



## **WHOIS and Data Privacy Overview of current practices**

*CENTR Secretariat*

*June 2006*

### **Executive Summary**

- One of a registry's key functions is to release information held on its register, as opposed to most bodies, for whom information release is a side-issue. This release of information has traditionally been via the WHOIS protocol, which was first outlined in 1984.
- Since 1984, public attitudes to data protection and privacy have moved on greatly, as has the law. Many registries are subject to data protection legislation, much of which is not written with the WHOIS system specifically in mind. Registrants are increasingly aware of privacy issues.
- Equally, there are many groups (of whom police are just one) for whom the information released by the registry is important, and who have a legitimate need to see some registry data (whether via the WHOIS or another process).
- The internet community has discussed the balance between data release and data secrecy for some time, often involving public consultations.
- This document seeks to summarise the arguments from both sides, highlight some interesting approaches, cover some generally accepted principles and form a basis on which registries can consult with their local internet community (which includes local privacy/data protection authorities).
- Ultimately, there is a trade-off between privacy and the need to publish some information, and that balance is one that each registry/registrar must make based on their circumstances, community views and local law.
- This paper does not recommend one system over another, or provide in-depth analysis of the law, although a schedule does provide advice about the nature and opinions of the Article 29 group (the committee of privacy bodies for the EU) for the benefit of the large number of CENTR members within the EEA.

The *Whois and Data Privacy overview of current practices* is considered to be a living document and will be regularly reviewed.

## Table of Contents

Executive Summary .....	1
Table of Contents .....	2
1. Introduction .....	3
1.1 What is WHOIS? .....	3
1.2 Who uses WHOIS and why? .....	4
1.2.1 General overview .....	4
While a few of these users could have their need served by special access to relevant data (law enforcement, for example) the majority are dependent on the data being publicly available. ....	6
2. Policies on WHOIS services .....	7
2.1 What information is available from WHOIS services? .....	7
2.1.1 gTLD Policies .....	7
2.1.2 ccTLD Policies .....	7
2.1.3 The information actually available .....	8
2.2 The impact of privacy legislation .....	8
2.3 Data Accuracy .....	9
2.3.1 The level of accuracy .....	9
2.3.2 Why accuracy matters .....	9
2.3.3 gTLD Requirements on accuracy .....	10
2.3.4 ccTLD WHOIS accuracy .....	11
3. Running a WHOIS – Questions to consider and Privacy issues .....	12
Appendix A: EC Data Protection Law .....	19
1 EC Legislation .....	19
2. Article 29 Working Party .....	19
3. The Data Protection Principles .....	20

## 1. Introduction

The WHOIS was outlined in an RFC published in 1984, at a time when most users of the internet were Americans, military, academics, or a mix of the three. As the domain name industry developed, large amounts of information about the registrants of domain names came into the hands of the registries (for ccTLDs) or registrars (for gTLDs).

At around the same time, particularly in Europe, public attitudes to the processing of person information (by all industries) developed, and data protection laws were put into place. As more people started using the Internet, more people started abusing it, and there was increased interest by various groups (such as the law enforcement and Intellectual Property communities) in obtaining data on domain names.

The WHOIS has therefore evolved, both technically in what *can* be done with it, and politically in terms of what *is* done with it.

### 1.1 What is WHOIS?

The concept of WHOIS was originally set out in informal documents like RFC and 812 and 954<sup>1</sup> and relating to the NICNAME/WHOIS server providing netwide directory service to [ARPANET|internet] users. These RFCs were later replaced by RFC 3912 which focused on protocol specifications. In its most basic form, WHOIS accesses databases containing information about the domain name, registrant and related information and displays this information as the result of a query.

However, virtually everything else about the WHOIS is subject to a great deal of variation amongst providers, as shown below.

There is variation in what database is used to provide the service:

- some systems use a separate database, and
- some provide a limited look at the main register database.

There is variation in what information is shown:

- some systems show virtually all information about the registration (e.g. *.com*),
- some show far less
- some show different amounts depending on the nature and preferences of the registrant of the domain (e.g. *.pl* and *.uk*)<sup>2</sup>,
- some show you bare details but will show more if you ask (e.g. *.fr*<sup>3</sup> and *.no*<sup>4</sup>) and
- some do not offer a WHOIS at all

There is variation in how users are permitted to search the database provided:

- some systems allow some degree of “wildcard” searches
- some require exact domain names only
- some require exact names in the WHOIS, but allow wider searches via other information release methods (e.g. *.uk*); and
- some allow ‘layered’ WHOIS services (e.g. *.name*)

---

<sup>1</sup> See <http://www.faqs.org/rfcs/rfc812.html> and <http://www.faqs.org/rfcs/rfc954.html>

<sup>2</sup> In the case of *.uk*, consumers (i.e. individuals who did not register the domain name as part of any business trade or profession, will not have their address shown on the WHOIS if they request that it be with-held).

In the case of *.pl* no data that identifies a private person is published unless direct consent of the person is given."

<sup>3</sup> For *.fr* clicking on the required information reveals it, but it is not shown by default.

<sup>4</sup> For *.no* clicking on the required information performs a new search based on the ID number given.

There is variation in how searches can be performed;

- some allow searches to be made on third party websites that then make their own WHOIS query;
- some systems allow queries via third party sites, but handle this through a variant or development of the WHOIS system (e.g. the so-called “WHOIS2” system used by *.uk*);
- some systems only allow searches from the registry’s own website, and/or prohibit connections to a WHOIS database.

There is variation in who actually provides the database:

- in some systems (including most ccTLDs), it is provided by the registry; and
- in many systems (including most gTLDs), it is provided by the registrars.

There is variation in the protection given the WHOIS data:

- in some systems (primarily the ICANN systems) the bulk data is sold, subject to some terms of use (although we have no examples of those terms ever being enforced);
- in most systems it is released subject to compliance with some terms of use;
- in some systems users via the website must type in a code that is designed to be non-machine readable (eg: *.se*, *.be*)<sup>5</sup>;
- many limit the amount of queries that can be made in a specified time;
- in some systems the body responsible claims intellectual property rights in the underlying data and takes legal action against infringements<sup>6</sup>; and
- the mechanisms for looking at volumes and patterns of queries (e.g. to stop attempts to copy the database) vary considerably.

The modern WHOIS is very diverse, but is provided in a very different way than it originally was when its main use was to allow network administrators to identify who was responsible for a domain name in order to solve connectivity problems and maintain the stability of the Internet<sup>7</sup>. While that use has not died out, many other users have come to rely on the WHOIS.

Not all of these other users are welcome – as one party, critical of the then-current ICANN regime noted, it can also be used as a weapon for corrupt governments prosecuting dissidents, spammers, aggressive intellectual property lawyers, and police agents without legal authority<sup>8</sup>.

## 1.2 Who uses WHOIS and why?

### 1.2.1 General overview

The basic WHOIS service is currently used by a wide range of people and organisations. As pointed out by the Organisation for Economic Cooperation and Development (OECD), “*WHOIS data is a critical source of information that assists in*

---

<sup>5</sup> Although there are ways around this, and potential problems with respect to equal treatment for the visually impaired.

<sup>6</sup> For example, Nominet UK, the *.uk* registry, has sued parties in Australia and the UK for misuse of WHOIS data, and obtained an Australian Federal Court judgement confirming that its WHOIS database is a copyright work.

<sup>7</sup> See for example <http://www.icann.org/committees/security/whois-recommendation-01dec02.pdf>

<sup>8</sup> See comment of Public Internet registry, operator of *.Org* in <http://www.dns0.org/dns0/dnsocomments/comments-whois/Arc03/pdf00000.pdf>

*accurately identifying the registrants of domain names. In many instances it is the only information that is available to identify the operators of commercial web sites.”<sup>9</sup>.*

Groups who currently use WHOIS data include:

- **Network Operators:** To identify appropriate contacts regarding network problems associated with the domain. In the traditional sense, this involves discussing technical DNS errors, routing, and other fundamental operations; or for more contemporary reasons such as identifying the source of spam and network attacks.
- **Anti Spam Bodies:** There are a range of groups dedicated to combating spam, from all sectors – network operators, government, regulators, registries and pressure groups<sup>10</sup>. Since spam is a major vector for viruses, phishing attacks and other anti-social behaviour these groups also work against these threats. The OECD<sup>11</sup> notes that *“Spammers often look for smaller ISPs ... especially where issues such as poorly maintained Whois records ... mean that complaints get directed to the abuse staff of a much larger ISP... So, the spammer find that they have a lead time of several days at the small ISP during which their website or spam sending server remains online.”<sup>12</sup>*. These groups use WHOIS to spot false data and suspect domains for the purposes of blocklists.
- **Registries, Registrars and Resellers:** To determine the availability of a domain name, confirm that the data held by the registrar is the same as that held by the registry, and to determine renewal status or expiry dates of domains. In many cases, this can also be done via non-WHOIS methods.
- **Security Certificates:** Certification Authorities (i.e. the companies that issue SSL certificates, a keystone of e-commerce) use the WHOIS in order to identify the registrants of domain names as one check made during the security process;
- **Business users:** Domain names have become essential to businesses and their marketing strategies – uses include:
  - checking whether a name is available to register;
  - secondary market (aka ‘dropcatching’) – monitoring valuable domain names to see the moment when they expire and then re-registering them for resale or for a customer who needs it;
  - confirming that the registration has been made to them;
  - confirming what domain names competitors have registered;
- **Intellectual Property interests:**<sup>13</sup> As it stores personal data on the registrant, WHOIS can be used to identify a domain name holder using the Internet to infringe on an individual or company’s intellectual property rights. These types of registrants are unlikely to comply with laws requiring them to give their address on their website.
- **Registries protecting their own WHOIS:** For example, Nominet UK made extensive use of .com WHOIS records when successfully tracing and suing those who had misused its .uk WHOIS in 2003<sup>14</sup>.
- **Consumers:** Domain names are the first identifier of an e-commerce site. WHOIS data can potentially be used by consumers to make sure the company

<sup>9</sup> In <http://www.oecd.org/dataoecd/16/8/2082033.pdf>

<sup>10</sup> See, for example, the membership of the London Action Plan ([www.londonactionplan.com](http://www.londonactionplan.com))

<sup>11</sup> Organisation for Economic Co-operation and Development – [www.oecd.org](http://www.oecd.org)

<sup>12</sup> p.21 in “Spam Issues in Developing Countries” DSTI/CP/ICCP/SPAM(2005)6/FINAL

<sup>13</sup> See, from the Intellectual Property Constituency of ICANN:

<http://www.icann.org/presentations/mutimear-whois-workshop-24jun03.pdf>

<sup>14</sup> <http://www.nominet.org.uk/disputes/courtcases/ukinternetreg/>

behind the site is legitimate. In less than ten years, the Internet and more precisely the World Wide Web have become to play a crucial role in commerce: according to a study, ecommerce should reach a value of \$6.8 trillion at the end of this year<sup>15</sup>. To quote the OECD, *“While the most obvious location for an online business to provide contact details is on the Web site itself, domain name registration information can serve as a useful complement. Conversely, businesses that provide false contact information can undermine the online experience of a consumer that decides to conduct a WHOIS search about the business”*<sup>16</sup>. In addition, local (and European) laws often require traders to provide information about themselves and their business<sup>17</sup> and particularly where they have failed to do so the WHOIS represents an alternative source for that information.

- **Registrants:** registrant can use WHOIS to determine whether a Domain name is available or not. Additionally, WHOIS can inform the existing registrant on the identity of another registrant of a similar domain. Registrants also use the WHOIS as a method for checking the data held on them by the registrar/registry.
- **Law enforcement personnel:**<sup>18</sup> When a Web site is the instrument of a fraud or other unlawful activity, law enforcement personnel can use WHOIS database to try to find more information about the fraudulent party. The WHOIS is of particular use as it allows them to obtain information quickly from multiple jurisdictions (many websites with a ccTLD domain may run on servers with a gTLD domain, instantly creating jurisdictional problems for investigating bodies).

**While a few of these users could have their need served by special access to relevant data (law enforcement, for example) the majority are dependent on the data being publicly available.**

<sup>15</sup> See <http://glreach.com/eng/ed/art/2004.ecommerce.php3>

<sup>16</sup> [http://www.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/98f97d6ef9579165c1256d39004ceb73/\\$FILE/JT00145317.PDF](http://www.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/98f97d6ef9579165c1256d39004ceb73/$FILE/JT00145317.PDF)

<sup>17</sup> EU E-commerce directive:

[http://europa.eu.int/ISPO/ecommerce/legal/documents/2000\\_31ec/2000\\_31ec\\_en.pdf](http://europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000_31ec_en.pdf), EU distance selling directive: <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31997L0007:EN:HTML>

<sup>18</sup> See presentation made on WHOIS by Maneesha Mithal from United States Federal Trade Commission at <http://www.icann.org/presentations/mithal-whois-workshop-24jun03.pps>

## 2. Policies on WHOIS services

### 2.1 What information is available from WHOIS services?

#### 2.1.1 gTLD Policies

The Internet Corporation for Assigned Names and Numbers (ICANN)<sup>19</sup> is responsible for policy coordination of the generic subset of Top Level Domains and has thus inserted special WHOIS provisions into its contractual agreements<sup>20</sup> with registrars<sup>21</sup> offering domain names registration in gTLDs. In the agreement, ICANN requires the public disclosure on the Internet of the domain names registrants' contact information (such as email address), technical contact information, administrative contact information and other information<sup>22</sup>. ICANN policy also insists that registrars must ask the registrant to maintain accurate and up-to-date<sup>23</sup> contact data.

The registrars are required to make the contact data publicly available through a WHOIS service<sup>24</sup>. In the event that a registrar fails to comply with its obligations in this respect, ICANN can terminate the accreditation of the registrar<sup>25</sup>. To date, ICANN has not undertaken any enforcement action to ensure compliance with the registrar Accreditation Agreement and as a result a plethora of WHOIS service levels has emerged as each registrar is able to interpret their Accreditation Agreement in a manner that best serves their business model.

Currently, gTLD registries use either the "thick" or "thin" approach for data storage<sup>26</sup>. In a thick approach, the registry itself holds all the relevant WHOIS data, whilst the thin model sees most data stored within the various registrars. The thick approach appears to be the most popular amongst newer gTLDs<sup>27</sup>.

Concerned about data protection issues, the *.name* registry has implemented a trial of a layered WHOIS approach<sup>28</sup>.

One aspect of the ICANN model of particular interest is that the Registrar Accreditation agreement requires registrars to sell their entire WHOIS database for a maximum of US\$ 10,000. Such a sale is subject to terms and conditions [see clause 3.3.6 <http://www.icann.org/registrars/ra-agreement-17may01.htm>] but we are not aware of any report of these terms ever being enforced, so it is unclear what abuses have (or have not) occurred.

#### 2.1.2 ccTLD Policies

The two-letter country code Top Level Domains registries (ccTLDs)<sup>29</sup> are accountable to the local communities they serve and must adhere to the laws that govern the registry. Generally, this includes providing registration information service (generally via WHOIS) and maintaining the associated databases<sup>30</sup>, in order to provide a utility that contributes to a stable operating environment.

<sup>19</sup> [www.icann.org](http://www.icann.org)

<sup>20</sup> <http://www.icann.org/registrars/ra-agreement-17may01.htm>

<sup>21</sup> <http://www.icann.org/registrars/accredited-list.html> for a list of current ICANN registrars having signed the agreement.

<sup>22</sup> See paragraph 4.2.1 below.

<sup>23</sup> <http://www.icann.org/registrars/wdrp.htm>

<sup>24</sup> See <http://www.icann.org/registrars/ra-agreement-17may01.htm#3> section 3.3.1

<sup>25</sup> <http://www.icann.org/registrars/ra-agreement-17may01.htm#5> section 5.3

<sup>26</sup> See presentation on <http://www.icann.org/presentations/bucharest-whois-ajm-28jun02.pdf>

<sup>27</sup> .info, .biz, .name, .museum, .coop, .aero and .pro

<sup>28</sup> <https://whoisbeta.gnr.com/> - note that the registry involved is based in the UK, and has an entirely different approach to Nominet, the *.uk* registry.

<sup>29</sup> See <http://www.iana.org/cctld/cctld-whois.htm> for a full list

<sup>30</sup> See Table 8 of the OECD paper at <http://www.oecd.org/dataoecd/46/38/2505946.pdf>



As the ccTLDs conform to the needs of their local communities there is a large diversity both in registration models and data models. This includes the amount of data held by the registry and the role of registrars in the input and maintenance of data. Some ccTLDs have no registrars at all.

As opposed to gTLDs, relations between ccTLDs and their accredited registrars are generally left to bilateral agreements between the two parties, with the ccTLD manager responsible for ensuring compliance with such agreement.

In addition, it is usually the registry (as opposed to the registrar) that provides the WHOIS service itself.

Each ccTLD must therefore establish and enforce a “privacy policy” in accordance with applicable laws. Because ccTLDs have a much more tightly defined local internet community, their privacy policy can be set after consultation with their local community, including local data protection authorities, if any.

As outlined above, WHOIS services across ccTLDs vary considerably.

### **2.1.3 The information actually available**

The ICANN accreditation agreement<sup>31</sup> lists the information that must be part of a WHOIS output on a domain name registered in a gTLD:

- The name of the authoritative name server(s) for the registered name.
- The identity of registrar (which may be provided through registrar’s web site).
- The date of initial registration.
- The current expiration date of the registration.
- The name and postal address of the registered name holder.
- The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the registered name.
- The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the registered name.

The data shown by a WHOIS is comparatively variable<sup>32</sup> - a 2003 summary by the OECD is instructive in setting out what data is returned<sup>33</sup>, and CENTR members can see a January 2005 CENTR survey on the topic<sup>34</sup>. As noted before various ccTLDs offer specific opt-outs or ‘data hiding’ mechanisms for individuals<sup>35</sup>, consumers<sup>36</sup> or other similar groups deemed needing protection or which do have protection under national laws.

## **2.2 The impact of privacy legislation**

Privacy law around the World is increasing, and CENTR has members in many jurisdictions so this paper cannot set out details for all areas. Appendix A gives an overview of the arrangements in the areas affected by European Community law (i.e. the 28 Member States of the EEA plus those countries amending their laws in advance of joining the EU).

---

<sup>31</sup> op.cit

<sup>32</sup> See paragraph 1.1 above

<sup>33</sup> See footnote 49

<sup>34</sup> <http://www.centri.org/surveys/whois200501/results> - CENTR login required

<sup>35</sup> See the .fr example for specific personal data policies reserved to individuals:

[http://www.afnic.fr/obtenir/chartes/nommage-fr\\_en#32](http://www.afnic.fr/obtenir/chartes/nommage-fr_en#32)

<sup>36</sup> See the .uk consumer opt-out explained at <http://nominet.org.uk/other/whois/optout/>

## 2.3 Data Accuracy

### 2.3.1 The level of accuracy

As explained above, uses of the WHOIS have changed considerably since the beginning of the Internet<sup>37</sup>, and these different users have different requirements from it. In most cases, they share a requirement that the WHOIS data must be accurate to be useful.

It is hard to quantify the level of 'inaccuracy' in the WHOIS database, and harder still to determine what proportion of that is deliberate (i.e. in any large database there will clearly be typing errors, lazy data entry, bona fide errors and information that is just 'out of date'). In addition, there will also be information which is deliberately incorrect – either because of a genuine desire for privacy or because the user is dishonestly hiding their identity to slow down or prevent investigators (either anti-spam<sup>38</sup> or criminal<sup>39</sup>). In another context, the UK's government register of driver and car identities, the DVLA was assessed in 2004 to be somewhere in the region of 55% accurate<sup>40</sup>.

In this context, in the gTLD system, there are now companies that register domain names in their own name in order to hide data on behalf of registrants. Anti-spam organisations have expressed their frustration at this tactic to the authors of this report.

It is also hard to quantify whether knowing that information will not appear in the WHOIS is likely to make a registrant give better information to the registry.

In terms of EC Data Protection law, Data Protection Principle 4 (see Directive 95/46) notes that "Personal Data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or purposes."

### 2.3.2 Why accuracy matters

The OECD is a particularly vociferous advocate of WHOIS accuracy, noting<sup>41</sup> *"accurate and available Whois data can help build consumer trust in the online marketplace..."* and *"... business that provide false contact information can undermine the online experience of a consumer that decides to conduct a Whois search about the business....Where the results of a Whois search produce obviously false information a consumer may be discouraged from doing business with the company in question, and more generally from engaging in e-commerce at all."*

In the same document, on the topic of law enforcement the OECD notes: *"...the problem of false domain name registration information has become an impediment to effectively identifying law violators. Whois is often a first step in investigating an online consumer problem. When its contact data are accurate and available, Whois can help law enforcers quickly identify actors responsible for the problem. Unless the company or individual can be quickly and efficiently located, however, pursuit of a consumer protection enforcement action may not be worthwhile."*

Finally, in a separate paper in 2005<sup>42</sup> the OECD notes; *"Another reason is that the anonymity of the Internet makes it much easier for a spammer to cover his tracks, set up a new domain with a different fake address and send out an entirely new spam....Therefore spammers are best tracked down when investigators have fresh*

---

<sup>37</sup> See paragraph 1.3

<sup>38</sup> See the OECD Quote at 1.2 above

<sup>39</sup> See p.5 of the OECD document

<sup>40</sup> <http://hardware.silicon.com/servers/0,39024647,39125553,00.htm>

<sup>41</sup> In DSTI/CP(2003)1/FINAL "Consumer Policy Considerations on the Importance of Accurate and Available WHOIS Data"

<sup>42</sup> In SDTI/CP/ICCP/SPAM(2005)6/FINAL "Spam Issues in Developing Countries".

*spam available, and can immediately reach out to ISPs and other organisations around the world, without undue delays ...”*

The WHOIS Taskforce of the ICANN DNSO<sup>43</sup> undertook a survey in 2002<sup>44</sup> outlining that 44% of the respondents had been harmed or inconvenienced by inaccurate, incomplete, or out of date WHOIS data. The study reported that the two most impacted groups were ISPs – of which 58% reported they had been harmed or inconvenienced – and Business users, as pointed out by the OECD<sup>45</sup>. But law-enforcement personnel also have issues with inaccurate WHOIS data: the US Federal Trade Commission<sup>46</sup> had (as at 2003) brought over 250 law enforcement actions involving Internet fraud, in part thanks to WHOIS data used either to identify where a perpetrator is located, or to determine the registrar who in turn was able to hand over useful data<sup>47</sup>.

However, inaccurate data is not entirely worthless. Anti-spam organisations have told the authors that even inaccurate Whois data is of use to them, because spammers tend to reuse inaccurate data – since spam-filters only need to identify suspect domains, not who is behind them, even inaccurate data has a use. Apparently, the lack of any WHOIS data (either because of opt-out or otherwise) is the big problem. Spammers will register domain names as disposable assets, so that in the day or two it takes for a court order to be obtained, or a privacy protection to be bypassed, they have moved on.

While the objective of total accuracy is undisputed, this must be measured against costs as these are ultimately borne by the registrants.

### **2.3.3 gTLD Requirements on accuracy**

ICANN's current accreditation procedure for gTLD registrars is covered in the registrar Accreditation Agreement (RAA)<sup>48</sup> which:

- Requires domain name registrants to give the registrar accurate and reliable contact details and to promptly correct and update them during the term of the registration.
- Makes wilful breaches of this obligation a basis for cancellation of the registration.
- Requires registrars to take reasonable steps to investigate claims of inaccurate WHOIS data when they are brought to their attention by any person; and
- Requires registrars to take reasonable steps to correct any inaccuracy in registrant contact data of which the registrar learns.

Necessary provisions are there in the agreement to put an obligation on the registrars to make sure the WHOIS data is accurate. However, a contractual obligation is of little use without ways to enforce it. That is why, ICANN issued a “Register Advisory Concerning WHOIS Data Accuracy”<sup>49</sup> to remind registrars of their current obligations under the RAA. ICANN followed up its advisory with an announcement on 3 September 2002 of several steps<sup>50</sup> to improve WHOIS data accuracy<sup>51</sup>.

<sup>43</sup> Archived on <http://does-not-exist.net/whois/>

<sup>44</sup> <http://www.dnso.org/dnso/notes/whoisTF/20020625.TFwhois-report.htm>

<sup>45</sup> See “Business Identification Guidance: Exposure Draft”, [www.oecd.org/pdf/M00028000/M00028484.pdf](http://www.oecd.org/pdf/M00028000/M00028484.pdf)

<sup>46</sup> <http://www.ftc.gov/opa/2002/05/whois.htm> and <http://www.icann.org/presentations/mithal-whois-workshop-24jun03.pdf>

<sup>47</sup> For a comprehensive case study see

<http://cyber.law.harvard.edu/people/edelman/invalid-WHOIS>

<sup>48</sup> See [www.icann.org/registrars/ra-agreement-17may01.htm](http://www.icann.org/registrars/ra-agreement-17may01.htm), op.cit.

<sup>49</sup> [www.icann.org/announcements/advisory-10may02.htm](http://www.icann.org/announcements/advisory-10may02.htm).

<sup>50</sup> See [www.icann.org/announcements/announcement-03sep02.htm](http://www.icann.org/announcements/announcement-03sep02.htm).

<sup>51</sup> One can now submit a WHOIS data problem report directly to ICANN using a specific web form, see [http://reports.internic.net/cgi/rpt\\_whois/rpt.cgi](http://reports.internic.net/cgi/rpt_whois/rpt.cgi)

### 2.3.4 ccTLD WHOIS accuracy

Because of the independent nature of ccTLDs, the “one size fits all” ICANN approach cannot and in any event should not apply. While some of the measures mentioned in ICANN's RAA also are used by ccTLDs, the requirements of local laws (including regional law, as for the European ccTLDs<sup>52</sup> and the needs of the local Internet community take precedence. Thus ccTLDs have diverse approaches - even when it comes to improving the accuracy of the WHOIS data.

Although there is diversity, some methods used by ccTLDs to improve the accuracy of the WHOIS data can be identified:

- The data holder (that is either the registry or the registrar) ensures through the registrant agreement that the registrant is required to give correct registration data, and to keep the data updated.
- The data holder ensures that they have some means of enforcing the registrant agreement (suspending or removing the domain etc.)
- Different syntactic checks are made automatically or manually to ensure that the data is of a correct format (ccTLDs that only accept registrants with a local address are able to have stricter format requirements than ccTLDs where the registrant can have an address in any country he/she chooses).
- By making the information concerning a domain publicly available the data holder makes it possible for other parties to find and subsequently report errors in the data.
- Registrants are given logins to update their details and encouraged to do so.

In addition, some ccTLDs give the registrant the right to protect himself, either by refusing to publish its address details or by allowing registrants to give any address which is sufficient to allow postal contact, even if this not their actual address<sup>53</sup> and this concept is mirrored in a recent ICANN WHOIS taskforce report<sup>54</sup>.

---

<sup>52</sup> See ECD 95/46/EC op. cit.

<sup>53</sup> For example, Nominet (.uk) have this policy.

<sup>54</sup> Preliminary Task Force Report on purpose of Whois and of Whois contacts”, v1.4, 19 January 2006, available from [www.icann.org](http://www.icann.org)

### 3. Running a WHOIS – Questions to consider and Privacy issues

When setting up a WHOIS service, or considering what changes might be made to an existing one, there are a number of considerations to take into account. The table below tries to pose some of the more standard questions. Where matters touch on privacy or data protection concerns, we have answered them by reference to EC law, but clearly the answers will be slightly different in other jurisdictions.

Question	Notes
How can the WHOIS be accessed? i.e. will there be a website based WHOIS? Will connections to port 43 of a WHOIS server be accepted?	Allowing port 43 access is useful for many purposes, but it means that automated queries are easier to perform. This may not be a bad thing – many legitimate users (such as registrars and their resellers) may wish to use port 43 access. Port 43 access prevents use of some types of security checks (like distorted images) but it may allow better disabled access and allows other sorts of checks (IP addresses etc.)
What volume limits are imposed?	If unlimited volumes are permitted, then it is much easier for people to copy the entire WHOIS database. EC data protection law imposes a requirement that data is kept securely <sup>55</sup> , and this might be compromised in this case.
How are volume limits enforced?	Limits are commonly imposed on the IP address of the querying party, often combined with some kind of increasing time window for queries from the same party. Such measures will hinder abuse to a certain extent but can be circumvented by determined parties with large bot nets.  Given the large volumes of queries a whois service responds to, automatic controls may be the only effective option in the future.

<sup>55</sup> Directive 95/46/EC, Articles 16 and 17.

Will other services, be offered rather than just 'plain vanilla' WHOIS?	One point of view is that the WHOIS is a single tool being used to do a wide range of things, and that the best way to control WHOIS is to offer a range of services, e.g. a low volume WHOIS to those who actually need it, a higher volume service which does not reveal any personal data to those making bulk queries, and more flexible searches to those who need them for specific, legitimate purposes.
Will 'layered' access to the WHOIS be offered?	In this system, anonymous users from the Internet of the WHOIS are only allowed to see very basic data, and those who wish to see more detailed registry data (whether via WHOIS or any other protocol) have to enter a password. However, defining services levels for the many different uses of whois (see 1.2 above) and administering passwords that allow access to the appropriate data can be complex and resource-consuming. The difference between this approach and the 'other services' approach immediately above is that in the 'layered' approach certain data fields are restricted to certain types of user, whereas in the 'other services' model the control is based on volume of use. The Article 29 working group <sup>56</sup> said in their 2003 opinion that: <i>"In the light of the proportionality principle, it is necessary to look for less intrusive methods that would still serve the purpose of the Whois directories without having all data directly available on-line to everybody."</i>

<sup>56</sup> See Appendix

<p>What terms of use are there? Are there different terms of use for those with different types of access to registry data?</p>	<p>Almost all registries seek to impose terms and conditions on users of the WHOIS. These terms generally include some or all of the following:</p> <ul style="list-style-type: none"> <li>• Restrictions on the later use of the data (e.g. no spamming or marketing)</li> <li>• Restrictions on the query levels</li> <li>• Intellectual Property notices in the Register</li> <li>• Limitation clauses, excluding liability for giving incorrect WHOIS data (note that these relate to the reliance on the data by third parties, not to any liability under data protection law to the registrant)</li> <li>• Guidance on the purpose of the WHOIS</li> <li>• Powers for the registry to change or withdraw WHOIS at any time – suspension of the WHOIS can be necessary if there is a particular security threat.</li> </ul>
<p>What rights does the registry have in the database?</p>	<p>The rights that a registry has in its data are important for two reasons. Firstly, they will form a part of the contract or terms the registry has with those that use its data, but secondly they also form a critical part of the armoury of the registry if third parties misuse the registry data and the registry seeks to prevent this occurring. Generally, WHOIS databases are likely to be protected by confidentiality, copyright or database rights. Certainly substantial judgements have been obtained in Australia on the basis of copyright infringement<sup>57</sup> and a damages order has been obtained<sup>58</sup> on the basis of EU Database Rights<sup>59</sup>, although the precedent value of this decision is not so good.</p> <p>Ironically, EC data protection law does not give you a cause of action as the data controller whose data was misused, so that if personal data from the WHOIS is misused, that in itself is not a basis for suing the party involved. Note that if the use they are putting it to relate to unsolicited communications, there may some assistance from Directive 2002/58.</p>

<sup>57</sup> <http://www.nominet.org.uk/disputes/courtcases/ukinternetreg/>

<sup>58</sup> <http://www.nominet.org.uk/disputes/courtcases/macrae/>

<sup>59</sup> Directive 96/9/EC

<p>If the registrant is a corporate body, will details about contact persons at that body be included ?</p>	<p>Corporate bodies are not protected in the same way as individuals. The Article 29 working group is clear that there should be a chance to opt-out: <i>"It should be noted however that, also in the cases of companies or organisations registering domain names, individuals can not be forced to have their name published as contact-point, as a consequence of the right to object. "</i></p> <p>An exception could be where the registrant contact information relates to a person legally responsible for the company, who might be required by local law to have their contact details published as a contact point for the company.</p>
<p>Will opt-outs be provided for particular categories of users? If so, which ones and why? How will you deal with (the inevitable) abuse of this option?</p>	<p>In the gTLD space, the registry for .org has suggested that as its users are non-commercial, they should be entitled to withhold more data<sup>60</sup> and the .name registry is trialling a service which contains less WHOIS data because their users are primarily individuals.</p> <p>As highlighted above there are ccTLDs that provide special protections and opt-out to consumers and individuals, and data protection law may grant rights in this respect.</p> <p>In order for these opt-outs to be effective on the scales involved in domain name registries (i.e. where hundreds of thousands of opt-outs may be claimed) these processes have to be scalable, presumably by setting a 'flag' field in the register database.</p> <p>Data protection advice would be that this option has to be clearly explained to the user and they have to have it explained to them how they can use this opt-out.</p> <p>The experience of those registries which implement opt-outs is that they will be abused, both by those ignorant of the rules, and by the dishonest (e.g. many spammers will select the opt-out by default, as it means that the data protection authorities investigating them are slower to react). If allowing opt-outs, consideration will have to be given to how they can be policed, and removed if not warranted – again this has to be scalable, because dealing with these complaints consumes staff time and those costs are passed back to the users.</p> <p>In as far as requests to withhold personal data from being published are concerned, registrars or registries should be clear about the associated procedures and about the criteria to be used, in order to ensure consistency in approach and decision making.</p>

<sup>60</sup> <http://www.pir.org/News/PressRelease.aspx?id=37>



<p>What address/contact details are acceptable? Is it enough to give an address via which they can be contacted, even if this is not their own (e.g. their registrar or a commercially provided secrecy company)?</p>	<p>As has been highlighted above, some registries show full address details, contact names, email and fax. For those not controlled by ICANN, there is a choice which details should be included.</p> <p>Data protection law would suggest that only the minimum amount necessary for the legitimate purposes for which the data was obtained should be shown.</p> <p>The other question is whether registrants must show their actual address or whether a 'service' address is sufficient. Several registries already accept this.</p> <p>It has been suggested that registrants be allowed to show one address for the WHOIS and a separate one to the registrar. However, this removes any pressure on the registrant to show 'real' data, and means that law enforcement and others will routinely ask for the underlying data, so it does not solve the problem.</p>
<p>What search mechanisms do you allow?</p>	<p>Most existing WHOIS services only allow access to the registry database using one kind of search term – the domain name. The WHOIS protocol, however, doesn't mandate any specific approach. Depending on the implementation, a WHOIS-provider could allow searches on any kind of data element, or allow for other sophisticated queries (e.g. searching by telephone number, email address, and so forth).</p> <p>One common addition to a simple domain approach is to allow lookups by "NIC handles" – unique codes assigned to administrative contacts, for example.</p>
<p>What uses of the WHOIS data provided are permitted? Is bulk access allowed?</p>	<p>There are three constraints:</p> <p>Firstly, data protection law is very clear that data may only be used for the purpose(s) for which it was obtained, so the registrant must have been told in advance that the data was to be used for the WHOIS and been able to find out what data the WHOIS returns. Bulk access is a different purpose to the usual one-domain-at-a-time format of the WHOIS, and is therefore likely to be prohibited.</p> <p>Secondly, certain activities related to unsolicited communications are prohibited by Directive 2002/58, so sales of data for this purpose are prohibited (and, in any event most registries would not co-operate in any activity liable to increase spam).</p> <p>Thirdly, the data that registrants are prepared to give you, and the accuracy of that data may be affected by the uses to which you will put it (even if you are not covered by data protection law).</p>

What structure output is produced? How will IRIS be dealt with?	WHOIS and IRIS both provide the capability to structure output in a machine readable format. In fact, the nature of the protocols makes it essentially impossible to avoid this. IRIS makes machine extraction even easier by using a standardised format designed to be parsed called XML. Registries considering the impact of machine readability should however know that any information that should ultimately not be machine-readable cannot be published via any of these information services. In any kind of text format, be it WHOIS, IRIS, web pages or other, processing output into a storable form is a trivial project for a computer programmer. However, if it is not machine readable, it will not be accessible to the visually impaired, which may put the registry in breach of obligations to the disabled.
Are activities which can assist WHOIS abuse prohibited?	The zone file provides a key of all the domain names currently active on the register, and accordingly if zone file transfers are permitted they can be used to assist in WHOIS abuse.  Registries will be aware of the objections raised in the IETF process to the draft DNSSEC standards, on the basis that they might assist WHOIS abuse.
What will the privacy policy be? How will it be made available?	This policy sets out the rights and duties of the registry and other parties and explains what data will be collected, why and what for. The policy will also cover the registrant's rights under data protection legislation, and the mechanisms that the registrant can use to see the data held about them, correct it etc.  In terms of availability, how easy will it be to find on the website and how easy is it to read?
How is the registrant informed about the privacy legislation and their respective rights <sup>61</sup> ? How is consent obtained from the Registrant? How specific does the consent have to be?	Registrants must make an explicit consent to the terms and conditions regarding privacy issues when entering a contract with the registry. Ensuring that the registrant is aware of the registry's terms and conditions can be challenging, as most registries will not deal with the registrants directly. Registries may therefore have to require registrars to bring their contracts to the registrant's attention in a way which allows the registry to highlight the important clauses (data protection, etc.) to them. Ideally, there should then be a positive acceptance of those terms.  You also have to tell the registrant that its personal data is collected and how it is used <sup>62</sup> .

<sup>61</sup> Directive 95/46/EC, Article 10

<sup>62</sup> Directive 95/46/EC, Article 10

How do registrants access their own data? How do they find out about this?	<p>Registrants have rights<sup>63</sup> to access the data held about them<sup>64</sup> and correct it (if needed)</p> <p>In an automated registration environment this may be of the form of a password-controlled webpage or interface that allows unassisted modification of the data. Another method could be to require the registrant to go to a registrar, who then has direct access to editing the data on behalf of the registrant.</p> <p>No matter which mechanism is chosen, it is important to in some way be able to track how a change was made, and identify who was responsible for making the change, in case there is a conflict concerning the change at a later time.</p> <p>Even for countries where this data protection point does not apply, it is likely to benefit the registry if registrants can update their data.</p>
Are you sure that you do not use the data for anything outside the policy?	Data protection law does not permit use of the data for any purposes other than those for which it was collected, so in any use of registrant data (WHOIS included) thought must be given to why that data was collected.
Do you want to transfer data to third parties (i.e. other than the WHOIS?)	The WHOIS effectively includes transfer to third parties. Even if you have consent for that, that consent may not cover transfer to other third parties for other similar purposes.
Have you fully understood that data protection law, and its provisions on overseas transfers, applies?	Directive 95/46/EC would prohibit the transfer of personal data to non-European Union nations that do not meet the European “adequacy” standard for privacy protection. Article 25 of the Directive gives the Commission the power to determine whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into <sup>65</sup> . The effect of such a decision is that personal data can flow from the twenty-five EU Member States and four EFTA member countries <sup>66</sup> to that third country without any further safeguard being necessary. Very few other bodies meet the standards (in particular, US non-Government bodies (e.g. ICANN) do not). The Commission has produced some standard contract wording which can be used in other data transfers (e.g. the US generally).

<sup>63</sup> Directive 95/46/EC, Article 12.

<sup>64</sup> Directive 95/46/EC, Article 11(c)

<sup>65</sup> See for an analysis: <http://www.dataprivacy.ie/6aii-3.htm#25>

<sup>66</sup> Norway, Liechtenstein and Iceland

How do you maintain the personal data?	Data should be accurate and kept up to date <sup>67</sup> – where there is a registrar involved, there will have to be some process to update them about changes. Registrants should also be told about the need for them to keep their held data accurate. In some registry models, registrants could be given the ability to update their own data via a password protected web site.
How do you tell the registrant who you are?	You should clearly <sup>68</sup> display who you are (i.e. legal name and status) and your contact details (e.g. name, e-mail, address, etc.), providing a straightforward method for the registrant to contact you regarding their data. In most cases, the registry will have to register with their data protection authority, as they will be a 'data controller';
How long do you keep the data?	The registry must not keep personal data for any longer than necessary <sup>69</sup> . If the data is to be held longer for statistical or other reasons, safeguards must be put in place (i.e. 'anonymisation' and compilation of the data). The registry should inform the registrant of their data retention policies.
What access do you provide to law enforcement? What about foreign law enforcement?	When deciding whether it is necessary to publish WHOIS data, do not forget that data needed by law enforcement bodies does not necessarily have to be publicly available – it may be sufficient if they have general access. Also note, if implementing tiered access, that data protection law does not assume that law enforcement should have unfettered access to data above and beyond that granted by the public.
What data do you actually need?	Only collect data if it is necessary for carrying out the registry operation. Data cannot be collected for other reasons and the law requires that it is not "excessive" <sup>70</sup> . The reasons for data collection will likely not be limited to those purely required for publishing data in a WHOIS service, but would also include data needed for other aspects of the registry/registrar business (for example, billing, legal matters etc.).The website or registration form would need to be explicit in advising the registrant that its personal data is collected and how it will be used.

<sup>67</sup> Data Protection Principle 5

<sup>68</sup> Directive 95/46/EC, Article 10.

<sup>69</sup> Data Protection Principle 6

<sup>70</sup> Data Protection Principle 4

## Appendix A: EC Data Protection Law

### 1 EC Legislation

The most important piece of EU legislation with regards to WHOIS is Directive 95/46/EC<sup>71</sup> 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”. The Directive defines data privacy within the context of data relating to identified persons and seeks to ensure that the same basic rules are obeyed throughout the Single Market and within all member-states.

There are considerable variations in the national approaches, but as far as WHOIS implementation is concerned, the eight basic data protection principles<sup>72</sup> tend to apply. The effect of these principles (which clearly do apply) is given in more detail in the guidance section. Other Directives of potential importance are:

- EC Regulation 45/2001 on protection of individuals with regard to the processing of personal data by the community institutions and bodies and on the free movement of such data – which is of narrow scope; and
- Directive 2002/58/EC on privacy and electronic communications. The applicability of this directive is a much more contentious matter. In brief, Article 12 of this directive (prefaced by recital 38) deals with the rights of ‘subscribers’ in relation to directories, and gives rights to withhold some or all data. The controversy arises because of the word “directory”, which is not a description of the WHOIS. The WHOIS (in normal implementation) has a different purpose to a directory, and a different method of searching. The classic directories are telephone directories, and it is clear that the purposes to which they are put are radically different to the purposes for which the WHOIS is used.

### 2. Article 29 Working Party

All supervisory data protection authorities in the European Union and the European Economic Area take part in this Working Party to discuss matters of common interest, and agree common positions on the application of the Directive<sup>73</sup>. Of particular interest to our topic is Opinion 2/2003 on the application of the data protection principles to the WHOIS directories<sup>74</sup>, which states:

- [The registry] must determine in “very clear terms” what is the purpose of WHOIS and which purposes can be considered as legitimate and compatible with the original purpose
- Clear limitations must be imposed concerning the collection and processing of personal data “meaning that data should be relevant and not excessive for the specific purpose”
  - Publication of certain information about a company or organisation (such as their identification and their physical address) is often required by law in the framework of commercial or professional activities they perform.
  - On the other hand, where an individual registers a domain name, the situation is different and while it is clear that the identity and contact information should be known to the registrant’s service provider, there is no legal ground justifying the mandatory publication of their personal data. In

<sup>71</sup> [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett)

<sup>72</sup> e.g. see

<http://www.informationcommissioner.gov.uk/eventual.aspx?id=6785&expmovie=1#About>

<sup>73</sup> See: [http://europa.eu.int/comm/justice\\_home/fsj/privacy/workinggroup/wpdocs/2005\\_en.htm](http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm)

<sup>74</sup> [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2003/wp76\\_en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp76_en.pdf)

other words, such data can be collected by the registry but not necessarily be published as the result of a WHOIS query.

- The Opinion of the WP advises the registry to look for “less intrusive methods in light of the proportionality principle” that would still serve the purpose of the WHOIS directories without making all the personal data publicly available to anyone browsing the Web.
- The fact that personal data are publicly available does not mean that the requirements of the data protection directive do not apply to that data
- Concern about proposals regarding more searchable WHOIS facilities
- Support for proposals concerning accuracy of the data and limitation for bulk access for direct marketing issues.

In summary, “The Working group encourages ICANN and the WHOIS community to look at privacy enhancing ways to run the WHOIS directories in a way that serves its original purpose whilst protecting the rights of individuals.”<sup>75</sup>

### **3. The Data Protection Principles**

There are eight data protection principles enshrined in Directive 95/46 which underpin the approach of EC privacy bodies and which should guide registries. These can be summarised as:

1. Personal data shall be obtained and processed fairly and lawfully;
2. Personal data shall be held only for one or more specified and lawful purposes;
3. Personal data held for any purpose shall not be used or disclosed in any manner incompatible with that purpose or those purposes;
4. Personal data held for any purpose shall be adequate, relevant and not excessive in relation to that purpose or those purposes;
5. Personal data shall be accurate and, where necessary, kept up to date.
6. Personal data held for any purpose shall not be kept for longer than is necessary for that purpose;
7. An individual is entitled, at reasonable intervals and without undue delay or expense to be informed whether a data user holds information about him and to access that data, and to have that data corrected or erased;
8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

All handling of personal data must comply with these principles.

---

<sup>75</sup> During the ICANN meeting in Montreal (June 2003) Mrs. Diana Alonso Blas of Directorate General Internal Market of the European Commission, has highlighted the need to respect the existing data protection framework in Europe, so that WHOIS directories can be run in a way that serves the original purpose whilst protecting the rights of individuals. Mrs. Diana Alonso Blas presentation at ICANN meeting in Montreal is available at: <http://www.icann.org/presentations/alonso-blas-whoisworkshop-24jun03.pps>