIS?

Sheldon Burshtein

Whazup with the WHOIS?

Sheldon Burshtein †

What Is the WHOIS?

The WHOIS is a database directory of domain names and relevant contact information maintained by each top-level domain (TLD) registry, which lists all relevant registrant contact information for each domain name registration. Through its contracts, the Internet Corporation for Assigned Names and Numbers (ICANN) requires registries and registrars to collect and display technical information and contact details for all registrants. The WHOIS is an important component of the domain name system (DNS). The WHOIS is used for a wide variety of purposes by registries, registrars, registrants, law enforcement authorities, consumers, and the general public. The WHOIS may enable identification of a domain name registrant or a Web site operator who registers or uses a domain name that violates trade-mark rights, or an Internet service provider (ISP) that hosts a site with infringing materials. In addition, the WHOIS enables trade-mark owners to conduct searches to avoid possible conflicts, and helps consumers to find out who is operating commercial sites. The .ca WHOIS may be seen at http://www.cira.ca.

In November 2004, the Canadian Internet Registration Authority (CIRA) proposed a new policy for the .ca WHOIS. This article summarizes the current state of WHOIS issues and focuses on the CIRA proposal.

Current WHOIS Issues

Questions have arisen as to which data should be collected and displayed in a WHOIS. The scope of information contained and made available in WHOIS databases, and their accessibility for data mining and other purposes has become a significant issue for those who operate and use the DNS. Among the serious problems with the current WHOIS system are: (i) inaccurate, false and incomplete registration data because many registrants use fictitious, misleading, or incomplete names and addresses; (ii) reduced searchability and functionality as compared to the prior Network Solutions, Inc. (NSI) system for the .com TLD; and (iii) the inability to access the WHOIS of all TLDs. In addition, the manner or format, and even the detail of information provided by the various registries is inconsistent. At least one TLD has an anonymous domain requiring only a mobile telephone and an e-mail address to register a domain name.[1]

The intellectual property community has asked ICANN to consider several measures which, by improving the transparency and functionality of the WHOIS, would make it easier for intellectual property rights holders to enforce their rights on the Internet. The community requested that the data be complete, updated, and accurate, with filters for obviously false data. The data should include the domain name, registrant name and address, e-mail and IP address, administrative zone, and technical and billing contacts in a form that is capable of real-time, unrestricted, and free boolean and combined searching for all TLD registries, with data given in consistent format irrespective of source. The information and functionality are needed to clear trade-marks and trade names for use and to enforce rights against registrants. Also requested are links to the registrar or registry sites for easy access to policies and contact information. However, there are competing interests. The first is that of individuals concerned with privacy, the second is that of those who use WHOIS data for business purposes,[2] and the third is that of registries, registrars and ISPs.

ICANN Task Forces

ICANN commissioned several task forces to examine how data is collected, displayed, and used and to recommend proposals for balancing the interests of all constituencies. First, a preliminary Task Force on WHOIS Accuracy and Bulk Access made a number of recommendations,[3] including that the use of bulk access WHOIS data for marketing should not be permitted. That Task Force said that the obligations contained in the relevant provisions of the Registrar Accreditation Agreement (RAA) should be modified to eliminate the use of bulk access WHOIS data for marketing purposes. It recommended a uniform, predictable, and verifiable

 Sheldon Burshtein is a partner of Blake, Cassels and Graydon LLP, Barristers & Solicitors and Patent & Trade-mark Agents, and practices in the Intellectual Property and Technology Group in the Toronto Office.

mechanism for the enforcement of the WHOIS-related provisions of the agreements. At least annually, a registrar should be required to present to a registrant the current WHOIS information for each registration, and remind the registrant that the provision of false WHOIS information can be grounds for cancellation of the registration. When a registration is deleted on the basis of false contact data or a failure to respond to a registrar inquiry, a grace period should be available. However, the domain name should be placed in registrar hold status until the registrant provides updated WHOIS information to the registrar. Subsequently, three other task forces were struck.

Task Force 1 focused on methods for restricting access to WHOIS data for marketing purposes to prevent data mining of the WHOIS database.[4] It concluded that the current mechanisms to limit data mining of the WHOIS database for marketing purposes are of limited success. It is not possible under the current specifications to create technical restrictions that will limit access for a specific purpose. Some members stated that they may not be opposed to having an automated mechanism to retrieve sensitive data for identified requestors with approved purposes, provided that certain terms and conditions apply, including: (i) entry of an electronic licensing agreement; (ii) identification of the requestor to the registrar, (iii) disclosure of the identity and purpose of the request to the registrant, with some exceptions; and (iv) the supply of data in human-readable form only. The Task Force recommended that, to the extent that data deemed to be sensitive by the Internet community was to be publicly disclosed by WHOIS Task Force 2, at a minimum, the requestor of WHOIS information should be required to identify itself to the registry, along with the reasons for which it seeks the data. Such information should be made available to the registrant whose WHOIS information is sought.

Task Force 2 reviewed the types of data collected by registrars and displayed in the WHOIS database.[5] It recommended that ICANN should encourage development of practices that will improve the effectiveness of giving notice to, and obtaining consent from, registrants for uses of registrant contact data. ICANN should incorporate compliance with the notification and consent requirement as part of its overall plan to improve registrar compliance with the RAA. It also recommended further inquiry into proxy registration services provided by registrars. The Task Force recommended tiered access (discussed in the next section).

Task Force 3 considered ways of improving the accuracy of the WHOIS database.[6] Among its recommendations were that ICANN should: (i) determine whether the current registrar contractual terms are adequate or need to be changed to encompass improved data accuracy standards and verification practices; (ii) solicit input from each registrar relating to its current level of compliance with existing agreements and plans to improve the accuracy of the data it collects; (iii) develop and implement a graduated scale of sanctions that can be applied against those who are not in compliance with their contractual obligations; (iv) work with registrars to create best practices to determine reasonable efforts to investigate inaccuracies in contact data; (v) specifically examine registrar data collection practices, including all options for the identification and viability of automated and manual verification processes, and the use of readily available databases to assist in data verification; (vi) consider including "last verified date" and "method of data verification" as WHOIS data elements; (vii) require registrants to update and correct WHOIS data on an annual basis; and (viii) consider requiring registrars to verify at least two of three registrant contact methods (telephone, facsimile, and e-mail).

Tiered Access

Task Force 2 recommended a system that provides different data sets for different uses and/or users to balance the privacy interests of registrants with the ongoing need to contact those registrants by other members of the Internet community. Technical and operational details about the registration should continue to be displayed to the public on an anonymous basis. The provision of some basic contact information may also be appropriate. Further contact details for the registrant and administrative contact would only be available in one or more protected tiers. Those meeting the requirements and identifying a legitimate use to access protected information should be able to obtain it in a timely manner after identifying themselves in a verifiable manner. There must be a legitimate use for each instance of access of protected data. Registrars and registries should continue to have full access to the WHOIS data for technical and operational purposes.

However, Task Force 2 also identified several issues that still must be resolved before a tiered access system can be implemented. It must be determined what process of notification to registrants, if any, should take place when their protected data is accessed other than in circumstances required by law or contract, such as the provision of contact information to dispute resolution providers during a dispute, or to another registrar during a transfer. It must be decided which contact data should be shown in the protected tier. ICANN will have to consider what mechanisms are available for identifying and authorizing those requesting access to protected information, and who will administer them, using what criteria. The costs of implementing technology standards to support such a tiered access system must also be considered.

Both Task Forces 1 and 2 assumed that some authentication mechanism would need to be in place to require WHOIS requesters to identify themselves to the

WHOIS provider. This is also a dramatic change from the present situation, in which WHOIS queries can generally be made on an anonymous basis. In addition, there was significant discussion by those Task Forces about whether and when the identity of the WHOIS requestor should be revealed to a registrant about whom information is sought.

Gaining entry to the "upper tier" of the tiered system would also require satisfying some set of qualifications about the purpose of the request and the use to which data results could be put. Some participants stressed that an entity should be able to qualify once and receive a credential that would enable it to access WHOIS data from all domain name registrars and registries as an "upper tier" user. This is a so-called "white list" approach. Others took the position that not only the identity of the requester, but also the purpose of each individual request, would need to be verified before access to the data would be allowed. This is the "individual list" approach.

Of particular interest to the intellectual property community are the recommendations relating to a tiered access system. Contact data submitted by domain name registrants has long been immediately available to the general public on an anonymous basis, for free, and with only limited restrictions on how the data can be used. A tiered access system would be a fundamental change to the present system. Tiered access would treat different WHOIS requesters differently in terms of the range of data to which they would have access. The general public would have access only to technical data and perhaps minimal contact data. The higher level of access would return more complete contact information for the registrant and administrative contact. The limitation to technical data in public WHOIS queries would reduce data mining because technical data is unattractive to data miners. A tiered system would protect the privacy of individual registrants, while still allowing legitimate users to access that information.

Legal Developments

The WHOIS has also been the subject of legislative initiatives and judicial decisions. In the United States, legislation has recently been enacted to amend trade-mark and copyright legislation to provide for greater damages against infringers who provide false information when registering a domain name used in *infringing intellectual property and for prison terms for such falsification.* [7]

On the judicial front, a United States appellate court has held that a registrar restriction on use of WHOIS data that is not initially seen, but appears only after the data is received, is enforceable when the querying party returns to the site to gather more data.[8] An ISP repeatedly retrieved registrant information from a registrar's WHOIS database and used the information for e-mail, telemarketing, and direct mail solicitation. A legend on the WHOIS prohibited this practice, but the legend was not seen until after the data was downloaded. Further, the restrictive legend contravened the terms of the registrar's RAA with ICANN. The Court held that the ISP could not rely on the RAA because the ISP was not a party to it. The Court granted a preliminary injunction against the ISP's activity, since the defendant knew of the restriction as a result of its numerous daily inquiries.

An Australian court has held that reproduction of a portion of the .uk WHOIS database constitutes copyright infringement, and that the sending of misleading notices to registrants in the database is a violation of Australian fair trading laws.[9] A group of linked Australian businesses and individuals data mined 50,000 United Kingdom-based registrants from the .uk WHOIS and sent correspondence that falsely suggested a connection with Nominet, the operator of the .uk registry.

National Initiatives

A number of ccTLDs are considering their positions regarding the WHOIS. For example, InternetNZ, the operator of the New Zealand .nz ccTLD has commenced a WHOIS policy review.[10]

At present, most of the technical and contact information collected from registrants is publicly available through the WHOIS directory on CIRA's Web site, including administrative and technical contact details (name, postal address, e-mail address, and telephone number) and technical information about the .ca domain name, such as DNS numbers and server IP names and numbers. Most of the other WHOIS directories make similar information available.

However, it is generally not possible to search the WHOIS database of most registries, including the .ca registry, by name of registrant. Therefore, it is very difficult to compile information regarding a pattern of multiple registration, as is sometimes required to establish bad faith in a proceeding under a domain name dispute resolution policy, such as the *CIRA Domain Name Dispute Resolution Policy (CDRP).*[11] Some have suggested that CIRA should expand and improve its WHOIS database capabilities.[12]

It is, though, possible to obtain from CIRA a list of all .ca domain name registrations in the name of a registrant on a request made pursuant to CIRA's *Registration Information Access Rules and Procedures (Access* Rules).[13] The request must identify the requesting party and, if the requestor is different from the potential complainant, the potential complainant. The request must identify a mark to which at least one domain name is confusingly similar and identify the registrant. The requesting party must certify that: (i) it or the person on whose behalf the request is being made has rights in a mark identified in the request; (ii) the requesting party is

eligible to initiate a proceeding under the CDRP or is validly authorized by an eligible person; and (iii) the request is made in good faith for the purpose of deciding whether to initiate a CDRP proceeding against the named registrant, and for no other purpose. The request must be made to CIRA in the applicable form, which must be completed, signed and sent by postal mail or courier.

CIRA reserves the right not to respond to a request that it believes for any reason is not made for the stated purpose. This may effectively permit CIRA to screen the provision of information; for example, if CIRA is of the view that none of the complainant's marks is at least arguably confusingly similar to at least one of the registrant's domain names. If the request complies with the Access Rules, CIRA provides a list to the requesting party and, within 10 business days of receipt of the request, CIRA uses reasonable commercial efforts to send an e-mail to the administrative contact e-mail address of the registrant for the relevant domain name registration(s) indicating: (i) what parts of the information CIRA disclosed; and (ii) to whom CIRA disclosed it.

Currently, CIRA discloses personal information, other than via the WHOIS and the Access Rules, only: (i) in the event that a law enforcement agency, court of competent jurisdiction, tribunal, judicial board, administrative body, judicial commission, or any other judicial body of competent jurisdiction requests personal information by way of an order, ruling, decision, subpoena, warrant, or judgment; (ii) pursuant to the *Personal Information Protection and Electronic Documents Act (PIPEDA);* [14] or (iii) if the domain name is subject to a proceeding under the CDRP, to the relevant dispute resolution provider. Unless prohibited by law, within 10 business days of receipt of the request, CIRA uses reasonable commercial efforts to send an e-mail to the administrative contact e-mail address of the registrant for the relevant domain name registration(s) indicating: (i) what parts of the information CIRA disclosed; and (ii) to whom CIRA disclosed it.[15]

CIRA WHOIS Proposal

During 2004, CIRA conducted its own consultation on the publication of registrant information with the view to ensuring that its policies and procedures comply with PIPEDA. In November 2004, CIRA introduced a proposed *WHOIS Policy.*[16] According to CIRA, the WHOIS is designed to provide limited information to site visitors about registered .ca domain names for several purposes: (i) to allow network administrators to find and fix system problems and generally to maintain the stability of the Internet; (ii) to help combat inappropriate uses of the Internet, such as spam or fraud; (iii) to facilitate the identification of instances of trade-mark infringement; and (iv) generally, to enhance the accountability of .ca domain name registrants.[17] CIRA's proposed approach is to provide different rules for individual registrants[18] than for others,[19] and to provide a means to access non-published information from CIRA in defined circumstances.[20]

CIRA proposes that, for each domain name registration in the name of an individual who is a Canadian citizen, permanent resident, legal representative, or aboriginal person, the WHOIS would only make accessible: (i) the domain name; (ii) the registrar's name; (iii) the expiration date; (iv) the registration date; (v) the last changed date of registration; (vi) whether the registration has been suspended or is in the process of being transferred; (vii) the IP address of the primary name server and secondary name server(s); (viii) if applicable, the other servers; and (ix) the corresponding names of those name servers.[21]

For the reasonable purposes of the operation of the registry and to facilitate registrar to registrar transfers, registrant to registrant transfers, the addition of new domain name registrations to an existing individual registrant's profile, and any other transaction for which the relevant registrar who is not the registrant's registrar of record reasonably requires additional registration information, as determined by CIRA at its reasonable discretion, the following information would be disclosed to the relevant registrar for each relevant registration: (i) the individual's registrant name; (ii) the category of registrant identified during the application procedure; (iii) the individual's registrant number assigned by CIRA; (iv) the *registration number assigned by CIRA; (v) the registrant's postal address, e-mail address, telephone number and,* where available, facsimile number; (vi) the name, postal address, e-mail address, telephone number and, where available, facsimile number of the administrative contact; and (vii) the name, postal address, e-mail address, telephone number and, where available, the facsimile number of the authorized representative (collectively, "Protected Information").[22] An individual registrant may voluntarily opt to disclose more registration information, including the Protected Information, in the WHOIS.[23]

For registrants other than individuals, all registration information collected by CIRA would be made accessible to the public through the WHOIS no less than 31 days after the date of registration. However, registrants other than individuals may request, in writing via postal mail, that the Protected Information not be disclosed to the public in the WHOIS. CIRA would, at its reasonable discretion, permit such a request. If CIRA accedes to the request, Protected Information would only be disclosed thereafter in accordance with the terms for disclosure applicable to individual registrants.[24]

Any person may use the WHOIS service, provided it is only: (i) to query the availability of a domain name; (ii) where permitted, to identify the holder of a domain name; and/or (iii) where permitted, to obtain contact and/or other information concerning individual registrants and non-individual registrants and the domain

names that they have registered and concerning registrars, administrative contacts and authorized representatives.[25] Information acquired from the WHOIS must not be used for any purpose other than the foregoing. Purposes that are prohibited include, but are not limited to, the carrying out of any activities that are unsolicited and can reasonably be viewed as involving: (i) the harvesting of electronic or other WHOIS addresses for the purpose of transmitting by e-mail, telephone, facsimile, or regular mail any commercial advertising; (ii) the performance of market research; (iii) solicitation activities; and (iv) any other purposes that may be reasonably viewed as intrusive to a reasonable domain name registrant. No user of the WHOIS is permitted to utilize automated or electronic processes that send queries or data to the WHOIS, except as is reasonably necessary to register domain names or modify existing registrations.[26]

Comment

If the proposed .ca WHOIS policy is adopted, .ca registrants, especially individuals, would be entitled to more restrictive disclosure of information through the WHOIS than most other TLD registries. There are arguments both in favour of, and against, the proposed policy.[27] One stated reason favouring the proposed policy is that the present policy of publishing contact information for individuals is instituted without consent and does not comply with PIPEDA. However, it is submitted that the CIRA Registrant Agreement expressly provides CIRA with consent to disclose information, including the registrant's name.[28] A second reason is that it is not necessary to release the contact information for individual registrants in order to hold them accountable. A third stated reason is that individuals are more vulnerable than businesses or organizations to harmful privacy breaches because they lack the same resources to protect themselves.

The main argument against keeping contact details for individual registrants private is that it is necessary to make such information publicly available in order to hold them accountable. A second stated reason is that those who do not violate rights or the law have no cause for concern. Interestingly, the CIRA report does not even reference in the executive summary the need for private interests, such as intellectual property owners, to have access to such information immediately, without condition, and without disclosure of their interest. Intellectual property owners will, no doubt, advocate for greater disclosure on this basis.

The evolution of the WHOIS databases of different TLDs will be matters of both interest and importance to all users of the Internet, especially intellectual property owners.

Notes:

[1] i.ph, DotPH, the Domain Registry of the Philippines.

[2] *Register.com Inc. v. Verio, 69 U.S.P.Q. (2d) 1545 (C.A. 2004), affirming 63 U.S.P.Q. 2d 1957 (S.D.N.Y. 2000); and Nominet UK v. Diverse Internet Pty. Ltd., [2004] FCA 1244 (Federal Court of Australia).*

[3] http://www.icann.org/gnso/whois-tf/report06feb02.htm.

[4] http://gnso.icann.org/issues/whois-privacy/*whois%20TF%201%20-%20preliminary%report%20V2.%201.0.pdf.*

[5] http://gnso.icann.org/issues/whois-privacy/TF2%20Initial%20Report3.pdf.

[6] http://gnso.icann.org/issues/whois-privacy/*TF3PreliminaryWithRCMR1.pdf.*

[7] United States *Fraudulent Online Identity Sanctions Act, Pub. L. 108–482.*

[8] *Register.com Inc. v. Verio, supra, note 2.*

[9] *Nominet UK v. Diverse Internet Pty Ltd., supra, note 2.*

[10] "WHOIS Policy Review", http://dnc.org.nz/content/whois.pdf.

[11] http://www.cira.ca.

[12] Treasury Board Secretariat Submission to CIRA, October 2001, http://*www.cira.ca.*

[13] http://www.cira.ca.

[14] S.C. 2000, c. 5.

[15] *CIRA Privacy Policy, http://www.cira.ca, section 6.*

[16] *CIRA Privacy Policy, Draft for Consultation, November 12, 2004, http://www.cira.ca, section 6.0.*

[17] *Id., section 6.1.*

[18] *Id., sections 6.1.1 and 6.1.2.*

[19] *Id., section 6.1.4.*

[20] *Id., section 6.1.3.*

[21] *Id., section 6.1.1.*

[22] *Id., section 6.1.2.*

[23] *Id., section 6.1.3.*

[24] *Id., section 6.1.4.*

[25] *Id., section 6.1.5.*

[26] *Id.*

[27] *A Report to CIRA: Findings From Public and Stakeholder Consultation on the Development of a Revised WHOIS Policy, The Strategic Counsel, April 2004.*

[28] CIRA Registrant Agreement, Section 4.1(*a*).