

July 25, 2005

IPC Constituency Statement – Background Paper
ICANN Task Force Terms of Reference 1

Purpose of the Whois Database

Term of Reference #1 is to define the purpose of the Whois database in the context of (1) ICANN's mission and relevant core values, (2) international and national laws protecting privacy of natural persons, (3) international and national laws that relate specifically to Whois services, and (4) the changing nature of Registered Name Holders. As explained in detail below, a free and publicly accessible Whois database is consistent with the purpose of the database in each of these contexts.

A. ICANN's Mission and Relevant Core Values

Pursuant to ICANN's mission statement (2) and core value (1),¹ requiring registrars to provide free, public access to accurate Whois data is necessary as part of ICANN's mission to coordinate the operation and evolution of the DNS root name server system to ensure a reliable and secure Internet. Open access to Whois data helps to ensure that domain names can be relied upon by the public to reach their intended destinations and in general to help ensure accountability for online activity. Accountability, in turn, further promotes the goal of online security, as it helps to ensure that those who choose to operate online behave in ways that do not threaten or undermine the security of the Internet. Indeed, reducing public access to Whois would be detrimental to the proper functioning of the Internet, to current Internet dispute resolution fora, and to a broad range of stakeholders.

Moreover, in the online environment, open access to accurate Whois data is especially crucial, as there may be little or no other opportunity for consumers or the public to verify with whom they are dealing. Open access to Whois data may be the only opportunity one has to determine who owns a particular domain name, or controls a particular website or other online resources with which the domain name is associated. Lack of such transparency increases the risk that some domain name owners may become emboldened to use their sites in ways that would have unpredictable consequences not only for reliability and security of the Internet in general, but also the underlying technical operation of the Internet as well.

B. International and National Laws Protecting Privacy of Natural Persons

¹ See <http://www.icann.org/general/bylaws.htm>.

The IPC does not purport to be experts in every potential international and national law that may protect the privacy of natural persons. However, we do wish to make some observations regarding some of the more well known laws.

1. European Data Protection Directive

The Data Protection Directive² requires organizations that process information that identifies an individual (“personal data”) to do so in accordance with a number of data protection principles. “Processing” is defined in Article 2(b) of the data protection directive as including the “disclosure by transmission, dissemination, or otherwise making available.” As discussed in detail below, a publicly accessible, complete, and accurate Whois database is both necessary and consistent with the Directive.

Personal data may be processed in several circumstances that would allow for the public dissemination of Whois data. In particular, Article 7(a) of the Directive provides that personal data may be processed if the person has “unambiguously given his consent.” Section 3.7.7.5 of the Registrar Accreditation Agreement already requires registrars to obtain consent from registrants to the processing of their contact information, including specifically a notification of the recipients of the data (i.e. the public via the Whois database). To the extent there is any concern that some registrars are not providing adequate notice, it would be a relatively simple matter to require improved notice that satisfies the Directive, rather than scuttling Whois as allegedly inconsistent with the Directive.

Even in the absence of such express consent, Article 7(e) of the Directive still allows processing of personal data if “necessary for the performance of a task carried out in the *public* interest.” (emphasis added). There is no requirement that the entity performing the task itself be a public entity. In addition, Article 7(f) allows processing if “necessary for the purposes of the legitimate interests pursued by . . . the third party or parties to whom the data are disclosed” -- in other words, for a legitimate *private* interest.³ An open Whois database promotes the effective enforcement of intellectual property rights, which is *both* in the public interest and a legitimate private interest.

Enforcement of intellectual property rights is in the public interest because it prevents consumers from being confused or deceived, and thereby enhances consumer trust and confidence in online commerce. In fact, the April 2004 European Union

² See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett..

³ See also Article 13(1)(g) of the Data Protection Directive allowing member states to restrict the rights of individuals provided under various articles of the directive when necessary to safeguard the “rights of others.”

Directive on Enforcement of Intellectual Property Rights states, “the protection of intellectual property is an essential element for the success of the internal market. The protection of intellectual property is important not only for promoting innovation and creativity, but also for developing employment and improving competitiveness. In this respect, the *means of enforcing intellectual property rights are of paramount importance* for the success of the internal market.”⁴ Ready access to contact information in the Whois database is precisely the type of tool that enables intellectual property owners to enforce their rights.

The EU Enforcement Directive also states that “[i]nfringements of intellectual property rights appear to be increasingly linked to organized crime. Increasing use of the Internet enables pirated products to be distributed instantly around the globe. Effective enforcement of the substantive law on intellectual property should be ensured by specific action at [the] community level.”⁵ Thus, European law specifically recognizes that abuse of intellectual property on the Internet is particularly harmful to the public.

In addition, the ECJ has held in a decision on the rights of trademark holders that enforcement of intellectual property is a legitimate private interest. The court confirmed that not only does trademark law protect consumers, but also “the proprietor [who] must be protected against competitors wishing to take unfair advantage of the status and reputation of the trade mark by selling products illegally bearing it.”⁶

The public interest in the enforcement of intellectual property and the need to recognize the legitimate interest of right holders have been spelled out in more detail and confirmed in the national legislation of European Union member states, e.g. in the French data protection law as updated in 2004,⁷ creating a specific set of rules for right holders and collecting societies to ensure effective management and enforcement of copyright.

Article 6(1)(c) of the Data Protection Directive also requires that personal data must be “adequate” in relation to the purpose of the collection of the data. In view of the implicit purpose of the Whois database to provide information regarding the domain name owner to help resolve intellectual property disputes as discussed above, the publicly accessible portions of the database should contain information sufficient to enable an intellectual property owner to readily contact the domain name holder to facilitate the resolution of any potential violation of law that otherwise might generate consumer confusion or worse, as well as to carry out further investigation and, where

⁴ Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights (emphasis added).

⁵ *Id.*

⁶ *See, inter alia, Hoffmann-La Roche*, paragraph 7, and *Case C-349/95 Loendersloot* [1997] ECR I-6227, paragraph 22.

⁷ LOI 2004-801 (6 August 2004) amending Loi 78-17.

necessary, serve court papers. This is to everyone's benefit, as it can expedite the resolution of conflicts with a minimum – and often without any – expenditure of private or public resources on court proceedings that could have been avoided with one letter or phone call.

The provision of contact information regarding individuals facilitates the enforcement of national laws, including legislation protecting consumers and intellectual property. This interest is taken very seriously in the EU, as documented in the EU Electronic Commerce Directive (2000), requiring every person or entity offering “information society services” to identify itself and supply relevant contact information.⁸ After all, whether or not they are subject to the EU E-Commerce Directive requirements, individuals may commit fraud, deceive customers, trade in illicit material, infringe intellectual property rights and otherwise engage in unlawful acts. Indeed, though statistics are hard to come by, it is quite likely that most unlawful activity that takes place online is done over websites owned by individuals rather than corporations. Limitations on access to this contact information would only serve to encourage the abuse of intellectual property, generate public confusion, and increase the amount of unlawful activity online.

In sum, a free and public Whois database, which facilitates protection of intellectual property rights on the Internet, is consistent with the Data Protection Directive.

2. Canadian Personal Information Protection and Electronic Documents Act

The disclosure of personal information is governed in Canada by the Personal Information Protection and Electronic Documents Act (“PIPEDA”).⁹ Several sections are applicable to the Whois database in the .ca ccTLD, and by extension are relevant to an analysis of the Whois database in the gTLDs.

Section 3 of PIPEDA provides that “[t]he purpose of this part is to establish . . . rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.” There is a public interest in the protection of intellectual property

⁸ See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, available at http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32000L0031&model=guichett.

⁹ S.C. 2000, c. 5.

rights, which a reasonable person would consider appropriate in making information available via the Whois database. In fact, of the adult Canadians surveyed by The Strategic Counsel for CIRA, “the plurality (44%) supports the availability of this [contact] information.” Further, among existing registrants, “almost half of individuals (48%) and more than half of organizations (54%) support the availability of contact information.” Finally, “[a] majority (62%) of registrars support the public availability of contact information for registrants. . .”¹⁰ These survey results show that public disclosure of contact information via CIRA’s Whois service is viewed as “reasonable” by a plurality if not a majority of Canadians.

The Supreme Court of Canada in *Ciba-Geigy Canada Ltd. v. Apotex Inc.* has recognized the consumer protection value of protecting trademarks, stating as follows:

[I]t should never be overlooked that . . . unfair competition cases are affected with a public interest. A dealer’s good will is protected, not merely for his profit, but in order that the purchasing public may not be enticed into buying A’s product when it wants B’s product. . . Accordingly, the power of the court in such cases is exercised, not only to individual justice, but to safeguard the interests of the public. . . The ordinary customer, the consumer, is at the heart of the matter here.¹¹

Section 4.3 of Schedule 1 to PIPEDA states that “[t]he knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.” This is consistent with Sections 3.7.7.4 and 3.7.7.5 of the Registrar Accreditation Agreement.

Section 4.3.2 of Schedule 1 to PIPEDA states that “organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.” Again, this is consistent with Sections 3.7.7.4 and 3.7.7.5 of the Registrar Accreditation Agreement.

Section 4.3.5 of Schedule 1 of PIPEDA states, “the reasonable expectations of the individual are also relevant.” With respect to existing Whois service in the gTLDs, the historical expectation of individual registrants has been for full disclosure of contact information. There is no indication that the expectations of individual registrants have changed in this respect.

PIPEDA and its exemptions recognize that a balance must be struck between privacy rights and the free flow of information for the proper functioning of systems of registries of ownership and rights intended for the benefit of all members of the public. While it has traditionally been the case that such registries are government-run, the fact

¹⁰ See The Strategic Counsel, *A Report to CIRA 37-38*, available at <http://www.cira.ca/en/Whois/documents/TSC-CIRA-pub-report-en.pdf>.

¹¹ [1992], 3 S.C.R. 120, pages 136-137, internal case cites omitted.

that the domain name system with its accompanying Whois database is non-governmental does not alter its fundamentally public purpose.

Making it more difficult to identify domain name holders does not serve the purpose of the Whois database. Delay in identifying an infringer of intellectual property rights would only prolong the public's confusion and perhaps even prolong fraudulent or criminal activity by unscrupulous domain name owners.

C. International and National Laws that Relate Specifically to Whois Services

Though perhaps not “law,” ICANN’s own Uniform Dispute Resolution Procedure contemplates full and open access to the Whois database. Specifically, Section 4(b)(ii) of the policy provides that evidence of “bad faith” may consist of a registrant who has “registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that [the registrant has] engaged in a *pattern of such conduct*.”¹² Determining whether a “pattern” exists requires access to ownership information – i.e. the Whois database. There is no exemption for domains owned by individuals or used for non-commercial purposes.

Similarly, in the United States the Anti-cybersquatting and Consumer Protect Act,¹³ evidence of bad faith may consist of a registrant’s “registration or acquisition of *multiple domain names* which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties.” Thus, the ability of trademark owners to readily determine what other domain names are owned by a potential cybersquatter is already enshrined in both ICANN policy and U.S. anti-cybersquatting legislation.

Furthermore, the United States has just adopted the Fraudulent Online Identity Sanctions Act.¹⁴ FOISA adds a new Section 35(e) to the Trademark Act that provides that a violation of the Act is presumed willful if the violator willfully provided materially false Whois contact information in registering, maintaining, or renewing a domain name used in connection with the violation. A similar change was made to Section 504(c) of the Copyright Act. FOISA also increases by up to seven years the

¹² See <http://www.icann.org/udrp/udrp-policy-24oct99.htm>. Furthermore, Rule 2(a)(i) governing UDRP proceedings provides that a dispute resolution provider can satisfy its obligations to use “reasonably available means” to contact the domain name owner by addressing communications to the contact information in the Whois database. See <http://www.icann.org/dndr/udrp/uniform-rules.htm>.

¹³ Adopted as Title III of Pub. L. No. 106-113, available at <http://www.patents.com/acpa.htm>.

¹⁴ Pub. L. No. 108-482.

maximum prison time for a felony criminal offense where the defendant falsely registered a domain name and knowingly used that domain in the course of the criminal offense.

Clearly, FOISA was enacted to help combat the problem of false Whois data, rather than to restrict access or otherwise encourage the provision of false data. This is consistent with the view of the purpose of the Whois database as a public resource of accurate information so that domain name owners can be readily contacted whenever there is a problem of any kind associated with a domain name.

D. The Changing Nature of Registered Name Holders

With the growth of the use of the Internet, and in particular commercial use of the World Wide Web since the mid-1990's, the typical registered name holder has changed dramatically since the early days of the Internet. No longer the sleepy province of academics, the military, and government users, the Internet today is an active, bustling marketplace of commerce, information, and ideas. Thus, the changing nature of domain name owners, in an online world where consumers may be defrauded before they have any reason to be suspicious, is even more reason to recognize that one of the purposes of open, public access to Whois data is to ensure that consumers (including intellectual property owners acting on their behalf) can verify who is operating a particular website. As well, since time is often of the essence in resolving disputes that arise online, victims of fraud and other complainants must pursue wrongdoers quickly in order to protect their rights and minimized damage. This is all but impossible unless basic information about a domain name registrant is not immediately available to the public.

It has sometimes been said that the original purpose of the Whois database was allegedly "to give people who operate networks a way of contacting the person technically responsible for another network, another domain, when there was a problem."¹⁵ However, the notion that Whois was intended only to ensure the efficient technical operation of the Internet is too restrictive and is not supported by the historical record. As discussed below, the original purpose of the Whois database was in fact not limited only to use for resolving technical issues, but rather to allow any person to contact any other person who had obtained an online address, regardless of purpose.

A review of the Requests for Comments by Internet architects establishing and later further developing the Whois database,¹⁶ as well as other relevant documents,

¹⁵ See Article 29 Working Party Opinion 2/2003 on the application of the data protection principles to the Whois directories, available at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp76_en.pdf.

¹⁶ See <http://www.faqs.org/rfcs/>.

demonstrates that use of the database to facilitate the enforcement of private rights – including intellectual property rights – is compatible with the original purpose of the database.

1. RFC 812

The Whois database can be traced back to at least as early as 1982, during the days of ARPANET, the U.S. Department of Defense’s precursor to today’s Internet. RFC 812 provided as follows:

The NICNAME/WHOIS Server . . . provides netwide directory service to ARPANET users. It is one of a series of ARPANET/Internet name services maintained by the Network Information Center (NIC) at SRI International on behalf of the Defense Communications Agency (DCA). The server is accessible across the ARPANET from user programs running on local hosts, and it delivers the *full name, U.S. mailing address, telephone number, and network mailbox for ARPANET users*. This server, together with the corresponding Identification Data Base[,] provides online directory look-up equivalent to the ARPANET Directory. DCA strongly encourages network hosts to provide their users with access to this network service.¹⁷

There is no restriction in RFC 812 on the uses or users of the Whois database. Rather, the service is described as a “netwide directory service” available to all users. Indeed, it is not surprising that in 1982 there was no express reference to allowing use of the Whois database for the enforcement of intellectual property rights. In 1982, the World Wide Web had yet to be invented, and commercial traffic on the Internet was non-existent. Thus, there was no need to expressly state that the Whois database could be used for intellectual property enforcement. Nonetheless, the fact remains that the original Whois database was open to use by all, for any purpose without limitation.

2. RFC 954

Continued development of ARPANET led to RFC 954 in October 1985, which further established Whois as a central directory service for everyone connected to the network. Similar to its predecessor RFC 812, RFC 954 stated:

The NICNAME/WHOIS Server . . . provides netwide directory service to **Internet users**. . . The server . . . delivers the *full name, U.S. mailing*

¹⁷ RFC 812, available at <http://www.faqs.org/rfcs/rfc812.html> (emphasis added).

address, telephone number, and network mailbox for DDN [Defense Data Network] users who are registered in the NIC database.¹⁸

It is particularly noteworthy that RFC 954 specifically refers to Whois directory services being provided to “Internet users,” which encompass all users. If the original purpose of the Whois database had really been for resolution of technical issues only, it would have been a simple matter for RFC 954 to refer to Whois directory services being provided only to “technical personnel,” “engineers,” or the like.

ICANN’s original Task Force 1, charged with studying various aspects of the Whois system, also recognized the absence of any limitation on the use of Whois data, finding that RFC 954 “does not set forth the reasons why such [Whois] data should be collected.” Furthermore, Task Force 1 found only that “it has been argued” by some in the “technical community” that the purpose of the Whois database was limited to resolution of technical issues.¹⁹ This is certainly not a finding that the original purpose of the Whois database was unequivocally so limited.

3. RFC 1834

As the Internet as we know it today began to take shape, RFC 1834, issued in 1995, provided as follows:

The Network Information Center (NIC) maintains the central NICNAME database and server, defined in RFC 954 providing online look-up of individuals, network organizations, key host machines, and other information of interest to users of the Internet. The usefulness of this service has led to the development of other distributed directory information servers and information retrieval tools and it is anticipated more will be created.²⁰

RFC 1834 expressly required the provision of the name of individuals and their organizations, as well as specific contact details for the administrative and technical contacts. More importantly, RFC 1834, like its predecessor RFC 954, did not contain any limits on the use of or accessibility to Whois data.

Moreover, from the infancy of commercial use of the Internet in 1995, domain name registrants were on notice that their contact information would be made available to all Internet users via the Whois database. Thus, public access to the Whois database

¹⁸ RFC 954, available at <http://www.faqs.org/rfcs/rfc954.html> (emphasis added).

¹⁹ See footnote 2 of Task Force 1’s 2004 preliminary report, at <http://gnso.icann.org/issues/whois-privacy/Whois-tf1-preliminary.html>.

²⁰ RFC 1834, available at <http://www.faqs.org/rfcs/rfc1834.html>.

for any purpose has always been an integral aspect of both commercial and individual use of the Internet and the World Wide Web.

4. **RFC 2167**

As the Internet continued to grow and the World Wide Web enabled more and more commercial use, RFC 2167 was released in 1997. This document set forth in great detail the technical parameters of a Whois system called “RWhois,” though it also included some very enlightening statements on the development of the Whois database to that point, as follows:

Early in the development of the ARPANET, the SRI-NIC established a centralized Whois database that provided host and network information about the systems connected to the network *and the electronic mail (email) addresses of the users on those systems* [RFC 954]. The ARPANET experiment evolved into a global network, the Internet, with countless people and hundreds of thousands of end systems. The sheer size and effort needed to maintain a centralized database necessitates an alternate, decentralized approach to storing and retrieving this information.

The original Whois function was to be a central directory of resources and people on ARPANET. However, it could not adequately meet the needs of the expanded Internet. RWhois extends and enhances the Whois concept in a hierarchical and scaleable fashion. In accordance with this, RWhois focuses primarily on the distribution of “network objects,” or the data representing Internet resources or people, and uses the inherently hierarchical nature of these network objects (domain names, Internet Protocol (IP) networks, email addresses) to more accurately discover the requested information.²¹

Thus, RFC 2167 specifically noted that the “original function” of the Whois database was simply to be a directory of resources and people on the Internet. Furthermore, like the RFCs before it, RFC 2167 does not limit the purpose of the Whois database or discuss any limitations on the use of Whois data.

5. **Early Network Solutions, Inc. Policy**

In addition to the RFCs, the working party is invited to consider that the earliest domain name dispute resolution policies refer to the use of administrative contact details (which are part of the Whois database) in resolving intellectual property-related

²¹ RFC 2167, available at <http://www.faqs.org/rfcs/rfc2167.html> (emphasis added).

disputes. The November 1995 policy of Network Solutions, Inc. required the applicant to affirm upon registration of a domain name that:

The use or registration of the domain name by applicant, to the best of applicant's knowledge, does not interfere with or infringe the right of any third party in any jurisdiction with respect to trademark, service mark, trade name, company name or any other intellectual property right.²²

Furthermore, in the event of an intellectual property-related dispute, the policy required that:

[n]otices shall be sent to the Domain Administrative Contact listed in the InterNIC Registration Services' database [Whois] or such other address as either party may specify in writing.²³

The above policy is also noteworthy because NSI was at the time the sole registrar of generic top-level domain names (e.g., .com, .net, and .org). All gTLD registrants were explicitly notified upon their application for a domain name that the information in the Whois database would be used for resolving intellectual property-related domain name disputes. By 1999 when ICANN expanded the pool of registrars, domain names registered through NSI numbered in the millions. Therefore, publication of Whois data for the purpose of intellectual property protection was widely known.

6. ICANN Registrar Accreditation Agreement

Building on the RFCs and NSI policy identified above, ICANN's Registrar Accreditation Agreement (RAA), as revised through 2001,²⁴ provides that Internet registrars must make certain information regarding domain name registrants publicly available via the Whois database. Like all the other Whois protocols and requirements that had gone before it, the RAA does not contain any limitations on the use of Whois data (other than limitations placed on bulk access for marketing purposes that is not relevant to use of Whois data for intellectual property enforcement).

In sum, it is clear that the original purpose of the Whois database – from its inception, through the commercialization of the Internet, and continuing today – has always been to provide the public with ready access to the identity and contact information for domain name registrants, without restriction on the use of the contact information. That purpose has never changed, and registrants have always been on

²² NSI Domain Name Dispute Policy Statement, Paragraph 1(c), Revision 01, Effective November 23, 1995, at <http://www.lectlaw.com/files/inp13.htm>.

²³ *Id.* at paragraph 9.

²⁴ See <http://www.icann.org/registrars/ra-agreement-17may01.htm>.

notice of the purpose, regardless of when they registered their domains. To argue that use of Whois data to enforce intellectual property rights is somehow contrary to the “original purpose” of the Whois database, or that the purpose of the database is limited to technical issues only, is inconsistent with the historical record as well as with the historical experience and expectation of Internet users and domain name registrants.