Complex nr. 2/2009

Dana Irina Cojocarasu

LEGAL ISSUES REGARDING WHOIS DATABASES

The Norwegian Research Centre for Computers and Law
Department of Private Law
Postboks 6706 St Olavs plass
0130 Oslo

Henvendelser om denne bok kan gjøres til:

Senter for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
Tlf. 22 85 01 01
www. jus.uio.no/iri/

ISBN 978-82-7226-121-3
ISSN 0806-1912

Utgitt i samarbeid med Unipub AS
Trykk: e-dit AiT AS
Omslagsdesign Kitty Ensby

Preface

This report is one element of a long-term research programme on Internet governance being conducted by the Norwegian Research Centre for Computers and Law (NRCCL), University of Oslo. The programme is primarily funded by UNINETT Norid AS ("Norid") – the organization that manages the .no top-level domain. Thanks go to Norid for their generous financial support in the research and writing of this report. Special thanks go to Annebeth Lange and Hilde Thunem of Norid for their valuable suggestions and information as well as for their patience during the one and a half years spent compiling the report.

It bears emphasizing, nonetheless, that the views expressed herein do not necessarily reflect the views of Norid or its staff. Moreover, any mistakes are my responsibility, not that of Norid or others.

My gratitude goes also to Professor Jon Bing who once again gave me a vote of confidence in entrusting me with this project. Jon, the project could not have been produced without your never-ending energy and inspiring involvement. It is hoped that the content of the report will convince you that your trust was not misplaced!

The report could not have been completed in time and with the requisite quality without the close guidance of Associate Professor Lee A. Bygrave. Thank you, Lee, for your support and encouragement, for your attention to detail and for your discovery of an optimal strategy for getting the chapters of the report submitted, *as often as possible*, by the agreed deadline. Thank you too for the great effort you made in editing and otherwise "fine-tuning" this report.

Last but definitely not least, thank you, Christian, for your warmth and for brewing many litres of tea whenever I had an approaching deadline to meet!

Unless otherwise stated, all references (including website addresses) in the report are current as of 1st March 2009.

Dana Irina Cojocarasu
NRCCL

Table of Contents

Introduction 7

1 The Domain Name System: Normative Framework 13
1.1 gTLD policy development process 14
1.2 ccTLD policy development process 21
1.2.1 ICANN's role in policy development at ccTLD level 21
1.2.2 Policy-making role of national authorities 23

2 WHOIS Service 27
2.1 Features of WHOIS databases 27
2.1.1 Evolution of WHOIS service and databases 27
2.1.2 Input, search and output variations 38
2.2 Functions of WHOIS databases 45
2.2.1 Technical operability 48
2.2.2 Transparency 49
2.2.3 Accountability 51
2.2.4 Accuracy: a prerequisite for effectiveness of WHOIS databases 52

3 Legal Protection of WHOIS Databases 71
3.1 Ownership of copyright / sui generis right 75
3.1.1 Individual queries 79
3.1.2 Multiple queries 81
3.2 Limitations in the exercise of the database rights 81
3.2.1 Statutory limitations of WHOIS database makers' rights 82
3.2.2 Contractual limitations of WHOIS database makers' rights 86

4 Protection of Personal Data in WHOIS Databases 93
4.1 Application of data protection legislation to WHOIS service 94
4.1.1 Nature of data processed 94
4.1.2 Operations involved in provision of WHOIS service 96
4.1.3 Identity and roles of WHOIS service providers 97
4.2 Legal basis for processing personal data when providing WHOIS service 104
4.2.1 The consent of the data subject 106
4.2.2 Other legal grounds 115
4.3 The features of a legally compliant processing of personal data via WHOIS service – a best practice framework 116
4.3.1 Personal Data Management 117
4.3.2 Data subject management 132
4.3.3 Confidentiality and security of processing 134

5 Effective Law Enforcement through a Privacy-Friendly WHOIS Database 141
6 Conclusions 151
7 Select Bibliography 155

Introduction

The domain name system (DNS) assists users of the Internet in navigating the network by translating Internet Protocol (IP) addresses, which are numeric, into conventional denominations more easily recognised and remembered by the users. A prerequisite for such a translation, however, is that the alphabetical identifiers are unique. In response to the need for maintaining the integrity of names already registered (thus ensuring that every name in the DNS is unique), the "WHOIS" service was created. In broad terms, WHOIS is a service which allows interested parties to address queries to databases (WHOIS databases) containing information about registered domain names, their registrants and the servers they use. Originally, the provision of the service was voluntary for both the registries responsible for managing and allocating domain names and the domain name registrants. The latter had the option of making their contact information available to their peers by registering themselves in a WHOIS database. Subsequently, the functionality of the service was expanded by enabling inquiries about the status and availability of a domain name. Nowadays, in response to a query to a WHOIS database, one is given access to information about one or more registered domain names, the identity of the registrants and the associated servers. The purpose of storing and displaying this information is to enable communication with a party responsible for the domain name in question or with a party that can reliably hand on data to a party that is able to resolve issues concerning the configuration of the records linked to the domain name.[1]

Taking as a point of departure the purpose of the WHOIS service, the goal of this report and the research behind it is to examine the roles and responsibilities of the actors involved in the creation and management of the WHOIS databases and to investigate the policies involved in the collection, processing and transfer of the information contained in WHOIS databases in selected top-level domains (TLDs).[2]

This report builds on a basic distinction between the policy model applicable to generic TLDs (gTLDs) and that of country-code TLDs (ccTLDs). This distinction has implications, in the given context, for which of the (public) authorities have the competence to decide upon and to implement the policies for the provision of WHOIS service and for the functioning of WHOIS databases.

---

1 See generally GNSO Whois Task Force, *Final task force report on the purpose of WHOIS and of WHOIS contacts* (15.03.2006), <http://gnso.icann.org/issues/whois-privacy/tf-report-15mar06.htm#0.1>.

2 The concept of "top-level domain" and related concepts in the DNS are explained in Chapter 1.

The distinction also has an impact on the enforcement mechanisms that can be implemented in the event that agreed rules are infringed.

In very general terms, the Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit corporation with functions relating to, among other areas, Internet Protocol (IP) space allocation, and gTLD name system management. ICANN has a de facto monopoly on establishing the policies that regulate the gTLDs. These policies are created subsequent to a decision-making process resulting in a consensus between the views of the supporting organisations and constituencies and those of the international Internet community (as expressed during the public review of the policy documents). In addition, ICANN has entered into direct agreements with the registries designated to operate each gTLD and has set up an accreditation procedure for registrars (i.e., those who carry out the actual registration of domain names) wishing to provide registration services to interested parties.

On the other hand, the management of country-code top-level domains is now assigned by ICANN to countries or regions and is primarily governed by rules established at national level.[3] According to the principles and guidelines for the delegation and administration of ccTLDs suggested in 2005 by the Governmental Advisory Committee for ICANN, "ccTLD policy should be set locally, unless it can be shown that the issue has global impact and needs to be resolved in an international framework".[4]

A registry for a ccTLD is typically appointed by its national government and the local Internet community to operate the namespace concerned. The registry and ICANN usually exchange formal letters of collaboration (or enter into a separate agreement), expressing a mutual commitment to cooperate in order to ensure the stable and secure operation of the Internet's unique identifier systems for the benefit of the Internet users. Subsequently, the national registry will set up policies for the accreditation of registrars and will stipulate conditions regulating how registrars may provide registration services under the national domain.

The normative framework for the provision of WHOIS service at the gTLD level is currently under review. Significant changes in the rules for the collection, use and transfer of the information stored in the WHOIS databases have been proposed in order to better meet the requirements of privacy and data protection legislation, to improve the accuracy of the information stored in the

3 See further, e.g., Lee A. Bygrave & Jon Bing (eds.), *Internet Governance: Infrastructure and Institutions* (Oxford: Oxford University Press, 2009), chapter 5 (sections 5.1.4, 5.4, 5.5).

4 Governmental Advisory Committee, "Principles and guidelines for the delegation and administration of country code top level domains" (Mar del Plata, 05.04.2005), <http://gac.icann.org/web/home/ccTLD_Principles.rtf>.

WHOIS databases and, at the same time, to cater for the legitimate interests of various stakeholders. This process has come to a temporary halt at gTLD level due to the difficulties encountered in reaching a broad international consensus.[5] While not directly affected by the gTLD policy process, the managers of European ccTLDs, like all ccTLD managers, continually face the challenge of implementing a WHOIS service that duly takes into account the needs of all the stakeholders legitimately interested in access to the WHOIS databases, while also complying with the obligations assumed through bilateral agreements in accordance with the law.

It is in this international climate that the analysis in this report takes place. In order to convey a multi-faceted image of WHOIS service, research was focused primarily on three business models: one applicable to domains registered at a gTLD level (.com) and the other two applicable to selected domains registered at ccTLD level (.no and .eu). The latter two models, however, differ from one another (although the domains are situated at the same hierarchical level in the DNS). Registration under the .eu domain is open for all citizens and organisations in the European Union and, by contrast to .no (or any other national domain), .eu functions according to rules set up at a supranational (as opposed to national) level.

In addition to its academic significance – as one of the few extensive legal analyses of a key service in the Domain Name System – the present report may serve as a practical contribution to management of the .no domain by identifying the benefits and shortcomings of the current policy model for that domain (as compared to the policies for .com and .eu) and by suggesting an improved framework with additional legal safeguards for the stakeholders involved.

The WHOIS service cannot be regarded as a stand-alone service, since it is meant to function as a support for the current DNS. Thus, in order to put provision of the service in its proper legal context, relevant elements of domain name management are explored in Chapter 1. Special focus is devoted to the decision-making processes and actors in the DNS, including the relevant agreements reached and their enforcement mechanisms.

Following a presentation of some key stages in the evolution of the WHOIS service, Chapter 2 examines the features and functions of WHOIS databases. The discussion in Chapter 2 sets the premises for evaluating the effectiveness of the WHOIS regime in safeguarding the privacy interests of the domain name registrants. It is argued that by clearly defining the purpose(s) of the WHOIS databases, the registries and registrars would be able to ensure that legitimate goals are pursued through collecting only the minimum necessary amount of

5 *Whois Study Group Report to the GNSO Council* (22.05.2008), <http://gnso.icann.org/issues/whois/gnso-whois-study-group-report-to-council-22may08.pdf>.

personal data from registrants. Chapter 2 focuses, therefore, on the possible legitimisation – de jure or de facto – of publication on the Internet of the registered information about the domain name and its registrant. If WHOIS databases are to function effectively, the input data must be accurate throughout the period during which the domain is active. Analysis of the agreements entered into by the registries, registrars and the domain name registrants discloses several challenges in terms of ensuring a high level of accuracy of the data fed into WHOIS databases.

Under the compulsory agreements entered into by the registries and registrars at the gTLD level, the provision of WHOIS service is obligatory. Registries and registrars are required to set up and to provide access to WHOIS databases, free of charge via the web and port 43, and with remuneration via bulk-access agreements with third parties. In the case of national (.no) and regional (.eu) TLDs, the decision regarding the content of, and access to, WHOIS data is made at the local level and published through the relevant domain name policies. Taking into account that the WHOIS service involves access to WHOIS databases created and managed by the registry (in the ccTLDs) or the registrars (in the gTLDs), Chapter 3 identifies the scope of the registries'/registrars' respective intellectual property rights in WHOIS databases as well as the consequences this has on the functioning of WHOIS service.

Subsequently, Chapter 4, the most extensive part of the study, addresses the "Gordian knot" of the policy reform process at gTLD level – that is, the content of the WHOIS databases. More precisely, it investigates the rights and obligations of the registries and registrars in lawfully processing the personal data submitted upon registration of the domain name. The chapter identifies the main requirements of the European data protection laws and illustrates how they can be understood as guarantees that should remain paramount during the provision of WHOIS service. Best practice examples are extracted from the existing regimes at ccTLD level, as well as from the proposals that were submitted during the consensus-building process at gTLD level. In the light of the legal requirements and of the existing practice, an argument is made out for the implementation of a layered access to WHOIS databases responding to the legitimate needs of potentially interested parties (as identified in Chapter 2) by providing only such information as is necessary and sufficient for the attainment of the specific purpose of the query. This argument is based on a reconciliation between the privacy interests of the registrant and the informational needs of the requestor.

However, when the query is made in conjunction with law enforcement, societal interests may outweigh the personal interests of the registrant. As detailed in Chapter 5, access to information for legitimate law enforcement purposes should be facilitated, and well-defined routines should be in place

to enable access and exchange of information between international law enforcement agencies. In this manner, the apparent dichotomy between privacy and disclosure could be replaced by the acknowledgement of the idea that a privacy-friendly WHOIS policy may lead to increased accuracy in the database and facilitate, in turn, the legal pursuit of those who abuse the domain name system and misuse WHOIS data.

1 THE DOMAIN NAME SYSTEM: NORMATIVE FRAMEWORK

The domain name system (DNS) was conceived as a distributed mechanism to transpose domain names – that is, user-friendly, alphabetic names for Internet sites (e.g., www.uio.no) – into numeric Internet Protocol (IP) addresses (e.g., 203.160.185.48). Domain names are divided by "dots" and hierarchically structured from right to left. At the top of the hierarchy lie the top-level domains (TLDs). These are the last label on the right-hand side of the dot furthest to the right in the domain name. Next in the hierarchy is the second-level domain (SLD) which is represented by the label situated immediately to the left of the "dot" before the TLD. For example, in the designation "uio.no", the "uio" element represents the second level while ".no" denotes the TLD reserved for Norway.

The TLDs are divided into two classes: generic top-level domains (gTLDs) (e.g., .com, .org, .net, .biz, .info, .name) and country-code top-level domains (ccTLDs). While an exhaustive description of the domain name system exceeds the scope of this research project and report, the distinction between gTLDs and ccTLDs is essential because it entails differences in both the applicable policies and the decision-making procedures for domain name registration and management of registrant data. As a consequence, the policies for WHOIS databases differ for ccTLDs and gTLDs respectively. Moreover, as explained in the following sections, the competence of the rule makers for gTLDs differs from that of ccTLD managers.

This chapter provides insight into the policy framework for the Internet domains situated at the highest level of the DNS hierarchy. Understanding this framework is crucial. The starting point of any regulatory intervention, whether it is shaped as a self-regulatory process or as a legal statute, is the fulfilment of a policy objective. The policy objective is usually expressed in the form of guiding principles for the activity to be regulated. Once agreed upon, these principles serve as a basis for setting up rules and standards and, indirectly, for defining activities and circumstances under which a violation of the rules/standards can be deemed to have occurred. The final component of a standard regulatory process entails the integration of the regulatory act in an enforcement context (for example, by determining the bodies competent to decide whether a violation has taken place and which are authorised to impose appropriate sanctions).

In analysing the scope of the substantive rights and obligations pertaining to WHOIS databases and the information contained therein, extensive reference is made in the following to the provisions of several national and international policy documents representing the legal basis of such rights and obligations. Most often these policy instruments are the result of a self-regulatory intervention of the stakeholders themselves, rather than a governmental intervention. Examining their legitimacy, the scope of their applicability as well as possible conflicts among them is a major task of the research. Moreover, where statutory regulation applies, it is vital to identify the applicable law for a given domain.

1.1 gTLD policy development process

Responsibility for managing the DNS inheres primarily in the Internet Corporation for Assigned Names and Numbers (ICANN). This is a non-profit organisation headquartered in California but with an international membership. Under ICANN's aegis, the multitude of various stakeholders in the DNS can have a say in the administration of that system and other aspects of the Internet.

According to Article I section 1 of its Bylaws,[6] ICANN's mission is "to coordinate, at the overall level, the global Internet systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems". In addition to performing technical functions, ICANN coordinates the development of policies inasmuch as they relate to these functions. The legitimacy of ICANN as a policy maker is said to derive from the direct involvement of different categories of stakeholders represented within the organisation through both elected bodies and nominated representatives, as well as committees, councils and supporting organisations.

Formally, ICANN's top policy decision body is the Board of Directors. The Board consists of fifteen voting members (Directors) and six non-voting liaisons (Article VI section 1 of the Bylaws). The composition of the Board is intended to reflect cultural and geographic diversity as well as a solid understanding of the potential impact of ICANN decisions on the global Internet community (Article VI section 3).

The decisions of the Board are typically based on policy recommendations that are thrashed out and agreed upon by one or more of ICANN's Supporting

6 The ICANN Bylaws have been amended several times since 1998. The version used for this research project was effective as of 29.05.2008. It is available at: <http://www.icann.org/en/general/bylaws.htm>.

Organisations and Advisory Committees (described immediately below), in accordance with their respective mandate.

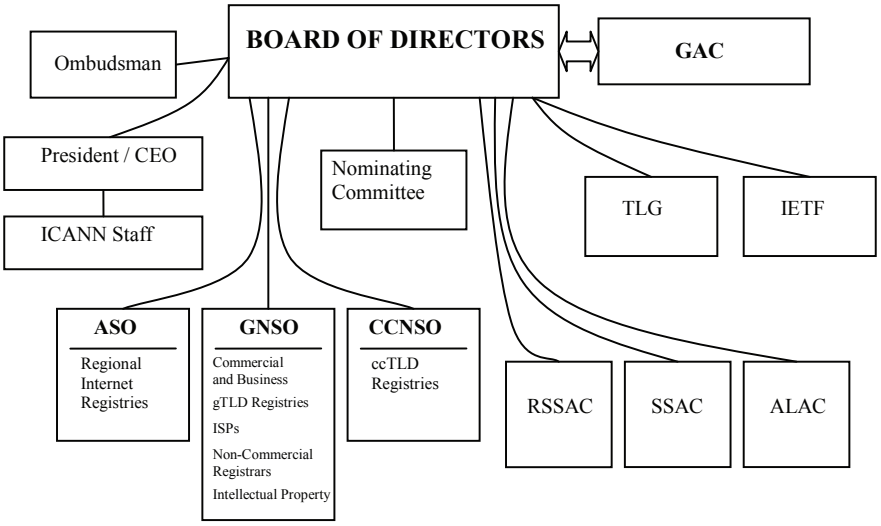


Figure 1. ICANN structure[7]

The Supporting Organisations are consultative and policy development bodies allowing multiple stakeholders in the global Internet community to contribute to policy making on matters that fall within ICANN's area of competence. The consensus reached on policy matters within one of the Supporting Organisations is duly considered in the final decision taken by the Board.

In the context of this study, the most important of the Supporting Organisations is the Generic Names Supporting Organisation (GNSO). This body is responsible for developing and recommending substantive policies applicable at gTLD level. Reference is made to the GNSO throughout this report since the organisation is leading the policy reform for the gTLD WHOIS databases. The GNSO has also been instrumental in the development of the Uniform Domain Name Dispute Resolution Policy,[8] the addition of new gTLDs and the protection of trademarks in the new TLDs. The GNSO comprises seven constituencies, representing the gTLD registries, registrars, Internet Service

7 Taken from Bygrave & Bing (eds.), *Internet Governance*, *op. cit.*, p. 107. There one finds also an explanation of the various acronyms and the organisations they represent.

8 For a brief description of this policy, see Bygrave & Bing (eds.), *Internet Governance*, *op. cit.*, section 5.2.2.

and Connectivity Providers, commercial and business users, non-commercial users and the interests of intellectual property rights holders.

The Country Code Names Supporting Organisation (ccNSO) develops and recommends global policies regarding ccTLDs, nurturing consensus across the ccNSO community and coordinating with other ICANN-supporting organisations. The technical administration as well as the policy making at ccTLD level have been delegated by ICANN to the national ccTLD managers (national registries). As a consequence, the policy competence of ccNSO is restricted (in accordance with Annex C of the Bylaws) to:

- developing best practice for ccTLD managers in order to ensure interoperability at a ccTLD level; and
- initiating generic policies delineating the division of competence between ICANN and the national decision-making authorities (governments and national registries).

The ccNSO is made up of those ccTLD managers (registries) that have agreed in writing to become members of it.

The third Supporting Organisation is the Address Supporting Organisation (ASO). This advises the Board on policy issues relating to the operation, assignment and management of Internet addresses.

In addition to the Supporting Organisations, several Advisory Committees have been created under the aegis of ICANN. These are the Governmental Advisory Committee (GAC), Security and Stability Advisory Committee (SSAC), Root Server System Advisory Committee (RSSAC) and At-Large Advisory Committee (ALAC). Although these committees have no legal authority to act for ICANN (Article XI section 1 of the Bylaws), their findings and recommendations are reported to the Board. The most influential committee (with respect to the Board) is GAC, which is made up of representatives of national governments, intergovernmental organisations (the International Telecommunications Union (ITU) and World Intellectual Property Organisation (WIPO)), the European Commission and other regional bodies. GAC provides advice particularly whenever there might be interaction between ICANN policies and existing national laws and international agreements or whenever public policy issues could be raised. For example, GAC has drafted the "Principles and guidelines for the delegation and administration of the ccTLDs",[9] broadly recognised as the framework for delineating the relative competence of ICANN from that of national governments and national registries. The Committee may propose issues for consideration to the ICANN Board either directly, by way of comment and prior advice, or indirectly, by recommending an action

9 Referenced *supra* note 4.

or a new policy development process, or by initiating the revision of existing policies. Although the views of GAC are not binding on the ICANN Board, the latter is obliged to find a mutually acceptable solution in the event that it wishes to act in a way that is inconsistent with GAC advice (Bylaws Article XI section 2(1)(j)).

Another significant committee (at least in respect of the issues taken up in this report) is the At-Large Advisory Committee (ALAC). This was founded to consider and provide advice on the activities of ICANN insofar as they relate to the interests of the individual Internet users. Obviously, ALAC may play a part in policy discourse on WHOIS issues, primarily as a voice for the concerns of individual Internet users in their capacity as WHOIS database registrants.

The substantive policies developed by ICANN for the gTLDs are the result of a self-regulatory process known as the GNSO's Policy Development Process (PDP). The process, described in Annex A of the Bylaws, aims at achieving legitimacy through ensuring that those entities most affected by it can assist in creating the rules they are supposed to apply.[10] A diagram of the GNSO's PDP is reproduced in Figure 2. Beyond the typical stages illustrated in the diagram, other intermediary procedures may be decided by the GNSO Council[11] when needed, such as, for example, the creation of a Working Group in order to improve and elaborate the recommendations in the Task Force Reports or additional public consultations.

The main features of the PDP are as follows:

1. It strives to ensure that the various stakeholders are represented in the decision-making process. The GNSO Constituencies, representing various groups of affected parties, have the opportunity to appoint representatives to both the GNSO Council and the GNSO Task Force. While the Council is competent to initiate the policy process, the Task Force gathers relevant information documenting the positions[12] of the Constituencies "as specifically and comprehensively as possible, thereby enabling the Council to have a meaningful and informed deliberation on the issue" (Bylaws Annex A paragraph 7(a)). In addition, the Task Force can solicit the input of external

10 See the core values of the ICANN decision-making process and actions as described in Article I section 2 of the Bylaws.

11 This is the case for the current discussions regarding the reform of WHOIS policies. See particularly "GNSO Consideration of Proposed Changes to WHOIS" (14.09.2007), <http://www.icann.org/en/announcements/announcement-2-14sep07.htm>.

12 See Bylaws Annex A paragraph 7(d)(1) for details regarding the compulsory contents of a Constituency Statement.

advisors, experts or members of the public.[13] Their views expressing assent or dissent will be included in the Task Force Reports. Moreover, two Public Comments sessions, each lasting 20 days, ensure that the relevant opinions of other interested parties not represented in ICANN are considered in the final decision of the ICANN Board.

2. It provides for well-informed rule making. First of all, reasoning must be given for all Constituency Statements (Bylaws Annex A paragraph 7(d)(1)). Moreover, again in accordance with the Bylaws, the level of consensus reached (supermajority vote, consensus, and dissenting opinions) must be documented; the same applies to the implementation issues identified. In addition, the outside experts or advisors involved must state in detail their qualifications and relevant experience as well as potential conflicts of interest that may influence their opinion. The Final Report of the GNSO Council (the "Board Report"), based on the conclusions of the Task Force report and the results of the Public Comments Sessions, informs the ICANN Board not only about the broad consensus reached but also, if applicable, all the dissenting opinions of the Council Members and their reasoning.
3. Being the result of mutual consultation and agreement, the policy transcends jurisdictional issues. The consensus policies resulting from the PDP apply to all the gTLDs, and are meant to be implemented by all ICANN-accredited registrars[14] (under the potential sanction of having their accreditation withdrawn) as well as the registries[15] designated by ICANN to manage gTLDs.
4. The PDP ensures flexibility in the adoption and modification procedures in the sense that the procedures for policy making may be amended or modified following a proposal from the GNSO Council, subject to the subsequent approval by the ICANN Board (Bylaws Article X section 3(4)). Moreover, as reflected by the PDP for WHOIS databases, if the GNSO Council considers that the Final Task Force Report leaves certain conceptual or implementation issues unanswered, it can decide to convene another

13 An independent report commissioned by ICANN to examine its accountability and transparency practices, has pointed out, however, that the corporation should make additional efforts to explain more clearly how input is used when making decisions, in order to ensure consistent engagement of the public. See One World Trust, *Independent Review of ICANN's Accountability and Transparency – Structures and Practices* (London, March 2007), <http://www.icann.org/en/transparency/owt-report-final-2007.pdf>.

14 See Section 4 of the Registrar Accreditation Agreement (17.05.2001), available at <http://www.icann.org/en/registrars/ra-agreement-17may01.htm>.

15 See Article III section 3(1)(b)(i) of the .com registry Agreement (01.03.2006) (available at <http://www.icann.org/en/tlds/agreements/com/>) and corresponding provisions in similar agreements for other gTLDs.

Working Group to further elaborate the conclusions reached by the Task Force, this prior to submitting a Final Proposal to the ICANN Board.

5. The Bylaws provide several guarantees for ensuring that the PDP is transparent from inception to implementation. Throughout the PDP, ICANN will maintain a status web page on its website, detailing the progress of each PDP issue and describing (see Bylaws Annex A paragraph 15):
   a. The initial suggestion for a policy;
   b. A list of all suggestions that do not result in the creation of an Issue Report;
   c. The timeline to be followed for each policy;
   d. All discussions among the Council members regarding the policy;
   e. All reports from task forces, the Staff Manager, the Council and the Board; and
   f. All public comments submitted.

The result of the PDP is a Consensus Policy, which is compulsory for both accredited registrars and gTLD registries, regardless of the national jurisdiction under which they otherwise function. ICANN remains thus the sole actor with policy-making competence in gTLDs whereas registries and registrars are only called upon to implement and comply with existing and future policies developed through a PDP, as well as with Temporary Specifications or Policies adopted by the ICANN Board.[16]

To date, two consensus policies have been adopted by the ICANN Board concerning WHOIS:

- The WHOIS data reminder policy (27.03.2003);
- The WHOIS marketing restriction policy (12.11.2004).

The Board has also adopted a policy for dealing with potential conflicts between WHOIS requirements and privacy laws (10.05.2006).[17] These policies are elaborated in Chapters 2 and 4.

As for the issues of collection, public display and transfer of WHOIS data, these have been the subjects of a consensus-building process for several years. However, a final decision on these issues has not yet been taken by the ICANN Board, so the rules in force for dealing with them still stem from ICANN's

16 Article III section 3(1)(a)(i) of the .com registry Agreement (01.03.2006).

17 As far as I understand, although the latter policy was endorsed by the ICANN Board through a formal procedure, this cannot be regarded as a fully-fledged Consensus Policy in the same way as the other two policies (marketing restriction and data reminder) because it does not impose any new obligations on any registries, registrars or third parties and it is intended only to guide ICANN's response to potential difficulties that its contracting parties could have in complying with ICANN contractual requirements.

practice and its binding agreements with the accredited registrars and the gTLD registries rather than from a consensus process as the one described above.

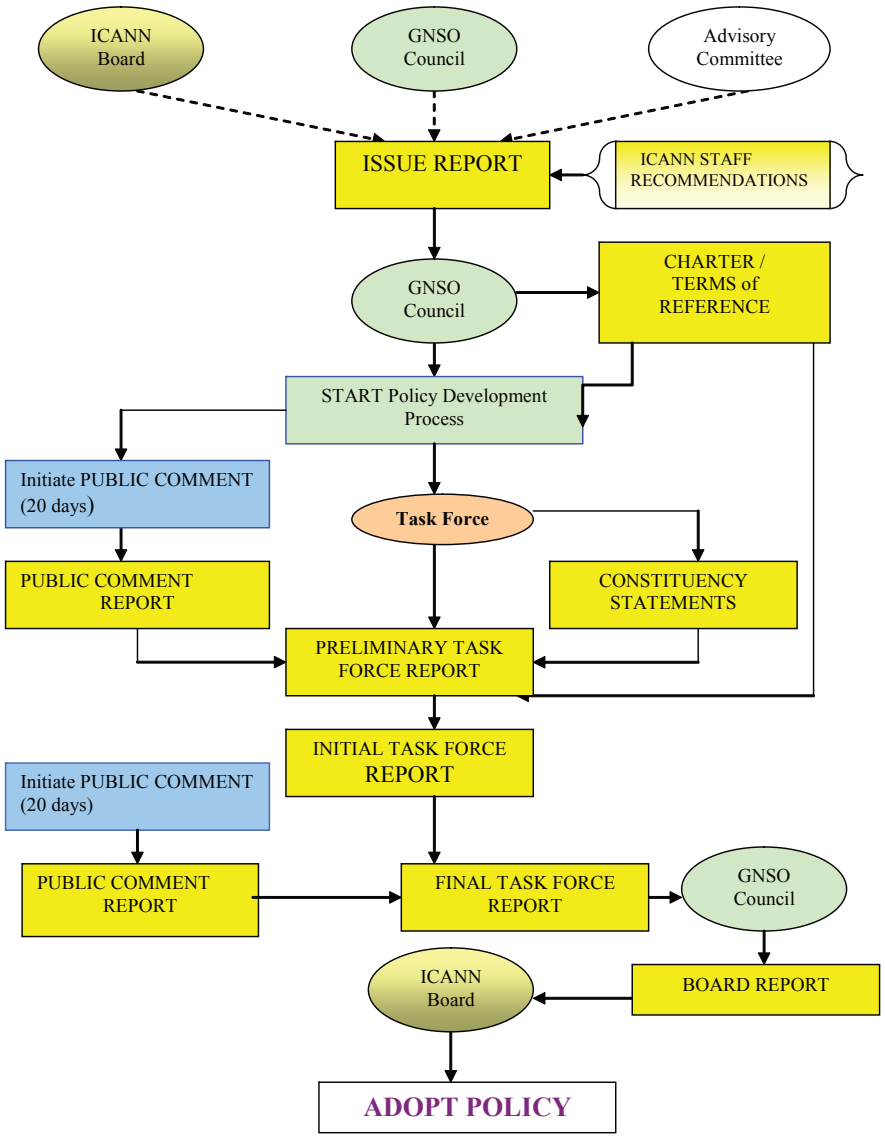


Figure 2. GNSO Policy Development Process

1.2 ccTLD policy development process

A country-code top level domain (ccTLD) is a domain used by and reserved for a country or a dependent territory. It is expressed in two-letter country codes mostly based on the ISO 3166-1 standard[18] (e.g., .no for Norway or.au for Australia). The country's top-level domain[19] is often viewed as the flagship of a country's Internet participation and as a strategic asset with symbolic, socio-economic and/or Internet stability and security implications.[20] Country-code TLDs were originally delegated in order to allow local Internet communities worldwide to develop their own locally responsive and accountable DNS services.[21]

1.2.1 ICANN's role in policy development at ccTLD level

As described in section 1.1.1 above, ICANN retains sole policy-making authority for the gTLDs. The question this section wishes to answer is to what extent policies developed by ICANN primarily for the gTLDs can be imposed upon the managers of the ccTLDs, in addition to or despite rules set up at a national level. This question becomes relevant especially given the current policy development process started by ICANN on the provision of WHOIS services and on the management of access to the personal data contained in WHOIS databases.

First and foremost, ccTLD issues are addressed under the aegis of ICANN within the ccNSO. This Supporting Organisation is opened to voluntary membership from ccTLD national managers.[22] In accordance with ICANN

18 According to this definition, .eu is technically not a ccTLD.

19 Historically, most ccTLDs were operated by academic organisations. In most cases, governments retain direct control over, or have instituted a formalised relationship with their national ccTLD operators. Most have established a subsidiary company of a government ministry or have entered into operational contracts with their national ccTLD registry through which they assert their ultimate authority. Only in a few countries have the governments insisted upon total control over TLD management, enacting specific legislation granting themselves final authority over their ccTLDs and setting out registration requirements (the case in Spain, Finland and Greece). In a similarly small number of countries (Germany, UK), there is no formal governmental role in their respective ccTLD at all. Their registries, in other words, act without direct statutory basis and independently of direct state control.

20 See OECD Working Party on Telecommunication and Information Services Policies, *Evolution in the management of Country-Code Top-Level Domain Names (ccTLDs)* (DSTI/ICCP/TISP(2006)6/FINAL; 17.11.2006), available at: <http://www.oecd.org/dataoecd/8/18/37730629.pdf>.

21 See particularly RFC 1591: Domain Name System Structure and Delegation (March 1994), <http://www.ietf.org/rfc/rfc1591.txt>.

22 NORID became a member of ccNSO on 06.12.2006.

Bylaws Article IX section 4(10), an ICANN policy shall apply to ccNSO members (by virtue of their membership) if certain cumulative conditions are met:

1. regarding the scope of the policy: it should address issues under the field of competence of ccNSO (a field which takes account of ccTLDs but which requires overall coordination from ICANN);[23]
2. regarding the adoption procedure:
   – the policy has been developed through a ccPolicy Development Process as described in Annex B of the Bylaws;
   – following the recommendation of the ccNSO, the policy has been adopted by the Board.

Over and above these conditions, ICANN polices shall not be imposed upon the ccNSO members when they conflict with the national law applicable to the ccTLD manager. The national law "shall, at all times, remain paramount" (Bylaws Article IX section 4(10)).

The above provisions in the Bylaws were introduced following a reform process initiated by the Governmental Advisory Committee (GAC). The process aimed at improving and better emphasising the division of responsibility between ICANN, national governments and the national registries regarding policy making for ccTLDs. The consensus reached within GAC on this point is expressed in its document "Principles and guidelines for the delegation and administration of country code top level domains".[24] The document represents the views of the national governments, distinct economies, multinational governmental and treaty organisations that are members of the GAC. The Principles are intended as a guide to the relationships between governments, their ccTLDs and ICANN; as such they are not meant to be binding.

The guiding principle in policy making at ccTLD level is that of subsidiarity – ccTLD policy should be set locally, by the local Internet Community, according to national law. Only exceptionally can a global approach be encouraged by ICANN, provided it can be shown that the issue has global impact and needs to be resolved in an international framework. This global approach is now pursued within the scope of ccNSO's activity.

The following figure depicts the relative division of policy-making authority among national governments, national registries and ICANN, as recommended by the 2005 GAC principles.

23 According to Bylaws Article IX section 6 and Annex C.

24 Referenced *supra* note 4.

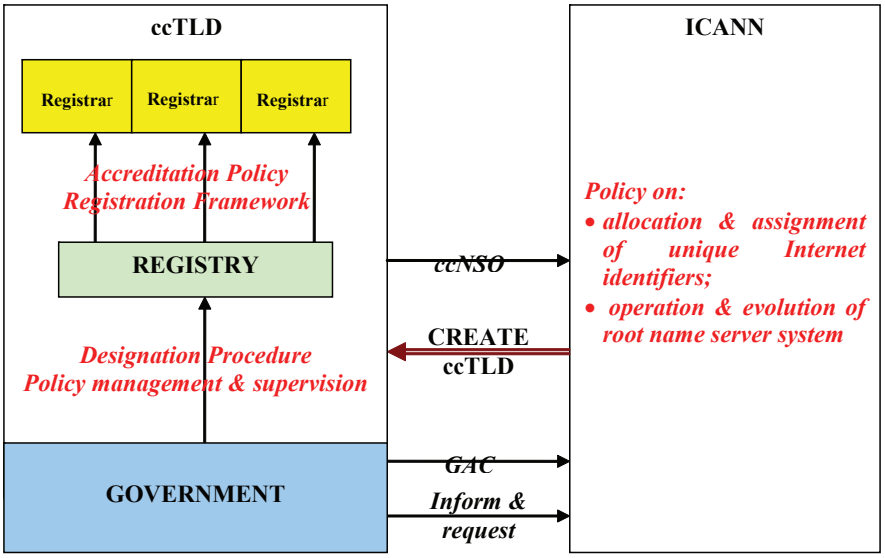


Figure 3. The division of policy-making competence at ccTLD level

1.2.2 Policy-making role of national authorities

In contrast to the situation for gTLDs, the policy-making competence regarding ccTLDs is shared between the relevant government or public authority and the registries. The national rule-making authority has the competence to set up the general policy rules applicable to the national domain in question. This high-level framework shall set up requirements for the domain name policy development process for each top-level domain, the minimum requirements that need to be met by a registry administering a top-level domain, and the consequences if those requirements are not met. In Norway this function is primarily performed by the Norwegian Ministry of Transport and Communications which sets the framework in a Regulation on domain names.[25] In the case of the .eu registry, the highest policy-making competence for defining the framework for domain name administration and the rules for the registration of domain names is assigned to the European Commission. In Commission Regulation

25 Regulation No. 990 of 01.08.2003 on domain names under Norwegian country code top-level domains (Forskrift om domenenavn under norske landkodetoppdomener). The statutory basis for the Regulation is the Electronic Communications Act (Act No. 83 of 04.07.2003) sections 7-1 and 10-1.

(EC) No. 874/2004 of 28.04.2004,[26] the Commission lays down public-policy rules concerning the implementation and functions of the .eu TLD and the principles governing registration under that domain.

As stated in the World Summit on Information Society (WSIS) Declaration of Principles of December 2003, the "policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues" (paragraph 49(a)). This statement is repeated in the WSIS Tunis Agenda for the Information Society of November 2005 paragraph 35.[27] Further, the WSIS Plan of Action of December 2003 invites Governments "to manage or supervise, as appropriate, their respective country code top-level domain name" (paragraph 13(c)(ii)). Working in collaboration with their local Internet community and considering the appropriate national laws and policies, governments are given a clear to mandate to decide on the rules for the designation of an appropriate manager for the national ccTLD.

The policy-making competence of the national government, absolute within the boundaries of its jurisdiction, is exercised in this field through the recognition of its right to make decisions concerning:

- requests to ICANN that its appropriate country code be represented as a ccTLD in the DNS;
- designation of the registry for the ccTLD concerned;
- the manner in which the core values of the domain name management should be transposed into policy principles to be followed in the accreditation of registrars and in the allocation of domain names.

1.2.2.1 Policy-making role of registries

Within the national framework thus set, the designated national registry will draw up the detailed policies concerning the accreditation of registrars as well as the registration of domains under the national domain name. Further, the ccTLD registry will provide a name service to the local Internet community in its jurisdiction, and according to a name policy as decided by the local community (including the government).

---

26 Set out in Official Journal of the European Communities (hereinafter "O.J.") L 162, 30.04.2004, pp. 40–50.

27 Cf. paragraph 63 of the Tunis Agenda: "Countries should not be involved in decisions regarding another country's country-code Top-Level Domain (ccTLD). Their legitimate interests, as expressed and defined by each country, in diverse ways, regarding decisions affecting their ccTLDs, need to be respected, upheld and addressed via a flexible and improved framework and mechanisms".

Take, for example, the role of EURid, which is the registry for the .eu domain. Under Article 4 of Regulation No. 733/2002 of 22.04.2002 on implementation of the .eu Top-Level Domain,[28] EURid is charged with the organisation, administration and management of the .eu TLD, including maintenance of the corresponding databases and the associated public query services, the accreditation of registrars, the registration of domain names applied for by accredited registrars, the operation of the TLD name servers and the dissemination of TLD zone files. In addition to this operative role, the registry shall organise, administer and manage the .eu TLD in the general interest and on the basis of principles of quality, efficiency, reliability and accessibility and it shall define and implement an extra-judicial settlement of conflicts policy. The registry shall also enter into accreditation agreements with registrars, defining the terms under which they have the right to register domain names under the ccTLD.

1.2.2.2 Scope of registrar's decision-making competence

A registry has a responsibility for shaping the registration regime so that the service it offers (registration of domains) abides by the domain name policy set by the regulatory authorities. This function includes defining the border between the tasks that should be centralised at registry level, and the tasks that should be handed over to registrars.

In the .no domain name policy, for instance, a registrar submits on behalf of an applicant an application to register a domain name under the domains that Norid manages in its role as registry. The registrar is obliged to comply with the regulations in effect at any time, as well as the guidelines and routines that Norid has provided on its Web pages. The registrar's decision-making competence is restricted to designing its own internal routines to best ensure compliance with the framework set by Norid while at the same time being economically efficient.

Similarly, each registrar accredited under the .eu domain shall be bound by contract with the registry to observe the terms of accreditation and in particular to comply with the public policy principles set out in the domain name policy. Registrars may also develop label, authentication and trustmark schemes. These schemes are regarded as a useful instrument for promoting consumer confidence in the reliability of information that is available under a domain name they registered, as well as a guarantee for compliance with applicable national and Community law.[29]

28 O.J. L 113, 30.04.2002, pp. 1–5.

29 Commission Regulation (EC) No. 874/2004, Article 5.

2 WHOIS SERVICE

This chapter presents firstly some key stages in the evolution of WHOIS service. It then discusses the features and the functions of WHOIS databases. The discussion in the chapter serves as a basis for understanding the efficiency and effectiveness of the policy rules governing the provision of the service, especially with regard to the balance struck among the conflicting legitimate interests of the stakeholders.

2.1 Features of WHOIS databases

2.1.1 Evolution of WHOIS service and databases

The idea of a net-wide directory containing information about the domain names already registered and about the identity of the registrant was first introduced in a Request for Comments (RFC) document issued by the Internet Engineering Task Force in 1982. The document, commonly known as RFC 812,[30] describes WHOIS in the following terms:

> *"[a] NCP/TCP transaction based query/response server, running on the SRI-NIC machine that provides netwide directory service to 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 [and requests that] each individual with a directory on an ARPANET host, who is capable of passing traffic across the ARPANET, be registered in the NIC Identification Data Base. To register, send full name, middle initial, U.S. mailing address (including mail stop and full explanation of abbreviations and acronyms), ZIP code, telephone (including Autovon and FTS, if available), and one network mailbox, via electronic mail to NIC@SRI-NIC."*

RFC812 was updated in October 1985 through RFC954,[31] which specified that the "NICNAME/WHOIS Server is accessible across the Internet from user programs running on local hosts" but stated at the same time that "this server,

30 RFC 812: NICNAME/WHOIS (March 1982), <http://www.faqs.org/rfcs/rfc812.html>.
31 RFC 954: NICNAME/WHOIS (October 1985), <http://www.faqs.org/rfcs/rfc954.html>.

together with the corresponding WHOIS Database can also deliver online look-up of individuals or their online mailboxes, network organizations, DDN nodes and associated hosts, and TAC telephone numbers".

The basis for what later became the controversial web-based and port 43 WHOIS access was present in 1985, at a time when the Internet was used only by a homogenous and limited community of academics who found it convenient to stay in touch with peers in a way similar to the offline practice of using a phonebook directory. What should be underscored in this context is that the registration in the WHOIS database was not regarded as operationally, contractually, or otherwise legally compulsory for the domain name registrant.

The information that was to be submitted voluntarily to the WHOIS database largely corresponds to the information that is compulsorily required nowadays of domain name registrants in compliance with current WHOIS policies.

Subsequent to the opening of the Internet to commercial registrants and the general public, and following the creation of the hierarchical DNS system as we know it today, the full implications and possible uses of the WHOIS service and associated databases emerged. As domain names acquired economic value, they began to be registered not only for lawful purposes, but also for purposes of speculation, and their content sometimes challenged legitimate intellectual property rights long consecrated in the offline world. Despite these changes, the WHOIS protocol remained unchanged.[32]

The provision of WHOIS service became compulsory upon the creation of ICANN. In 1998, the Memorandum of Understanding between ICANN and the US Department of Commerce,[33] as well as the ICANN Bylaws annexed to it, introduced a new system in which the functions of the registries were separated from those of the registrars. While the registries[34] had a monopoly over the management of the TLDs to which they were assigned, multiple registrars had to compete for providing registration services to the end-users within the same TLD. Thus, the maintenance of customer account records was distributed

32 RFC 954 was superseded as late as 2004 by RFC 3912. The latter removed from the previous document the elements that were "no longer applicable in today's Internet" but did "not attempt to change or update the protocol per se, or document other uses of the protocol that have come into existence since the publication of RFC 954". See Abstract for RFC 3912: Whois Protocol Specification (September 2004), <http://www.faqs.org/rfcs/rfc3912.html>.

33 For details of the Memorandum of Understanding and other aspects of the relationship between ICANN and the US Department of Commerce, see Bygrave & Bing (eds.), *Internet Governance*, *op. cit.*, Chapter 3 (section 3.2.8) and Chapter 5 (section 5.1.3).

34 Originally, in accordance with Definition 4 in the Registry Agreement of 04.11.1999 between NSI and ICANN, NSI was the only registry for .com, .net, and .org TLDs, and any other new gTLDs that were to be established. The agreement is available at <http://www.icann.org/en/nsi/nsi-registry-agreement-04nov99.htm>.

among multiple registrars and the previously centralised WHOIS records were spread among multiple databases.

As a consequence of the opening of the market for registrar services, previously achievable WHOIS searches (e.g., a search for all .com/.net/.org domains registered by a particular person) were no longer possible on a TLD-wide basis.[35] Instead, separate WHOIS databases were provided by the registrars and their cooperation was needed for any future re-establishment of a wide TLD search functionality.

Prior to the provision of any kind of services to interested parties, the gTLD registrars needed to undergo an accreditation procedure by ICANN. The first version of the Registrar Accreditation Agreement (RAA)[36] stipulated in section F that registrars "*shall* provide an interactive web page and a port 43 WHOIS service providing free public query-based access to up-to-date (i.e. updated at least daily) data concerning all active SLD registrations sponsored by registrar in the registry for the .com, .net, and .org TLDs" (emphasis added).[37]

However, as stated at the time by ICANN's general counsel, Louis Touton,[38] several difficulties arose in the attempt to implement WHOIS policies in accordance with the newly introduced distributed registration system. The different formats that had already been implemented by registrars hindered the provision of a consistent TLD-wide domain-name-lookup service.[39] Moreover, some registrars provided additional information in response to a WHOIS query (i.e., whether the domain was subject to a UDRP procedure). It was unclear whether limitation of the number of queries could be introduced in order to prevent abusive use or overly burdensome use of WHOIS service. Additionally, although the RAA compelled the registrars to require the designation of technical and administrative contacts by the registrants, their roles were unclear.

35 See too section 6 of RFC 1580: Guide to Network Resource Tools (March 1994), <http://www.faqs.org/rfcs/rfc1580.html>.

36 The first version was issued in 4.11.1999. It can be consulted at <http://www.icann.org/en/nsi/icann-raa-04nov99.htm#IIF>. The revised version of the RAA, issued in 2001, is still in force.

37 The obligations imposed on the registrars by ICANN through the RAA with regard to the collection and further processing of data in WHOIS databases is analysed in detail in Chapter 3.

38 See Letter from Louis Touton to the Committee Requesting Advice on Implementation (01.12.2000), at <http://www.icann.org/en/committees/whois/touton-letter-01dec00.htm>.

39 A .com/.net/.org WHOIS Committee was convened by the ICANN staff to give advice on implementation of WHOIS service for the .com/.net/.org domains as required under the Registrar Accreditation Agreement. This Committee recommended in response to Touton's Letter that .com/.net/.org registrars should provide WHOIS replies in a standard format. See the Committee's response of 06.03.2001 at <http://www.icann.org/en/committees/whois/committee-recommendations-06mar01.htm>.

There was also insufficient information as to whether the RAA opens for the possibility of providing anonymous registration mechanisms and if so, which ones.

It soon became apparent that the simplistic InterNIC WHOIS service that existed in .com, .net, and .org prior to the introduction of multiple registrars was no longer adequate in the distributed DNS. On the other hand, the data made freely available through WHOIS databases gained greater economic significance, so that there was an increase in political pressure from the various groups wanting to advance their interests. One began to encounter cases in which trademark-monitoring service providers systematically collected WHOIS data and compiled it in analyses that were then sold to trademark holders. Domain name registration and web site hosting began to evolve into a profitable industry, and access to registration records and to zone files[40] was also being used to gain marketing data.

Thus, within a few years from the Internet's commercialization, it had become fairly common practice to use WHOIS as a form of identification, surveillance and data mining, often with the help of automated bots to gather data. An instance of this practice came into focus in the case *Register.com, Inc. v. Verio, Inc.*[41] Verio's activity involved periodic collection of zone files from the .com, .net, and .org registry. Subsequently, by comparing sequential versions of those files to determine which names were newly registered, automated processes could be set up for querying the WHOIS service of Register.com. Based on the data obtained in this way, Verio was spamming the Register.com registrants by e-mail and by telephone. Verio's behaviour was in blatant breach of a restriction introduced by Register.com in an annex to its WHOIS data policy which prohibited the use for direct marketing purposes of the data made available via WHOIS. However, in an *amicus curiae* brief filed in the litigation,[42] ICANN considered that the limitation imposed by Register.com towards direct marketing violated the provisions of the RAA. The RAA expressly prohibited the registrars from introducing more restrictive policies regarding access to their services than those set forth by ICANN on access and use of WHOIS data. Nonetheless, acknowledging that Verio's activity or similar behaviour could adversely affect Register.com as well as the other registrars' operation of the domain-name

40 The zone files contain a list with all the registered domain names in a certain top-level domain.

41 *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), available at <http://www.spamseminar.com/materials/register-verio.html>.

42 Brief of 22.09.2000 available at <http://www.icann.org/en/registrars/register.com-verio/amicus-22sep00.htm>.

registration system, ICANN subsequently introduced, in a "Zone File Access Agreement",[43] some restrictions on the use of the publicly accessible data.

Parallel to the creation of the ccTLDs, the increase in the number of registered domain names and the diversification in the purposes for using WHOIS data, legally-based principles for privacy and data protection were taking shape in Europe. A new category of players and interests thus joined the discussion concerning the most appropriate WHOIS policies.

In Europe, Directive 95/46/EC[44] introduced several guarantees for ensuring that the processing of personal data is lawful and that the data subject provides informed consent to the collection of own personal data. The rights of the data subjects as well as the requirements imposed on the data controllers were a central issue for debate. The International Working Group on Data Protection in Telecommunications released in May 2000 a "Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet"[45] in which they raised the issue concerning personal data (such as name, address and telephone number) being collected from the applicants for domain names and then regularly making this information publicly available on the Internet via the WHOIS database. They expressed the concern that the Registrar Accreditation Agreement (RAA) developed by ICANN does not sufficiently reflect the goal of personal data protection for domain name holders and recommended areas for improving such protection.

On the other side of the Atlantic, however, in the USA, most of the stakeholders invited to the discussions on WHOIS databases were fervent supporters of interests different from those of the privacy activists. Three Congressional hearings addressing WHOIS issues were organised between July 2001 and September 2003.[46] During those hearings, the privacy and data protection concerns relating to the wide availability of personal data, although acknowledged,

43 See, e.g., Article 4 of the Agreement for VeriSign, Inc. at <http://www.verisign.com/static/002493.pdf>.

44 Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. L 281, 23.11.1995, pp. 31–50).

45 Available via <http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group>.

46 The three Congressional Hearings were "WHOIS Database: Privacy and Intellectual Property Issues" (12.07.2001; transcript at <http://commdocs.house.gov/committees/judiciary/hju73612.000/hju73612_0f.htm>), "Accuracy and Integrity of WHOIS Database" (22.05.2002; transcript at <http://commdocs.house.gov/committees/judiciary/hju79752.000/hju79752_0f.htm>) and "Internet Domain Name Fraud – The US Government's role in ensuring public access to accurate and up to date WHOIS data" (04.09.2003; transcript at <http://commdocs.house.gov/committees/judiciary/hju89199.000/hju89199_0f.htm>).

were to a great extent regarded as incidental and relatively insignificant when compared, for example, with the interests of intellectual property rights holders or the goal of prompt law enforcement. ICANN was encouraged to use all its prerogatives afforded by the Bylaws to ensure that registrars publish accurate WHOIS data (especially concerning the registrant) and that they keep these data freely accessible.

Such opinions, however, disregard the technical status of the WHOIS protocol, as widely acknowledged by the RFC specifications. RFC 3912 expressed in 2004 the concern that the

> *"WHOIS protocol has no provisions for strong security. WHOIS lacks mechanisms for access control, integrity and confidentiality. Accordingly, WHOIS-based services should only be used for information which is non-sensitive and intended to be accessible to everyone. The absence of such security mechanisms means this protocol would not normally be acceptable to the IETF (Internet Engineering Task Force) at the time of this writing."*

The Congressional hearings raised a political issue as well. One of the major obstacles in making use of WHOIS data was that the information entered into it was not verified or authenticated at the point of entry, which led to inaccurate, obsolete, or deliberately misleading records. While some constraint on the gTLD registries and accredited registrars had been introduced by their agreements with ICANN, the same could not be imposed on the ccTLD registries and their registrars.

In addition to being pressured to use its prerogatives and enforce the agreements entered into with gTLD registrars and registries, ICANN was subjected to political pressure from the US-based stakeholders, who claimed that through its participation in GAC, the US government should "continue to urge its foreign counterparts to insist that the operators provide free, real time, unrestricted access to public access to the full range of WHOIS data elements".[47]

Acknowledging the multitude of conflicting interests at stake in the debate over WHOIS service, ICANN implemented by early 2001 a Policy Development Process aimed primarily at clarifying the status and the policies relating to WHOIS service under the new distributed databases regime. The fact that this process has not been finalised at the time of concluding this report illustrates the difficulty in reaching international consensus on fundamental legal questions that are encountered when analysing WHOIS.

---

47 See written statement submitted by Stevan D. Mitchell on behalf of the Interactive Digital Software Association at the Congressional hearing of 12.07.2001; accessible via <http://commdocs.house.gov/committees/judiciary/hju73612.000/hju73612_0f.htm>.

In a teleconference of the DNSO Names Council held 08.02.2001,[48] it was unanimously decided to set up a WHOIS Committee with a mandate to:

- request ICANN to create a web site and mailing list for the purpose of soliciting comments of substance on the ICANN (Staff) WHOIS Committee[49] report and inviting other interested groups to submit Position Papers for substantive comment on the web site and mailing list;
- assimilate the submitted Position Papers and comments into a report highlighting areas of convergence and identifying areas where more work may be necessary;
- prepare a Charter, where additional work areas are identified, to be considered by the entire DNSO Names Council, leading in turn to the possible appointment of a Task Force and/or Working Group to address the identified issues.[50]

A WHOIS Task Force was subsequently set up by the DNSO Names Council and it issued a Policy Report on "Accuracy and Bulk Access" in November 2002.[51] The report included recommendations for further work in two key areas:

1. Improving the accuracy of the data collected in the WHOIS database;
2. Examining the use of WHOIS data for marketing purposes and the provisions regarding bulk access to WHOIS databases.

Based on feedback on the report from the Names Council, constituencies and the Internet community, a Final Report was published in February 2003.[52] The recommendations expressed therein were considered by the ICANN Board, which adopted two Consensus Policies:

48 "DNSO" stands for "Domain Name Supporting Organization", the predecessor of GNSO.

49 Reference is made here to the .com/.net/.org WHOIS Committee which between March 2001 and April 2001 made recommendations for the ICANN staff on implementation issues under the contractual provisions already in place between ICANN and .com/.net/.org registrars. On the other hand, the Committee that was just started during the DNSO Names Council teleconference in February 2001 was to consider proposals for changes in WHOIS policy in the framework of DNSO (now GNSO) – primarily responsible for working toward consensus-based recommendations on DNS policy.

50 See Agenda Item 3 of the minutes of the meeting, at <http://www.dnso.org/dnso/notes/20010208.NCtelecon-minutes.html>.

51 Report issued 30.11.2002; available at <http://www.dnso.org/dnso/notes/20021130.NCWhoisTF-accuracy-and-bulkaccess.html>.

52 Final Report of the GNSO Council's WHOIS Task Force, "Accuracy and Bulk Access" (06.02.2003); available at <http://www.icann.org/en/gnso/whois-tf/report-19feb03.htm>.

1. the WHOIS Data Reminder Policy which requires registrars, on an annual basis, to provide the registrants with whatever data are available in the WHOIS Database concerning the respective domain name(s) registered, and to give them an opportunity to make corrections and or update information;[53]
2. the WHOIS Marketing Restriction Policy prohibiting, via bulk access agreements, the use of data made available by the registrars to third parties for any marketing activities.[54]

As Consensus Policies, they are binding on the gTLD ICANN-accredited registrars. The remainder of the rules applicable to WHOIS service remain in force as a consequence of inertia and maintenance of the original WHOIS protocol, enforced via binding agreements.

The WHOIS Task Force did not, however, address other relevant issues regarding the management of the data included in the WHOIS database.[55] This led to the creation in October 2003 of three other WHOIS Task Forces, as part of the GNSO's Policy Development Process.

WHOIS Task Force 1 was commissioned

> *"to determine what contractual changes (if any) are required to allow registrars and registries to protect domain name holder data from data mining for the purposes of marketing. The focus is on the technological means that may be applied to achieve these objectives and whether any contractual changes are needed to accommodate them".*[56]

While the above-mentioned WHOIS Marketing Restriction Policy addressed only the issue of WHOIS data made available via bulk access agreements, the activity of this Task Force concentrated on the protection of the data made available via port 43 and query-based web access to the same data. While the beneficiaries of the bulk access to WHOIS data are known (since they signed an agreement), the identities of the holders of the information obtained through data mining are far less obvious, making enforcement actions against them a much more laborious process.

---

53 Adopted 27.03.2003; available at <http://www.icann.org/en/registrars/wdrp.htm>

54 Adopted 27.03.2003 (applicable from 12.11.2004); available at <http://www.icann.org/en/registrars/wmrp.htm>.

55 See too a WHOIS Privacy Issue table drafted 14.08.2003 by GNSO, based on an evaluation of relevant WHOIS issues done by the GNSO Constituencies.

56 See Terms of Reference at <http://gnso.icann.org/issues/whois-privacy/tor.shtml>.

WHOIS Task Force 2 was commissioned to review the data collected and displayed in WHOIS databases and the practices around the notification of the registrants regarding the uses for which the data are collected and processed.[57] Among the questions to be answered were: What is the best way to inform registrants about what data are made publicly available? What changes, if any, should be made to the data elements that must be collected from registrants at the time of registration? Should registrants be allowed to remove certain parts of the required contact information from public display?

WHOIS Task Force 3 had as its task "to develop mechanisms to improve the quality of contact data that must be collected at the time of registration, in accordance with the registrar accreditation agreement (in particular clauses 3.3.1 and 3.7.7.1), and the relevant registry agreement".[58]

The Task Forces started their tasks separately, but due to numerous overlaps in their fields of competence, they continued their activity together from 2005. Functioning jointly, the Task Forces were assigned five research tasks by the GNSO:

1. Define the purpose of WHOIS service;
2. Define the purpose of the registered name holder, technical, and administrative contacts, in the context of the purpose of WHOIS, and the purpose for which the data were collected;
3. Determine what data collected should be available for public access in the light of the purpose of WHOIS. Determine how to access data that are not available for public access;
4. Determine how to improve the process for notifying a registrar of inaccurate WHOIS data, and the process for investigating and correcting inaccurate data;
5. Determine how to resolve differences between the obligations of, respectively, registered name holders, gTLD registrars and/or gTLD registries to abide by all applicable laws and governmental regulations that relate to WHOIS service, as well as the obligation to abide by the terms of the agreements with ICANN that relate to WHOIS service.[59]

In tackling the first-listed research task, the constituencies expressed their position on the purpose of WHOIS and WHOIS contacts and drafted in

57 See Terms of Reference at <http://gnso.icann.org/issues/whois-privacy/tor2.shtml>.
58 See Terms of Reference at <http://gnso.icann.org/issues/whois-privacy/tor3.shtml>.
59 See Terms of Reference for the functioning of the joint WHOIS Task Forces at <http://gnso.icann.org/policies/terms-of-reference.html>.

March 2006 the "Final Task Force Report on the Purpose of WHOIS and WHOIS Contacts".[60] However, they failed to reach consensus during the subsequent discussions held on the topic in the GNSO Council.

Aware that the fulfilment of the subsequent four research tasks depended on a definitive statement regarding the first issue, and being obliged to choose between two possible definitions of the purpose of WHOIS service, the GNSO Council decided,[61] for the purposes of carrying out research on tasks 2–5, that the Task Force should adopt the narrower and more technical of the two definitions. That definition states:

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

Concrete results were also achieved with respect to the fifth-listed research task. A policy recommendation was drafted for a procedure by which to handle conflicts between a registrar's or registry's obligations under local privacy laws and their contractual obligations to ICANN.[62] The recommendation was incorporated into the GNSO Council Report to the ICANN Board and approved by the latter as consensus policy on 10.05.2006.[63]

Research tasks 2, 3 and 4 were the focus of a Final Task Force Report on WHOIS Services, issued 16.03.2007.[64] The Task Force submitted for debate two reform proposals, the one commonly known as the Operational Point of Contact Proposal (The OPoC proposal) and the other one known as the Special Circumstances Proposal. The result of the Task Force members' vote was a simple majority of 7:6 in favour of the OPoC Proposal, which was therefore adopted with significant reservations as the Task Force Recommendation to the GNSO Council.

---

60 Report of 15.03.2006 available at <http://gnso.icann.org/issues/whois-privacy/tf-report-15mar06.htm#0.1>.

61 See minutes of the GNSO Council Meeting of 12.04.2006 at <http://gnso.icann.org/meetings/minutes-gnso-12apr06.shtml>.

62 Available at <http://gnso.icann.org/issues/tf-final-rpt-25oct05.htm>.

63 The GNSO Council Report is available at <http://gnso.icann.org/issues/whois-privacy/council-rpt-18jan06.htm>. The approved procedure is elaborated in Chapter 4.

64 Available at <http://gnso.icann.org/issues/whois-privacy/whois-services-final-tf-report-12mar07.htm>. The Preliminary Report of 22.11.2006 is available at <http://gnso.icann.org/issues/whois-privacy/prelim-tf-rpt-22nov06.htm>.

In broad terms, the OPoC Proposal introduced the possibility of a new identity layer between the domain name holder and the registrar. Rather than publishing the contact details of the domain name holder in the WHOIS database, the contact details of an OPoC would appear instead. The registrar, the domain name holder itself, or a third party it designated would be able to fulfil the role of an OPoC.

In March 2007, the GNSO Council created and chartered a WHOIS Working Group to further develop the recommendations of the previous Task Force by addressing the concerns raised by the community during the public comments sessions and to seek to reach greater consensus on improvements to WHOIS service.[65]

The Working Group endeavoured itself to achieve a consensus among stakeholders on the following issues:

- the roles, responsibilities, and requirements of the contacts available for unrestricted public query-based access, as well as consequences of non-fulfilment;
- how and which legitimate third parties may access registration data that is no longer available for unrestricted, public, query-based access;
- whether a distinction could be made between the amount of publicly available contact information according to either the nature of the registered name holder (e.g., legal as opposed to natural persons) or to the use of the domain name (e.g., commercial as opposed to non-commercial use).

The Working Group provided a Final Outcomes Report to the GNSO Council in August 2007.[66] Based on the conclusions of this report, the GNSO Council requested in early September that the ICANN staff prepare an overview and implementation notes regarding WHOIS.[67] These documents were delivered to the GNSO Council a month later. The ICANN staff suggested in the implementation notes that a streamlined implementation of the OPoC proposal may be more appropriate than a "full-blown" one, in order to minimise the complexity, cost or other potential challenges inherent in an extensive transformation such as that called for in the Working Group's Proposal.

65 The Charter incorporating the Working Group's working plan, objectives and methods is available at <http://gnso.icann.org/issues/whois-privacy/whois-wg/whois-working-group-charter-16apr07.pdf>.

66 Report of 20.08.2007 available at <http://gnso.icann.org/drafts/icann-whois-wg-report-final-1-9.pdf>.

67 The implementation notes are available at <http://gnso.icann.org/drafts/gnso-whoiswg-report-staff-implementation-notes-11oct07.pdf> ; the overview at <http://www.gnso.icann.org/drafts/icann-staff-overview-whois13sep07.pdf>.

However, the ICANN Board failed to reach consensus on the OPoC proposal at the ICANN meeting in Los Angeles (29.10.–02.11.2007), despite the suggested streamlined implementation and the fact that the proposal represents a relatively broad consensus among stakeholders. Consequently, the WHOIS database regime remains governed at gTLD level by the policies in the Registrar Accreditation Agreement of 2001 and the corresponding Registry Agreements. At the ccTLD level, the provisions of the national laws and locally set policies continue to apply, regardless of the Policy Development Process occurring at gTLD level in the ICANN framework.

2.1.2 Input, search and output variations

Despite a de facto agreement on the need to make publicly accessible the identity of a domain name registrant as well as their contact details and servers used, many divergent opinions exist on how WHOIS service should be provided. At gTLD level, due to the centralised policy-making competence of ICANN, the provision of WHOIS service is more standardised in comparison with the national ccTLD domains. Without discussing the legal implications of the different solutions, this section illustrates some of the major differences in the provision of WHOIS service in .com, .eu and .no. The arbitrarily selected examples are <www.access.com>, <www.access.eu> and <www.access.no>.

In .com, WHOIS service is provided both by registrars and registries, although a different range of information is made publicly available at each level. WHOIS data are displayed via three methods: individual web-based query, port 43 queries and bulk access to zone files. In order to look for information about a certain name in the .com domain in the WHOIS database, the exact domain name must be introduced in a given field on the respective website of the registrar or registry.

As a result of a web-query, the registry will display information about the identity of the registrar, its WHOIS server and website, the name servers used, as well as information about the creation and expiry dates and the date when the information was most recently updated. On the other hand, the *registrar's* WHOIS database displays all information collected from the registrant upon registration of the domain name, irrespective of whether the registrant is a natural or a legal person. This model is commonly known as the "thin model". An example is set out in Figures 4 and 5 below:

```
Domain Name: ACCESS.COM
Registrar: MARKMONITOR INC.
Whois Server: whois.markmonitor.com
Referral URL: http://www.markmonitor.com
Name Server: HORSE.AVNET.COM
Name Server: SPARROW.AVNET.COM
Status: clientTransferProhibited
Status: clientUpdateProhibited
Status: clientDeleteProhibited
Updated Date: 01-feb-2007
Creation Date: 25-aug-1991
Expiration Date: 24-aug-2012
```

Figure 4:
Model WHOIS search registry .com

```
Registrant:
        Avnet, Inc. (DOM-1585750)
        30 S. McKemy Avenue
        Chandler AZ 85226
        US

   Domain Name: access.com

        Registrar Name: Markmonitor.com
        Registrar Whois: whois.markmonitor.com
        Registrar Homepage: http://www.markmonitor.com

   Administrative Contact:
        Administrative Contact (NIC-14210347)  Admincontacts (AD6687-ORG)
        30 S. McKemy Avenue
        Chandler Az 85226
        US
        admincontacts@avnet.com
        +1.4806436547
        Fax- +1.4806436996
   Technical Contact, Zone Contact:
        Technical Contact (NIC-14210349)  techcontacts(TE778-ORG)
        30 S. McKemy Avenue
        Chandler AZ 85226
        US
        techcontacts@avnet.com
        +1.4806436547
        Fax- +1.4806436996

   Created on..............: 1991-Aug-24.
   Expires on..............: 2012-Aug-23.
   Record last updated on..: 2007-Feb-13 12:35:27.

   Domain servers in listed order:

   HORSE.AVNET.COM
   SPARROW.AVNET.COM
```

Figure 5:
Model WHOIS search registrar .com

Section 3.3.1 of the Registrar Accreditation Agreement (RAA) requires that the WHOIS database at registrar level be maintained separate from the "registration data database", whereas a centralised WHOIS database containing information about all the domain names registered under .com should be provided at the registry level. This registry's WHOIS database contains the information that each registrar providing registration services under .com is committed to supply to the registry by virtue of section 3.2 of the RAA. All the information is displayed in text format.

The .com registry also provides bulk access to zone files (with the names of all the domains registered under .com) to third parties with whom it entered into a bulk access agreement. However, the agreement prohibits, among other things, the use of the data for direct marketing purposes as well as the subsequent transmission of the data to another entity that would use them for similar marketing purposes.

In .eu, the WHOIS database is provided by EURid, the .eu registry, and not by the individual registrars. In compliance with Article 4.4 of the ".EU Registry Agreement between EURid and ICANN", the .eu registry is obligated to abide by existing or future policies developed by ICANN where they concern the interoperability and technical operation of the domain. Arguably, given the purpose of WHOIS service, the policies concerning the provision of that service would come under the scope of this provision. However, it is unclear to what extent ICANN would be willing to react to an alleged infringement of this provision by sanctioning the behaviour of the registry.

EURid has adopted a "thick model" for providing WHOIS service. By this is meant that the registry (and no registrars) owns a centralised WHOIS database and provides access to it.

EURid requires the domain name registrant to provide the same amount of information as requested by ICANN policies. However, the amount of information displayed following a web query differs for registrants who are legal persons and registrants who are natural persons. For legal persons, all data collected are publicly displayed, whereas only the e-mail address of a natural person is made publicly available (unless otherwise requested by the registrant). All the other information collected from natural persons is kept by the registry for internal use. This may be released to third parties only following the request of a law enforcement authority or after the requesting party fills in an application form identifying the requestor and the purpose of the request. After verification and approval of the application by EURid, the information is transferred to the requesting party.

When making a simple web query, the user initially receives only information on whether the domain is registered or currently available. If the requesting party needs more information, an automatically generated random code must be filled in (see below). Since the code is not machine-readable, this measure hinders, to a certain extent, the possibility for automatic queries. Once the code is filled in, the full WHOIS records are displayed.

As opposed to the .com WHOIS service, the .eu registry restricts the number of requests coming from the same source to 100 domain names per day. Moreover, the personal information displayed appears as images and not as text records.

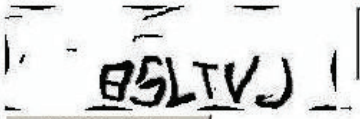
access.eu: Not available for registration

What this means

This domain name is not available for registration.
If you believe you have the right to a .eu domain name that is already registered, you may dispute the registration.

More information

For additional details on access.eu, type the code below into the text box provided and click on More Information. Users of the WHOIS database are required to enter a code as a security measure as it stops automated programs from getting and abusing WHOIS information.



More information

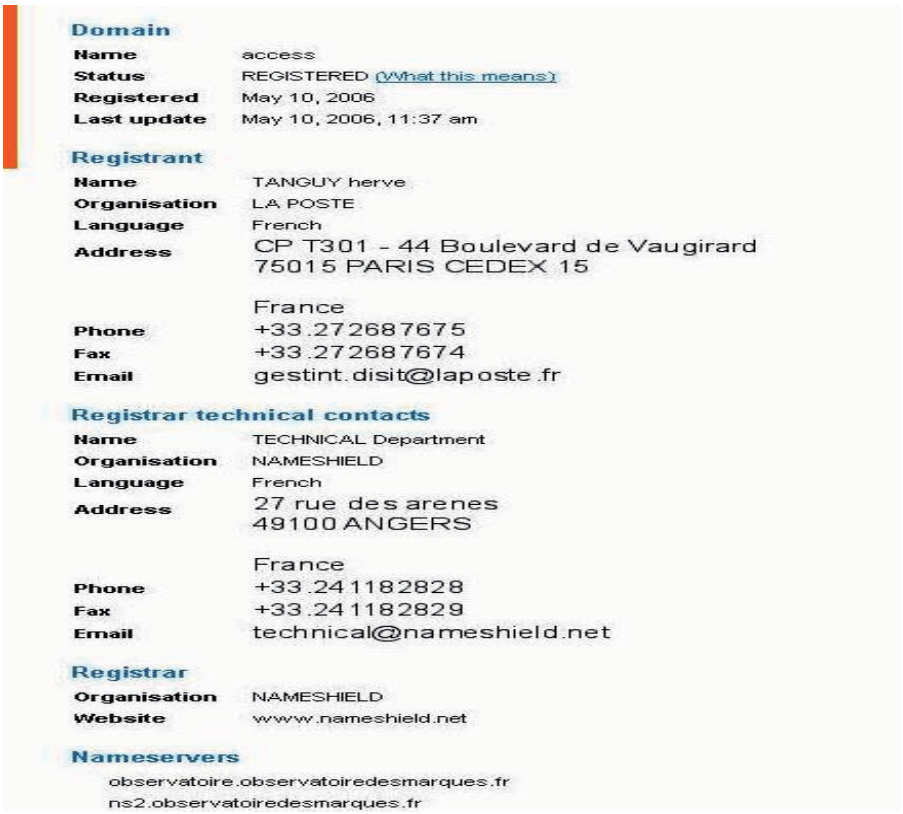
WHOIS legal statement and terms & conditions

The WHOIS service offered by EURid and the access to the records in the EURid WHOIS database are provided for information purposes only. It allows persons to check whether a specific domain name is still available or not and to obtain information related to the registration records of existing domain names.

EURid cannot, under any circumstances, be held liable should the stored information prove to be wrong, incomplete or inaccurate in any sense.

By submitting a query you agree not to use the information made available to:

- Allow, enable or otherwise support the transmission of unsolicited, commercial advertising or other solicitations whether via email or otherwise;
- Target advertising in any possible way;
- Cause nuisance in any possible way to the registrants by sending (whether by automated, electronic processes capable of enabling high volumes or other possible means) messages to them.



Domain

Name	access
Status	REGISTERED (What this means)
Registered	May 10, 2006
Last update	May 10, 2006, 11:37 am

Registrant

Name	TANGUY herve
Organisation	LA POSTE
Language	French
Address	CP T301 - 44 Boulevard de Vaugirard 75015 PARIS CEDEX 15 France
Phone	+33.272687675
Fax	+33.272687674
Email	gestint.disit@laposte.fr

Registrar technical contacts

Name	TECHNICAL Department
Organisation	NAMESHIELD
Language	French
Address	27 rue des arenes 49100 ANGERS France
Phone	+33.241182828
Fax	+33.241182829
Email	technical@nameshield.net

Registrar

Organisation	NAMESHIELD
Website	www.nameshield.net

Nameservers

observatoire.observatoiredesmarques.fr
ns2.observatoiredesmarques.fr

Figure 6: Model registry WHOIS search in .eu

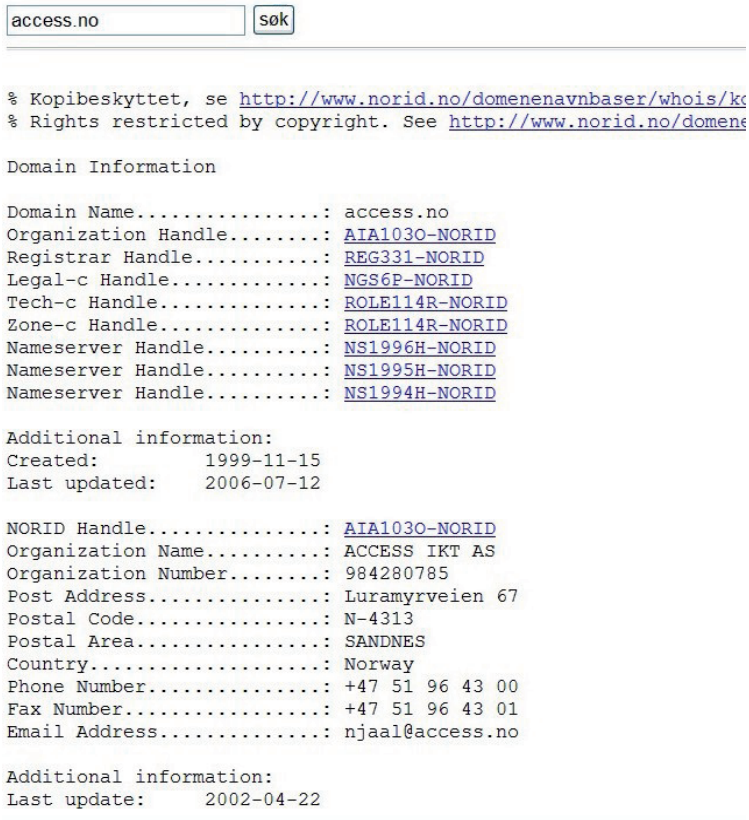
The data in both the .com and the .eu WHOIS database are protected against destruction through Data Escrow Agreements.

The third example considered for this study is the .no WHOIS service. Following the "thick model" as well, the registry for the .no domain owns the WHOIS database and provides WHOIS service. As opposed to .eu, only legal persons may currently register domain names under .no.[68] After verifying the correctness of the application forms filled in by the registrants, the registrars

68 NORID is currently considering the possibility of opening domain names to registration by natural persons.

submit the request to Norid for registration. The registry will then collect the information in the customer database and subsequently provide access to parts of the customer database through the WHOIS protocol (the same types of data as requested by ICANN).

The special feature of the WHOIS data display mode in the .no domain is the creation of "handles", i.e., record-IDs designating the same set of data. The handles prevent duplications in the database and allow for a broader range of searches in addition to those using the exact name of the domain as search word. Each handle can be individually searched resulting in information about the set of data it designates as well as information about other .no domain names where the same handle also appears (in the same role or a different one).



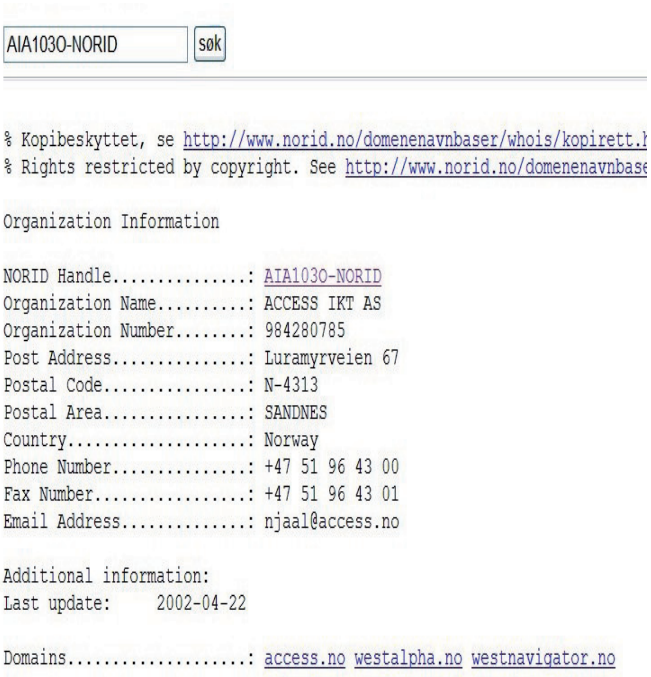


Figure 7: Model registry WHOIS search in .no

Bulk access to .no zone files is not permitted and the WHOIS database is not the object of a data escrow agreement with a third party.

2.2 Functions of WHOIS databases

This section explores the issue of usefulness or usability of the information made publicly available via WHOIS databases. The focus is therefore on the part of registration data that is made freely available to the public via web,via port 43 or as part of bulk access agreements. Data about the registrant are collected upon the registration of a domain name not only as a requirement for enabling the technical operation of the domain name, but also in order to provide WHOIS service. This section looks into the possible legitimate uses made of the public WHOIS data.

The anticipated, intended outcome or guiding purpose for the provision of the gTLD WHOIS service, according to the GAC[69], is:

> *"to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS nameserver".*

The European Commission Regulation for the .eu domain (Regulation (EC) No. 874/2004) acknowledges that the WHOIS database is a source of information. However, the definition of the service does not specify the usage of the information thus collected:

> *"The purpose of WHOIS database shall be to provide reasonably accurate and up to date information about the technical and administrative points of contact administering the domain names under the .eu TLD" (Article 16(1)).*

The ".eu Domain Name WHOIS Policy" issued by EURid states, moreover, that disclosure of personal data beyond what is made freely available through WHOIS service may be justified for "legitimate purposes", but these purposes are not explicitly specified.

In the .no ccTLD, the registry defines the WHOIS database as "a searchable database which contains all registered information about .no domains. […]".[70] In the memorandum provided by the registry on "Use of information stored in Norid's customer database,[71] a distinction is made between the customer database, which is used only by Norid in order to "ensure the effectiveness and the quality of the registration services provided", and the WHOIS database, which includes the section of the customer database that is made available to third parties. Norid subsequently provides a non-exhaustive list of legitimate uses that can be made of the data published via WHOIS:

- to check whether the domain name is available or registered;
- to find out information about who is responsible for a certain registered domain;
- to check whether one's own registered information is correct or updated;

---

69 The definition by GAC is admittedly a working definition, which enabled the GNSO WHOIS Task Force to continue research on relevant WHOIS issues.

70 See <http://www.norid.no/ordliste/index.en.html>.

71 See entry for "Bruk av informasjon lagret i Norids Kundedatabase" at <http://www.norid.no/domenenavnbaser/personvernpolicy.html>.

- to allow rights holders to verify whether an infringement of their rights has occurred;
- to allow law enforcement actions by the police.

Whereas .com and .eu policies stipulate the overall purpose for the provision of WHOIS, the .no WHOIS policy exemplifies, rather than defines, the purpose of the service. This approach could hinder the effort to rank or balance the various uses for which WHOIS information should be employed, when the legitimate interests exemplified clash with other values guaranteed by national legislation. A definition in clear terms of the purposes for collecting the data, rather than an identification of the people who may benefit from publicly accessible information, is a prerequisite for formulating effective policies governing collection, access and transfer of data. Policy requirements can be derived from an explicit, well-defined purpose in order to protect data subjects from abuse by data collectors or by third parties using the data. Furthermore, a clear definition would facilitate the detection and investigation of behaviour different from or incompatible with the purpose that legitimised the collection of WHOIS data.

In examining what the practical uses of the published WHOIS data are, one may distinguish among several classification criteria:

- the stakeholder who would benefit from accessing the database (the registrant, the IP rights holders, consumers, law enforcement authorities, network administrators);
- the purpose of the query (to check, to obtain information, to request an action); or
- the core values that are served by the publication of some registrant data, in the light of the core values of ICANN and of DNS management.

The third of the above criteria is regarded as most appropriate in the context of the study, for three main reasons. Firstly, it enables one to assess the utility of the WHOIS database in the context of the DNS operation rather than as a stand-alone service, thus making apparent the central role played by WHOIS service in the overall management of the DNS. Secondly, it emphasises the high-level values aimed for through the provision of the service, regardless of the conflicting interests of the various categories of stakeholders. Thirdly, it emphasises that the WHOIS service is provided in the interest of general values whose legitimacy transcends the boundaries of national jurisdictions, thereby justifying the adoption of consensus policies at international level.

The following sub-sections describe the three main functions of WHOIS data and identify requirements for their fulfilment.

2.2.1 Technical operability

As explicitly acknowledged by GNSO's definition of the purpose of the WHOIS service, the technical rationale of WHOIS data is central to the provision of the service. The main mission of ICANN is "to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems" (Bylaws Article 1). A reliable WHOIS service may contribute to the achievement of this mission.

The WHOIS service was developed in order to allow network operators to contact each other in order to ensure efficient connectivity between networks.[72] Nowadays, WHOIS still provides an essential capability to network operators and security personnel to identify system failures and track down those seeking to propagate computer viruses or otherwise cause harm. The technical operation of the DNS is dependent on the possibility to identify and to contact the responsible party for the technical operation of a domain name, for informing a person or organization about inappropriate use of their resource (security), or about incorrect configuration of their resource (stability). WHOIS data, therefore, are important for the security and stability of the Internet since the administration and control of Internet resources are widely distributed.[73]

WHOIS data do not disclose merely the identity of the registrant and their technical contact point, but also reveal domain delegation data,[74] such as, in the examples provided in section 2.1.2, the zone that was delegated ("avnet") and the zone that the delegation belongs to ("com"), the date that the delegation was granted and when the delegation next expires, which domain name servers are authoritative for this particular zone ("horse and sparrow.avnet.com") and the status of the delegation ("REGISTRAR-LOCK"). Such data facilitates the technical co-ordination and inter-operation of specific delegations within the registration and the DNS.

Some examples of technical operations enabled by WHOIS data are:

---

72 See, *inter alia*, OECD's Working Party on Telecommunication and Information Services Policies, "Comparing Domain Name Administration in OECD Countries" (DSTI/ICCP/TISP (2002)11/FINAL; 08.04.2003), available at <http://www.oecd.org/dataoecd/46/38/2505946.pdf>.

73 See WHOIS Recommendation of ICANN's Security and Stability Advisory Committee (SSAC), issued 07.02.2003; available at <http://www.icann.org/en/committees/security/sac003.pdf>.

74 See comments of the Registrar Constituency to WHOIS Task Force Report on the purpose of WHOIS and of WHOIS contacts, at <http://gnso.icann.org/issues/whois-privacy/tf-report-15mar06.htm#0.4d>.

- "Resolving issues related to lame delegation (i.e. delegation records that specify nameservers that are not authoritative for the delegation in question).
- Determining which name servers are intended to be authoritative for a specific delegation (i.e. comparing the delegation records with data from other sources while troubleshooting configuration issues).
- Determining the status of a delegation (INACTIVE, CLIENT LOCK, PENDING RENEW, and other status codes).
- Determining which delegant is responsible for the activity of a specific network host.
- Determining when a specific delegation was granted".[75]

However, for WHOIS data to be used by network administrators in the manner provided above, certain requirements should be met:
- The data must be accurate. The risk of inaccurate data exists especially where the registrants themselves provided the input information. This risk is lower for the data generated by the registrar;
- The configuration of WHOIS records and the protocol used should allow cross-registry searches without the need of a centralised WHOIS database;[76]
- WHOIS records should be provided in a common, standardised format that would make the data readily accessible and understandable, while providing sufficient guarantees against data harvesting.[77]

2.2.2 Transparency

WHOIS records convey three groups of information:
- (i) identity (the registrant, the technical and administrative points of contact, as well as the registrar who handled the registration);
- (ii) location (either physical address or e-mail address of the registrant, the contact points and the registrar); and
- (iii) domain related information (status, servers, registration and expiry dates, last update).

75 *Idem*.

76 Cf. the work of the now concluded CRISP (Cross-Registry Information Service Protocol) Working Group of the Internet Engineering Task Force. For an overview of that work, see <http://www.ietf.org/html.charters/OLD/crisp-charter.html>.

77 It is worth noting, however, that the requirements identified by ICANN's SSAC concern only WHOIS data accessible through the port 43 WHOIS protocol, not the results of web-based WHOIS queries.

Different groups of stakeholders may become interested especially in the availability and the accuracy of one or more of these types of information and may therefore claim a legitimate interest in having access to it.

When the identification information made available by an information society services provider on its website is non-existent or insufficient (despite the requirements of the EU's E-Commerce Directive),[78] the data in the WHOIS database may serve as an additional guarantee that the business operating on the Internet is legitimate. Additionally, WHOIS can inform one registrant about the identity of another registrant of a similar domain. Since domain names have become part of a company's marketing strategy, it can be useful to have an overview of websites operated by a competitor.

The registrants also use WHOIS as a method for checking data held by the registrar/registry, so that necessary corrections and updates can be made.

The information displayed via WHOIS allows business users to monitor the expiry dates of valuable domain name registrations and to reregister them for resale (dropcatching) at a profit. Moreover, bulk access to complete WHOIS records offers the opportunity to create value-added products and services (statistics, estimates, rankings).

The purpose of WHOIS databases has been narrowly defined by the GAC. In their view, justification for transparency of the registrant data (the possibility *to contact a responsible party*) is mainly the need to solve *issues related to the configuration of the records*. Although commercial gain cannot be said to represent a function incompatible with the general purpose of WHOIS records, it is definitely deemed, in GAC's view, to fall outside the scope of the provision of the service. It is questionable whether a "de facto" use justified by a commercial interest in the data could be used as a valid argument against initiatives leading to a decrease in the amount of information displayed as a result of privacy concerns. At the same time, the transparency achieved through the publication of personal data in WHOIS databases may represent a risk of privacy infringement. In some cases transparency may hinder the expression of controversial ideas and information that would fall, for example, under the protection of anonymity. Out of the need to limit potential harms arising from the unlimited availability of identity and location information via WHOIS, the registrars or third party service providers introduced software solutions to conceal or replace the information most targeted by such attacks (proxy services are one example of such technological measures). The shortcoming of this solution is that it makes the exercise

78 Directive 2000/31/EC of 08.06.2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (O.J. L 178, 17.07.2000, pp. 1–16); see particularly Article 5. This is described in more detail, *infra*, footnote 218.

of legitimate interests more time- and resource-consuming. The effect of the current WHOIS privacy policies for the .com, .no and .eu domains is discussed in more detail in Chapter 4.

For WHOIS service to create an adequate degree of transparency about the registrant and their contact points, about their location or about the domain name, certain requirements should be met:

- the information should be accurate;
- the information should be sufficient for allowing the contact to be made;
- the information should be provided in a format that minimises the risk of misuse.

2.2.3 Accountability

One of the most discussed functions of WHOIS databases is their ability to convey information about the identity of a domain name registrant to law enforcement authorities and to other stakeholders who may have a legitimate interest in holding accountable a registrant for detrimental or illegal activities perpetrated via the registered domain. WHOIS data may be used for law enforcement purposes, either directly by the prejudiced stakeholder or as part of a legal investigation. Chapter 5 of this report addresses in further detail questions related to the persons who should be given access to which information, under what policies and with what procedural guarantees of legitimacy. This section addresses only the potential of WHOIS data to be used in investigations, as witnessed in public and private organisations whose investigative practices include consultation of WHOIS databases. It also emphasizes the practical difficulties identified in accessing or properly using these data.

Since at least 2002, government agencies, particularly in the USA, have been very active in using WHOIS databases in investigations of crimes or other legal infringements committed via the Internet.[79] These agencies are the main proponents of the idea that, when creating policies governing the availability and accuracy of WHOIS data, one capital objective is to facilitate and implement effective law enforcement mechanisms. WHOIS data are used for a variety of law enforcement purposes, such as countering cybersquatting, enforcing intellectual property rights, combating deceptive spam, helping victims of identity theft and enforcing the privacy commitments of companies.[80] Obviously, law enforcement on the Internet requires that illegal activity and the perpetrators

79 See, e.g., the testimony given at the Congressional hearing organized 22.05.2002 on "Accuracy and Integrity of the WHOIS Database"; available at <http://commdocs.house.gov/committees/judiciary/hju79752.000/hju79752_0f.htm>.

80 *Idem*.

of that activity be quickly identified; it also requires an ability to quickly collate information about international entities and organizations. As one actor has stated, "[a]ccurate WHOIS data is essential to these efforts, and inaccurate data can significantly frustrate them".[81] However, even the patterns used by the perpetrators in providing false data can also serve as evidence during investigations.

The main requirements for a reliable use of WHOIS data for law enforcement purposes are:

1. WHOIS data should be accurate;
2. law enforcement authorities, as defined/recognised by national laws or international agreements, must be granted full access to the data records in the scope of the enforcement actions;
3. international enforcement initiatives across TLDs should be supported through both policies and technical mechanisms.

2.2.4 Accuracy: a prerequisite for effectiveness of WHOIS databases

Both the Registrar Accreditation Agreement (RAA) and the Registry Agreement set explicit requirements for providing correct WHOIS data and for maintaining their accuracy in updated form. Similarly, at ccTLD level, the domain name policies stipulate obligations for the registrants, the registrars and the national registry (as owner of the WHOIS database) to guarantee that WHOIS data are accurate. This section shows, nevertheless, that the current contractual provisions aimed at guaranteeing the accuracy of WHOIS data are insufficient, since they provide little practical guidance on the measures to be applied, little incentive to the responsible actor for compliance and few guarantees of enforcement.

Inaccurate WHOIS records can be the result of input errors made in good faith. This is the case, for example, when the language of the registration forms is not adequately understood by the registrants, or when the user fails to notify changes in the contact information provided, resulting in outdated WHOIS records. In such cases, notifying the registrant about unintentional errors may suffice in restoring the accuracy of WHOIS records.

However, inaccurate records may also be the result of deliberate action on the part of a registrant who wishes to disguise or conceal their identity, whether out of concern for data protection practices of the registrar, or out of bad faith and intended concealment of identity associated with illegal activities

81 Testimony of Howard Beales, Director of the Bureau of Consumer Protection at the US Federal Trade Commission, *idem*.

through the registered domain. In the latter case, effective enforcement actions are a must.

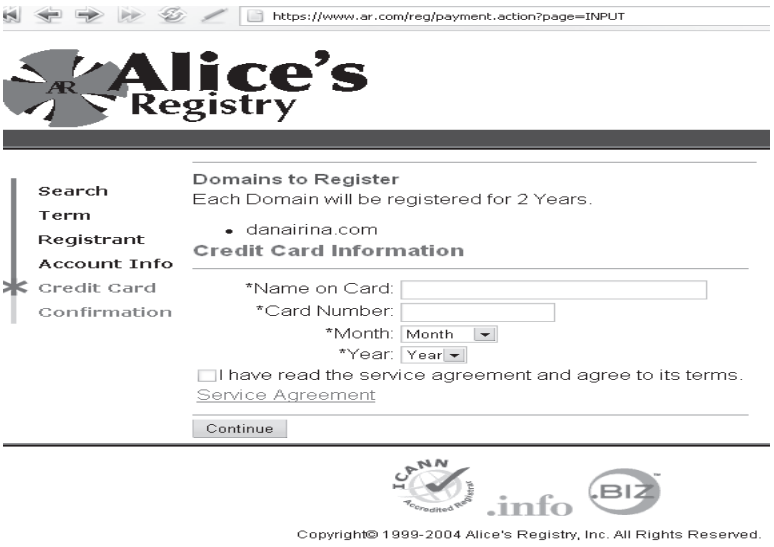
2.2.4.1 Obligations of registrants

Registrants are required by the Registration (Service) Agreement entered into with the chosen registrar, to provide accurate WHOIS data. Through the RAA, the registrars are in their turn under obligation to require the registrants to provide "… accurate and reliable contact details and update them during the term of the Registered name registration …" (section 3.7.7.1). Furthermore, the wilful provision of inaccurate or unreliable information, as well as the wilful failure to promptly update the information provided to the registrar, or failure to respond within 15 days to inquiries by the registrar concerning the accuracy of contact details, shall constitute material breach of the Registration Agreement and be grounds for cancellation of the name registration (section 3.7.7.2). A natural person registrant may, however, reserve the right to opt out of having their personal records included in Bulk Access Agreements for marketing purposes (section 3.3.6.6).

Despite the above-mentioned requirements, provision of accurate and reliable contact data is, in practice, not always an operational prerequisite for registration – as evidenced further below. Despite the technical possibility to crosscheck the data provided upon registration with the credit card records used for payment, and despite the fact that automated systems are capable of crosschecking a registrant's name, address, and postal code using only publicly available databases, these crosschecking methods are not often used. Moreover, even if the registrant provided accurate contact details upon registration, they have the possibility of modifying them subsequently and of disguising their identity before engaging in unlawful activities.

In order to verify the time and manner in which a registrant encounters the terms and conditions of their registration agreement, I made an attempt (at the beginning of November 2007) to register the domain name <www.danairina.com> by randomly choosing Alice's Registry, Inc. as registrar. After filling in blatantly false contact data, I was directed to the payment section in the registration process where I would only have to tick an "I agree" button as well as the payment information and have the domain registered to me. In such a situation, it is very likely that registrants are little aware of the obligation to provide accurate registration information. Even were curiosity to lead a registrant to read through the Registration Agreement, the requirements regarding

WHOIS data only appear in section 12 and are therefore easily missed, even in good faith.[82]



The current system provides to the registrants little incentive for compliance. Once payment has been made, the domain name is registered without any further checks on the accuracy of the contact details provided. More generally, despite bearing the primary responsibility for providing complete and accurate WHOIS data, the registrant is currently not required to bear the costs of non-compliance other than in exceptional circumstances under which the registration is cancelled and the domain is lost. This point is elaborated in the following.

Under the provisions of the "WHOIS Data Reminder Policy" (adopted by ICANN as consensus policy 27.03.2003),[83] the registrant shall be presented "at least annually" with WHOIS information held by the registrar to date and with a reminder that the provision of false WHOIS data "can be" grounds for cancellation of their domain name registration. Yet while the registrar has the right to cancel a registration for material breach of the service agreement, it is apparently not required to make use of that right. Since enforcement actions tend to consume resources, the registrar will often have little incentive to initiate them. In addition, the registrars are not provided with substantial guidance

82 The Registration Agreement of Alice's Registry Inc. is available at <http://alices-registry.com/ra.jspa>.

83 The policy is available at <http://www.icann.org/en/registrars/wdrp.htm>.

as to how to establish bad faith on the part of the registrant or as to how to address complaints about inaccurate WHOIS data.

Section 3.7.8 of the RAA stipulates that:

> *"Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy."*

There is currently no authoritative guidance as to what "reasonable steps" shall denote. The Final Report of the GNSO's WHOIS Task Force on WHOIS data accuracy and bulk access contained a recommendation on the procedure to be followed in handling accuracy complaints but this recommendation has not been adopted as Consensus Policy by the ICANN Board.[84] The recommended procedure is arguably so cumbersome and time-consuming that, if followed to the letter, it effectively gives the registrant in bad faith several other options aside from actually supplying the correct data. According to the recommded procedure, upon receiving a complaint about WHOIS accuracy, the registrar may first seek evidence or justification from the complainant. Subsequently, the registrar should attempt to contact the domain name registrant by using all of their contact points as provided in the WHOIS database (information which could be false anyway). This initial contact, even if it succeeds, will only inform the registrant about the complaint and request the information be updated, with a reminder that the registrant risks having the domain cancelled if compliance is not forthcoming. If a response is received, the registrar is supposed to take "commercially reasonable steps to check whether the information is plausible". The standard of "plausible" (likely) would seem to be lower than the standard of "accurate" (exact); therefore, the registrant in bad faith is given yet another opportunity to conceal their true identity by providing a new set of "plausible" albeit "inaccurate" data. The provision of a real address, but without a link to the registrant or registrant's activity fulfils the criterion of "plausible", but not "accurate" information. Documentary evidence attesting to the accuracy of the data provided is required only if the registrar considers the data implausible. During all this time, the domain name would continue to be functional and the registrant would be able to continue activity under the domain.

The recommended procedure stipulates further that if no response is received from the registrant following the first notification from the registrar,

84 The report is referenced *supra* note 52. The recommended procedure is set out in section II(1)(b) of the report.

the domain is then to be placed ON HOLD or equivalent status until updated information is provided by the registrant. As noted above, that updated information would not necessarily be accurate. According to the recommended procedure, for a domain to be taken off the ON HOLD status, the registrar must be able to confirm that the registrant is contactable via the new information submitted. The check is performed most likely by sending an automatic message requesting a reply to confirm that the address is valid, and is thus inadequate. It does not guarantee that the e-mail address was not set up with false data for the sole purpose of responding to the check and subsequently abandoned. Moreover, the fact that the registrant is reachable via e-mail, does not mean that the rest of the registration data provided are correct.

Another possible problem concerns the situation where a registrant has registered several or more domain names. Multiple registrations are quite common and present particular difficulties when the registrant intentionally provides invalid WHOIS data.[85] If a complaint is mounted about the (in)accuracy of WHOIS data for one of the registered names and the registrant finds that the data are indeed inaccurate, it is not entirely clear if the registrar must then take the initiative to extend its investigations to other names registered by the registrant in question and check whether the WHOIS data provided for those names are correct. Arguably, the "reasonable steps" criterion in section 3.7.8 of the RAA does require such an extension in the registrar's investigatory efforts but the requirement ought to be spelled out more clearly. Further, it would be useful to registrars if "best practices" in terms of reasonable efforts to address complaints about inaccurate WHOIS data were compiled and made available to all registrars.

The ccTLDs which are the focus of this research have adopted the "thick model" for registration and therefore the registry provides a single centralised WHOIS database for the respective domain name. Still, the above-identified shortcomings of a voluntary accuracy compliance policy, coupled with loose enforcement requirements imposed on the registrars, are largely as applicable to ccTLDs as they are to gTLDs.

The Domain Name Policy for .no states:[86]

85 See, e.g., the results of an investigation by Benjamin Edelman published in 2002 (Edelman was then a research fellow at Harvard Law School's Berkman Center for Internet & Society) which revealed that a firm calling itself "NicGod Productions" operated at least 2754 domain names that most often redirect(ed) the user to a page offering a list of links not related to the requested domain. See "Large-Scale International Invalid WHOIS Data: A Case Study of 'NicGod Productions' / 'Domains for sale'" (02.06.2002) at <http://cyber.law.harvard.edu/archived_content/people/edelman/invalid-whois/>.

86 Available at < http://www.norid.no/navnepolitikk.en.html>.

> *"Before submitting an application, applicants must familiarize themselves with the domain name policy and ensure that registration of the domain name does not violate Norwegian law or the rights of third parties, and does not create an unwarranted impression of being associated with public-sector administration or the exercise of public powers. Norid does not undertake any checking of this. The applicant bears the sole responsibility, including criminal liability and liability for damages, for consequences of the registration and use of the domain name" (section 14.1).*[87]

The applicant for registration must provide correct information, both at the time of application and for as long as the registration is maintained and must keep the registered information (both contact and technical information) up to date at all times (sections 14.3 and 14.4). Additionally, section 14.5 of the Policy stipulates that the applicant must reply to queries from Norid regarding the continued accuracy of the registered information. The applicant must then document directly to the registry the information provided (rather than leaving it up to the registrar to request such evidentiary documentation). In this manner, incidence of blatantly false data can be reduced.

The .no system of encoding each set of information provided upon registration into Norid's ID Handles, makes it possible to detect immediately, with relatively little investment of resources, when a given set of data appears in more than one registered domain name. It is therefore to be expected that once a complaint is received, the investigation will be extended to all other domain names displaying the same ID Handle.

If the applicant or the party acting on their behalf provides incorrect information upon registration they risk the sanction of compulsory deletion of the domain name (not merely having the domain placed "on hold")(section 11.1(b) of the Policy). Lack of a signed declaration form is regarded as well as provision of incorrect information. Quite fairly, the holder of the domain name is given an opportunity to respond to the allegation before the domain is deleted. Deletion of the domain name may also occur in the event that the holder of the domain name is no longer registered in Norway's Central Coordinating Register for Legal Entities, or has ceased to exist (section 11.1(c) of the Policy).

87 Note too that the .no registrant must make a self-declaration ("egenerklæring") acknowledging that the registration (i) is in conformity with Norwegian and international law as well as with the Domain Name Policy for .no, (ii) is not (to the best of the registrant's knowledge) an infringement to the rights of a third party, whether registered or not, and (iii) does not convey the appearance that it concerns the exercise of a public function or authority. See section 14.6 (and Appendix G) of the Policy.

In 2006, Norid (the registry for the .no domain) undertook a check of the national Whois database with the view of eliminating false, inaccurate or out-of-date data records. The main focus was placed on domains of registrants which, according to Norway's Central Coordinating Register for Legal Entities, had ceased to exist or had changed owner. A total of 14208 domain names were affected by this "wash" of the database. The registry sent between May- June 2006 a total of 9159 e-mails to the registered contact points for these domain names. Sixty three percent of these emails resulted in error messages and 190 replies were received. During the winter of 2006/2007 the registry attempted to contact the domain name owners via e-mail and traditional letter to one of the addresses registered in the Whois database. Seventy percent of the emails resulted in error messages and 43% of the letters were returned to the sender. The registry received about 700 emails, 30 faxes and letters and about 300 telephone calls from domain name owners updating the domain or asking for some more time to provide the updates. As of 1st June 2007, only 25 of the initial 14208 domains remained in the Whois database. However, the registry realised by that time that hundreds of other legal entities had ceased to exist or had changed owner in the meantime.

The above example shows that striving towards a high degree of accuracy of a WHOIS database is by no means easy. The example also illustrates that the "ex-post" measures are only partially successful and require significant resources. Additional research is necessary in order to assess whether "ex ante" controls of the data provided upon registration, doubled by automatic update messages from the Central Coordinating Register for Legal Entities would result in a higher degree of accuracy of the records in the database.

2.2.4.2 Obligations of TLD registrars

In accordance with section 3.3.1 of the RAA, the gTLD accredited registrars must provide "at their expense" an interactive web page and a port 43 WHOIS service allowing "free, public, query based access to up-to-date data including all active registered names sponsored by the registrar". Sections 3.3.1.1–3.3.1.8 of the RAA specify the information that registrars should collect from registrants for the purpose of making it freely available. As noted, to access the WHOIS database is free of charge. Consequently, the registrars support the costs of any implementation of WHOIS service as well as the costs of any implemented policies for the WHOIS database. In the interest of maintaining a competitive business they must transfer the incurred costs to the registrants, and their revenues are dependent on the number of registrants who choose their services over those of competing registrars. The registrar's interest, therefore, is

to provide an attractive service to the registrants, while keeping the costs for the provision of WHOIS service to a minimum.

According to section 3.3.2 of the RAA, the registrar has the duty to promptly update the database as soon as it receives data updates from the registered name holder. The RAA stipulates further that the:

> *"registrar shall not activate any Registered Name unless and until it is satisfied that it has received a reasonable assurance of payment of its registration fee. For this purpose, a charge to a credit card, general commercial terms extended to creditworthy customers, or other mechanism providing a similar level of assurance of payment shall be sufficient" (section 3.7.4).*

Therefore, as a condition for registration, the registrar is not required to actively check whether the data provided by the registrant are complete and accurate, but rather whether the payment is assured.

The responsibility for providing complete and accurate data resides first and foremost with the registrants. The question is: what are the practical obligations of the registrars in ensuring that the WHOIS database contains accurate data about the registrants? Section 3.7.8 in combination with section 3.7.7.2 of the RAA provide that a registrar may consider the cancellation of a domain name in the event the Registered Name Holder wilfully provides inaccurate or unreliable information, wilfully fails to promptly update the information provided to the registrar, or fails to respond within fifteen calendar days to inquiries from the registrar concerning the accuracy of contact details provided. These three circumstances "shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for cancellation of the Registered Name registration" (section 3.7.7.2). Arguably, this formulation allows the registrar to choose to react to the breach in a manner that does not entail cancellation of the domain name.

The registrars are only expected to make a minimal effort to ensure the accuracy of the WHOIS database. They are to apply, in accordance with section 3.7.8 of the RAA, "reasonable and commercially practicable (a) verification, at the time of registration, of contact information associated with a Registered Name sponsored by Registrar or (b) periodic re-verification of such information". Further, as already noted, the registrar "shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by registrar, take reasonable steps to investigate that claimed inaccuracy. In the event the registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy". The language of these provisions is very loose and devoid of any best practice guidance for the registrars; the latter

have a great deal of discretion in terms of measures to be applied in investigating accuracy complaints.

As pointed out above, the WHOIS Data Reminder Policy (WDRP) issued by ICANN in 2003 introduced a requirement for the registrar to provide the registrant at least once a year with the current WHOIS information, and to remind the registrant that provision of false WHOIS information may be grounds for cancellation of their domain name registration. Registrants must review their WHOIS data, and make any corrections. The WDRP Notice can be presented via web, fax, postal mail, e-mail, or other appropriate means, but the registrant is not required to acknowledge receipt. Silence on the part of the registrant may therefore be interpreted, in this case, not necessarily in the sense of Section 3.7.8 of the RAA (failure to respond) but as a reconfirmation of existing data.[88]

The vote of the ICANN Board in favour of the adoption of this reminder policy was based on the conclusions of the "Final Report of the GNSO Council's WHOIS Task Force on WHOIS Data Accuracy and Bulk Access".[89] However, by looking at the interim version of that report, which was submitted for public comment in 2002,[90] it becomes apparent that the Task Force failed to reach consensus on stricter requirements for intervention from the registrars, together with sanctions for noncompliance.

The Interim Report points out several shortcomings of the existing accuracy mechanisms. These shortcomings still remain at the time of the writing of this study report. One shortcoming is that the registrars may only be penalised for a breach of contract by a revocation of the domain name. This all-or-nothing system may actually impede enforcement, especially since registrars have not established clear enforcement mechanisms to ensure that their customers (resellers, ISPs or end-users) provide accurate data. In the words of the Interim Report:

> *"The Task Force believes that a method of graduated sanctions or enforcements against parties who breach the requirement to provide accurate information and to maintain an accurate WHOIS database, potentially as a combination of policy and financial penalties, should be considered, in order to facilitate the actual enforcement of the current policy with respect to WHOIS data accuracy".*

88 See model WDPR notice "If your review indicates that all of the information above is accurate, you do not need to take any action".

89 Referenced *supra* note 52.

90 Interim Report of the Names Council's WHOIS Task Force (14.10.2002), available at <http://www.dnso.org/dnso/notes/20021015.NCWhoisTF-interim-report.html>.

Further:

> *"ICANN should instruct registrars to use commonly available automated mechanisms to screen out obviously incorrect contact data (e.g., ZIP code/ postcode matching software [at least for North American registrants], rejecting incomplete fields in contact data"*.

Another shortcoming is that there is currently no agreement on the criteria to be considered by the registrar when examining whether the inaccuracy is due to a mistake or to a wilful act. The Interim Report suggested that this breach can be detected on the face of the data submitted if it is blatantly false as it is extremely unlikely that someone would submit such contact data other than wilfully. The Report went on to suggest that wilful breach of contract should lead to cancellation of the registration unless there are extenuating circumstances. Moreover,

> *"in these circumstances there is no need to attempt to contact the registrant before cancellation, and no need to wait 15 days for a reply. Once this wilful conduct is brought to the attention of registrars, the registration should be subject to cancellation"*.

Allowing the registrants a 15 days period for reply to WHOIS accuracy queries from the registrars, at the end of which the only check to be done by the registrar is whether the data are accurate, as currently required, is insufficient. The Interim Report proposed that

> *"the response be accompanied by documentary proof of the accuracy of the 'corrected' data submitted. A response lacking such documentation can be treated as a failure to respond and thus could constitute grounds for cancellation of the domain name registration"*.

Under the current system, it is at least arguable that registrars are not required to investigate all registrations that contain contact data identical to the data reported/documented as inaccurate. According to the Interim Report, registrars should be instructed

> *"to treat a complaint about false WHOIS data in any one registration as a complaint about false WHOIS data in all registrations containing identical contact data, and all such registrations should be made the subject of inquiry, corrected, or cancelled, as the case may be, en bloc"*.

Registrars faced with intentional registrations of false data, are advised in the Interim Report to immediately cancel the Domain Name Registration subject to a Redemption Grace Period, but requiring submission of verified contact data for redemption. The Final Report of the Task Force maintained the idea that a domain name registered with false data should be removed from the zone file with a possibility that the domain be re-included during the Redemption period subject to the submission of accurate and verified contact information. However, following the opinion of the Implementation Committee, this requirement was limited to the maintaining of the respective domain in the zone file "On Hold" Status, until the provision of "updated and accurate" data. Since the requirement for verification was not implemented, it may be concluded that updated data are to be presumed accurate until a new complaint is made. Although this provides an easy solution for the registrar, the presumption is unlikely to be effective in increasing the accuracy of WHOIS data.

In addition, it is unclear how the registrar should react in the case of partial inaccuracy of WHOIS data, for example if the registrar is able to contact the Domain Name Holder (legal person) via one of the e-mail addresses provided, but the rest of the WHOIS records for that entity (name, addresses, telephone numbers) are false, and in addition, illegal activities are carried out under the domain name.[91]

It is arguable that under the current discretionary enforcement of the accuracy requirement, the registrars have an incentive to interpret in a more rigorous way the minimal standards required by the relevant provisions of the RAAs. The costs of the inaccurate data are not borne by the registrars, but by the relevant stakeholder, be it law enforcement agency, cybersquatting victim, consumer or trademark owner. On the other hand, rigorous implementation translates into additional costs for the registrars. If they cannot transfer the costs of the accuracy investigation efforts onto the offending registrant or onto the complainant, they will be encouraged to keep these costs to a minimum. Moreover, given the competition between the registrars, a stricter registrar will face the risk of losing future income from the registrant that it was obligated to exclude, and without the possibility to compensate this material loss through an increase in its reputation. ICANN rarely applies sanctions to the registrars that routinely ignore reports of inaccurate or incomplete data, and at the same time ICANN does not commend registrars with "high enforcement rates".

91 Note, e.g., the difficulties faced by OECD in recovering the domain name <ocde.org> from a cybersquatter, as reported in "Cybersquatting: The OECD's Experience and the Problem it Illustrates with Registrar Practices and WHOIS System" (2002), available at <http://www.oecd.org/dataoecd/46/53/2074621.pdf>.

The shortcomings identified above are applicable to the two ccTLD domain names which are the focus of this study, with one major difference. The difference is that, operating under a thick registration system, the main interest and responsibility in ensuring the quality of the data in WHOIS database rests with the designated registry for the domain, rather than with multiple registrars.

In .no, despite being the owner of the WHOIS database and holder of intellectual property rights in it, Norid (the registry) waives all responsibility to check the accuracy of the information provided by the registrant upon registration.[92] Very little information is available on the actual division of responsibilities among the registrars accredited for the .no domain and Norid in ensuring the accuracy of the WHOIS database, as well as on the enforcement standards and mechanisms of such provisions. Moreover, it would be relevant for Norid to provide more information regarding the extent to which the existing accuracy requirements are upheld and what criteria are used for evaluating that the existing framework is adequate and sufficient to ensure a high degree of accuracy in the WHOIS database.

According to the Registrar Agreement for .no,[93] the registrars have duties to inform the applicant about the applicant's duties under the regulations, and emphasize that the applicant has independent duties in relation to Norid, including the duty to keep contact information up-to-date. Further, the registrars must check whether the applicant is represented by the person who has contacted the registrar, and that this contact person has the necessary authorizations. This is one obligation that the gTLD registrars do not have, and it ensures that the correspondence between the identity of the applicant and the legal person on behalf of whom the name is registered, is accurate.

Another check to be done by the registrar concerns the correctness of the application to be filled in, and that the applicant has acknowledged his duties by filling inn correctly and signing a copy of the applicable declaration form. On this point, it is unclear whether the registrars are required by Norid to check whether the contact information provided by the registrant is accurate at the moment of registration (i.e. if the information belongs to the registrant) or the correctness check refers only to the technical steps leading to the filling inn of the application form.

The registrar is also obliged to receive and forward to Norid details about changes to information registered regarding the domains for which the registrar holds registrar responsibility. The registrar is also obliged to ascertain that the notifications come from a person who represents the subscriber, and that this contact person has the necessary authorisations. Again, it is unclear if any

92 Domain Name Policy for .no, section 14.1.

93 Available at <http://www.norid.no/registrar/regavtale.en.html>.

accuracy check is to be made by the registrar prior to the forwarding of the data to the registry. If the registrars do not have such responsibility, according to the Registrar Agreement for .no, and the registry waives liability as well, then the risks and the detrimental effects of an inaccurate WHOIS record will impact on the stakeholders and the general Internet community rather than on the entities that in fact would have the policy-making competence, the necessary information and the enforcement mechanisms.

The Registrar Agreement states further that Norid may reject a correctly filled-in application to register a domain name or a correctly filled-in notification regarding a change of details. Norid shall inform the registrar of the rejection through electronic notification and state the reason for this. It is unclear whether an assessment of the accuracy of the data provided could be involved in the decision to reject a correctly filled in application form and, if the answer is affirmative, what criteria and/or procedures are in place for the applicant to correct the inaccuracy.

The Agreement also stipulates that "Norid does not become involved in the relationship between registrar and applicant/subscriber beyond what is explicitly stated in this contract" (paragraph 5). Thus, it would seem that the interested party should direct complaints about the accuracy of WHOIS data to the registrars rather than to the registry. However, since the registrar has no express obligation to investigate such claims, nor a direct interest in the WHOIS database, it is unclear who a third party might rely on for taking direct measures against bad faith registrants.

According to the .eu WHOIS Domain Name Policy, which is a self-regulatory policy document issued by EURid, the latter (as registry for .eu) collects one set of personal information from the registrant (full name, technical contact name, postal address, e-mail address and telephone number) for its internal database, while making the rest available through a WHOIS lookup facility. Section 1.2 of the Policy states that the information provided must belong the registrant. However, it is uncertain, based on the documents made available on the registry's website, what the minimal checks to be made are and which evidentiary documents are to be provided by the applicant. Section 2.1 stipulates that "if the registry is holding false, incorrect or outdated information, the registrant will not be contactable and may lose the name". The wording of section 2.1 would lead one to the conclusion that the accuracy requirement, absolute at the gTLD level, translates at .eu level into mere availability and contactability. Thus, submission of inaccurate data would not constitute in itself a breach of contract as long as contact with the registrant can be established through at least one of the types of contact information provided. This conclusion is supported as well by the definition EURid gives of the purpose of WHOIS: to give information about the administrative and the technical contact administering

the domain name. The conclusion is contradicted, however, by the subsequent statement in section 2.1 that "[b]y deliberately submitting inaccurate information, the registrant would also be in breach of the Terms and Conditions which could also lead to loss of the Domain Name".

Similar to the situation analysed for the .com and .no domains, the main responsibility for the submission of accurate contact data is borne by the registrant, who could (rather than will) face the sanction of losing the domain name in case they wilfully provide inaccurate data.

The sanction of revocation of the domain name is to be applied, however, by the registry and not by the registrars. Articles 20 and 21 of Commission Regulation (EC) No. 874/2004 provide the legal basis for the application of this sanction (revocation) when, *inter alia*:

1. the holder is in breach of the terms of registration under Article 3 (including that to the best of the knowledge of the registrant, the registration is made in good faith and does not infringe any rights of a third party). In the case of breach, the registry may revoke a domain name at its own initiative and without submitting the dispute to any extra-judicial settlement of conflicts;
2. the holder has registered the domain name without rights or without legitimate interest in the name or has registered or subsequently used the domain in bad faith. In case of such speculative or abusive registration, the domain name shall be subject to revocation, using an appropriate extra-judicial or judicial procedure.

Based on Articles 20 and 21, it may be concluded that the registry may apply its own judgement and its procedures only when it assesses the position of the registrant during the application for registration. Subsequent intervention, conditional on the abusive use of the domain name, must be dictated by the appropriate extra-judicial or judicial enforcement body.

According to Article 3 of the Regulation, the registry is expected to verify the validity of the applications for registration, only subsequent to the registration either of its own initiative, or pursuant to a dispute for the registration of the domain name in question.

At the moment of registration (submission of the application), all necessary checks should be made by the accredited registrars. In particular, the registrars have an obligation to require all applicants to submit accurate and reliable contact details of at least one natural or legal person responsible for the technical operation of the domain name that is requested (Article 5). Moreover, under a Code of Conduct to which they can voluntarily subscribem, registrars are to ensure, *inter alia*, that (i) the registration details are those of the original

requestor of the domain name; (ii) the country code used during registration is the correct one and is a true reflection of the residential (physical) address of the registrant.[94]

The above-described rules apply for the registration of domain names during the general phase of registration of .eu domain names. However, holders of prior rights recognised or established by national and/or Community law and public bodies were eligible to apply to register domain names during a period of phased registration before general registration of. eu domain started (see Article 10(1)). The data provided during the phased application had to be attested by written documentation proving the existence of prior rights in the domain. According to Article 14, "all claims for prior rights … must be verifiable by documentary evidence which demonstrates the right under the law by virtue of which it exists" and were to be submitted directly to EURid and validated by a designated validation agent rather than a registrar (Articles 13–14). Among the evidence that EURid was to consider as attesting prior rights in the domain name, was reference to the legal basis in national or Community law for the right to the name, and other relevant information, such as trademark registration number, information concerning publication in an official journal or government gazette, registration information at professional or business associations and chambers of commerce (Article 12(3)).
The information made available by EURid does not, however, clarify how the accuracy of the data submitted by the registrants of domain names after the phased registration must be ensured.

2.2.4.3 Enforcement of accuracy requirement

Better assurance of the accuracy of WHOIS databases would require at least the following set of measures:

1. Clear guidance from the policy-making authority in the respective TLD as to the expected activities to be taken in order to certify in a concrete case the "willingness to provide inaccurate data", "material breach", as well as how to deal with "partially inaccurate WHOIS records";
2. Restoring the cost-benefit balance by placing the cost burden for non-compliance with the entity best able to combat the non-compliance. At the present time, the registrars are unable to claim the costs of enforcement from the registrant at fault, and they risk little in terms of reputation or revenues by loosely enforcing the RAA terms. In this regard, the Interim

94 See Code of Conduct for EURid Registrars section 2. The Code is available at <http://www.coc.eu/images/Documents/Code_of_Conduct/coc_current.pdf>.

Report of the WHOIS Task Force proposed a three strike gradual enforcement mechanism against non complying registrars.[95] Although consensus

95 The report is referenced *supra* note 90. The proposed three strike procedure is provided below:

(c-1.) Strike One:

The registrar shall be provided thirty calendar days to take necessary action to correct documented inaccuracies in WHOIS data. If, at the expiration of the thirty-day period, the information in WHOIS database has not been corrected, and the registrar does not submit to ICANN evidence of having taken vigorous steps to correct such inaccuracies, the registrar shall be:

a) Provided a notice of non-compliance with ICANN contract regarding WHOIS accuracy

b) Levied a fine of $250 for each instance of non-compliance. The fine would be collected from funds deposited by registrars with registries (ICANN agreements with registries would also have to be revised to authorize this collection). (A collection mechanism would also need to be provided with respect to thick registries.)

c) Asked to provide a plan to ensure correction of accuracy of WHOIS data

d) Given a further thirty days to take action to correct documented inaccuracies in WHOIS data, with penalties for non-compliance as below

(c-2) Strike Two:

The registrar shall be provided a further thirty calendar days to take necessary action to correct documented inaccuracies in WHOIS data. This time period shall commence at the conclusion of the first thirty-day period automatically. If, at the expiration of the thirty-day period, the information in WHOIS database has not been corrected, and the registrar does not submit to ICANN evidence of having taken vigorous steps to correct such inaccuracies, the registrar shall be:

a) Provided a second notice of non-compliance with ICANN contract regarding WHOIS accuracy

b) Levied a fine of $500 for each instance of non-compliance.

c) Asked to provide a plan to ensure correction of accuracy of WHOIS data

d) Informed that they have one more opportunity to take steps to correct WHOIS data before more serious action is taken against them for material breach of contract

e) Given a final thirty days to take action to correct documented inaccuracies in WHOIS data, with penalties for non-compliance as below

(c-3) Strike Three:

The registrar shall be provided a further thirty calendar days to take necessary action to correct documented inaccuracies in WHOIS data. This time period shall commence at the conclusion of the first thirty-day period automatically. If, at the expiration of the thirty-day period, the information in WHOIS database has not been corrected, and the registrar does not submit to ICANN evidence of having taken vigorous steps to correct such inaccuracies, the registrar shall be:

a) Provided a third notice of non-compliance with ICANN contract regarding WHOIS accuracy

b) Levied a fine of $1,000 for each instance of non-compliance.

c) The registrar's name shall be placed on a public non-compliance list, prominently displayed on ICANN and other public Internet sites.

d) Asked to provide a plan to ensure correction of accuracy of WHOIS data

e) Informed that under the terms of their RAA, they are in danger of incurring further serious penalties, including, should it be so decided, a suspension of registrar accreditation.

f) Given a final thirty days to take action to correct documented inaccuracies in WHOIS data, with penalties for non-compliance as below

has not been reached at gTLD level in this regard, this model is worth considering in the future for .no;
3. Providing clear mechanisms for the handling of inaccuracy complaints, with feedback mechanisms indicating the registrars who make only limited or insufficient efforts to ensure the accuracy of WHOIS records.

A "WHOIS Data Problem Report System" (WDPRS) has already been implemented by ICANN and put into practice from 2003. This is a system to receive and track complaints about inaccurate or incomplete WHOIS data entries. Individuals who come across inaccurate or incomplete entries in the WHOIS database are able to notify ICANN by completing an online form, which isthen forwarded to the registrar of record for appropriate action.[96] After 45 days, ICANN requests the feedback of the person who filed the report, which involves checking the WHOIS data once again and indicating the practical outcome of the complaint:

- (i) the data were corrected;
- (ii) the domain name was deleted;
- (iii) the data were unchanged; or
- (iv) there is some other disposition.

According to statistics provided by ICANN in April 2007, there were for the period February 2006 to February 2007 50,189 reports for which ICANN received follow-up responses.[97] Of these, 34,029 unique domain names were subject to reports. One individual in that period filed nearly 40% of all reports received. The top 20 contributing individuals accounted for over 83% of the 50,189 reports. The fact that less than 1% of reporters accounted for almost 90% the reports poses an issue for statistical analysis of the data. On a per TLD basis, .com represented 74.43% of confirmed reports (37,357), with .net and .info constituting 13.36% and 8.28% respectively, with an estimated 35% of reported domain names with bad data corrected, suspended, or no longer registered. A further 28% of domains with clearly bad information were not changed, leaving approximately 37% of the reported domains' WHOIS data without obvious errors.

As part of the process for renewing registrar accreditation in 2005, ICANN reviewed each registrar's level of compliance with the WDRP and required

(c-4) **Next Step**: Suspension of accreditation and rights to register new names for 5 days.
(c-5) **Final Step**: Removal of accreditation.

96 See further <http://wdprs.internic.net/>.

97 See *ICANN's Whois Data Accuracy and Availability Program: Description of Prior Efforts and New Compliance Initiatives* (27.04.2007), available at <http://www.icann.org/en/whois/whois-data-accuracy-program-27apr07.pdf>.

the non-compliant registrars to come into compliance before granting them accreditation renewal. ICANN also launched a Data Accuracy Programme in April 2007 involving:

- an annual WHOIS Data Accuracy Audit;
- monitoring of registrars' WHOIS server functionality;
- annual publications of the statistical data gathered via the WDPRS.[98]

Registrars found failing to take action to address complaints submitted via the WHOIS Data Reminder Policy are to be notified of their breach of section 3.7.8 of the RAA (set out above) and receive a 5-day deadline to justify their lack of action. ICANN will take action against them as deemed appropriate in each case and ultimately publish findings at the end of each audit period. Additionally, ICANN has initiated a new registrar WHOIS compliance program that involves both automated and manual auditing of registrars' port 43 WHOIS services to check that these services are both functional and responsive to WHOIS queries in accordance with RAA requirements.[99]

98 *Idem.*
99 *Idem.*

3 LEGAL PROTECTION OF WHOIS DATABASES

According to the Registrar Accreditation Agreement (RAA) and pursuant to the Registry Agreements (RA), the provision of WHOIS service represents an obligation for the registrars (RAA section 3(3)(1)) and the registries (.com RA section 3(1)(c)) at the gTLD level. Registries and registrars are required to set up WHOIS databases and to provide access to them free of charge via the web and via port 43 and remunerated via bulk access agreements[100] with third parties.

The provision of WHOIS service at the level of the two ccTLDs that are the focus of this research (.no and .eu) involves access to the respective centralised WHOIS database owned by the registry concerned. While bulk access to the entirety of the WHOIS database is allowed under the .com domain, this possibility does not exist, for the information collected until this point, under .no or .eu.[101]

This chapter identifies and discusses the scope of the owners' rights in regard to the WHOIS database itself (rather than the rights to the individual records associated with a domain name). The first step is a description of the object of the legal protection, in the light of the criteria stipulated by the applicable law. The second step is an identification of the criteria that are established by law in order to decide whether a database qualifies for the one or the other regimes of protection (copyright or sui-generis database protection right). Thirdly, the scope of the owners' rights in the database as well as the limitations in the exercise of these rights, are analysed.

In Europe, an attempt to harmonise the regime for protection of databases was made through Directive 96/9/EC (hereinafter "Database Directive").[102] Whether the various national implementations of the Directive have achieved the goal of harmonisation is outside the scope of this report. In the following, reference is made to two of the national laws transposing the Directive in the jurisdictions of Norway and Belgium.

The WHOIS database for the .no domain is provided by the registry for the .no domain (Norid) and is governed by Norwegian law. Norway transposed

100 According to the terms of Appendix 3 of the .com registry Agreement

101 However, an interested user can request in writing and obtain from EURid access to unpublished data about the domain name registrants.

102 Directive 96/9/EC of 11.03.1996 on the legal protection of databases (O.J. L 77/20, 27.03.1996, pp. 20–28).

the Database Directive in 1998 by amending the Copyright Act of 1961.[103] It should be noted that, prior to this transposition, the Copyright Act already gave some protection to databases under the so-called "catalogue rule" contained in section 43. This protection extends to catalogues, tables and other collections of information which do not fulfil the criteria for copyright protection but are the product of significant effort. Creating a special regime of protection for non-copyrightable collections of information allowed the Norwegian courts to maintain a narrow interpretation of the criteria for copyright while ensuring protection for the economic interests of the person(s) who invest considerable effort in collecting, arranging or structuring large quantities of information. Thus, transposition of the Database Directive into Norwegian law required only minor changes or reinterpretations of the pre-existing framework, as well as the inclusion of the term "database" in the text of section 43.[104] That framework, as subsequently amended, is a principal legal source of rights and obligations for Norid in managing the WHOIS database. In addition, to the extent that allowance is made for contractual derogations from the legislative regime, references are made in the following to provisions of the agreements entered into by Norid.

The WHOIS database for the .eu domain is provided by the domain name registry for .eu (EURid). The registry is a non-profit organisation established in Belgium and has been selected by the European Commission to operate the .eu domain. The Database Directive was transposed into Belgian law in 1998.[105] Both the copyright regime and the sui generis regime for protection of databases were introduced in Belgian law, with just minor changes from the text of the Directive.

The applicable law for the .com WHOIS databases is more difficult to determine. The difficulties arise first and foremost out of the "thin" WHOIS

103 Act No. 2 of 12.05.1961 relating to copyright in literary, scientific and artistic works (Lov om opphavsrett til åndsverk m.v.) as amended. An unofficial English translation of the Act is available from the website of the Norwegian Ministry of Culture and Church Affairs, at <http://www.regjeringen.no/upload/KKD/Medier/Acts%20and%20regulations/Aandsverkloven_engelsk_versjon_nov2008.pdf>. In the following, quotations (in English) from the Act are based on this translation. The main preparatory work on transposition of the Database Directive is Ot.prp. nr. 85 (1997–98) *Om lov om endringer i åndsverkloven (gjennomføring av EU-direktiv om rettslig vern av databaser)*.

104 See generally Ot.prp. nr. 85 (1997–98) *Om lov om endringer i åndsverkloven (gjennomføring av EU-direktiv om rettslig vern av databaser)*.

105 See Law of 31.08.1998 transposing into Belgian law the European Directive of 11.03.1996 concerning the legal protection of databases" (Loi du 31 août 1998 transposant en droit belge la directive européenne n° 96/9/CE du 11 mars 1996 concernant la protection juridique des base de données), published in *Moniteur belge / Belgisch Staatsblad*, 14.11.1998, p. 36.914.

regime characteristic for the .com gTLD, which involves distributed WHOIS databases across the accredited registrars as well as one centralised WHOIS database at registry level. Each accredited WHOIS registrar is governed by the national law of the country where it is established. At the same time, it has the RAA-imposed obligation to collect registrant data and to provide its own WHOIS database. Additionally, the .com registry provides a centralised WHOIS database for the entire .com domain, including only partial registrant data transferred to it by the registrars, as well as data about the registrar which handled the domain name application on behalf of the registrant. Adding to the complexity is the fact that some cross-registry WHOIS facilities are provided, for example, by Internic or by Verisign, and these entities may also make claims to rights in the database.

A functional view of this layered applicable law situation would require one to consider that each database at registrar level is governed by the national law applicable to the registrar, while the registry-level WHOIS database is governed by the law of the registry. Verisign, the registry for the .com domain, is registered in Virginia, USA; therefore, the law of that jurisdiction would apply. The terms and conditions for access to the WHOIS database of Verisign, as stated on the Verisign website, do not seem to indicate that another law has been contractually designated as being applicable.

According to the Database Directive, a "database" is a "collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means" (Article 1(2)). From this definition, a database (for the purposes of the Directive) must meet the following cumulative criteria.

First, it must constitute a collection of independent works, data or other material. As a "collection", it is (in accordance with Article 2(5) of the 1886 Berne Convention for the Protection of Literary and Artistic Works), a group of selected items viewed as a whole and arranged in a specific way. As for the reference to "independent", this means that the consituents of the database are separable from one other without their informative value being detrimentally affected; they must have "autonomous informative value".[106] This criterion is fulfilled by the WHOIS databases, which include data records on domain name registrants, records that are by nature independent of one other.

Secondly, the data must be arranged in a systematic or methodical way. The added value of the database as a whole is to be found in the relation generated among the individual constituent elements. This relation is expressed both by the organisation and structure of the database and the criteria used for the

106 See decision of European Court of Justice in *Fixtures Marketing v. Organismos Prognostikon Agonon Podosfairu* (Case C-444/02) [2005] ECDR 43, paragraph 33.

selection of its elements. The selection and the arrangement of the independent elements should be the result of a devised plan, rather than a disordered gathering of materials. In other words, arrangement cannot be haphazard.[107] According to some expert commentators, a database on the Internet, despite its contents being distributed among different locations across several computer servers, can probably be regarded as a systematic and methodically arranged whole provided that any part of the contents can be accessed from a single source, such as a specific website.[108] The requirement for a systematic or methodical arrangement of the contents translates into the need for an identifiable unity in the organisation, since stable access to the database falls under the database makers' control and responsibility. This point is especially relevant given the fact that the registry WHOIS database merges registrant data collected from the registrars with information provided by the registrars about themselves. It is likely that the records are not copied to a single location, but that a distributed management of access rights will be in place.

Thirdly, the contents of the database should be individually accessible by electronic or other means. For this condition to be fulfilled it should be possible to find a specific item in a database without having to go through all the contents. The search and find function should be available either directly, or indirectly, via an index, thesaurus or computer programme.[109] The contents of the WHOIS database are accessible individually through electronic means, that is to say via the website of the corresponding registrar (or of the registry) as well as via port 43.

There can be little doubt that WHOIS databases fulfill the three above-described criteria, and that those maintained by European bodies – such as EURid and Norid – come under the national transpositions of the Database Directive. The exact nature of the legal protection afforded to the database maker is dependent, however, on additional criteria. Legal protection can be either by way of copyright or by way of sui generis database protection. Copyright protection is afforded to "databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation" (Database Directive Article 3(1)). *Sui generis* database protection is provided as a recognition of the legitimate economic interests of the maker of a database who has made a "substantial" "qualitative and/or

107 *Id.*, paragraph 30 *et seq*.

108 See, e.g., Annemarie Beunen, *Protection for databases. The European Database Directive and its effects in the Netherlands, France and United Kingdom* (Nijmegen: Wolf Legal Publishers, 2007), p. 52.

109 *Id.*, p. 59.

quantitative investment" in either the "obtaining, verification or presentation of the contents" (Article 7(1)).

The main distinction between the two protection regimes is that the primary objective of copyright is to provide an incentive for further intellectual creations. Copyright is aimed at encouraging others to build upon the information and ideas conveyed by the work while protecting the original added value of the creation. The copyright protection extends only to those aspects that embody and reflect the originality of the creator. The *sui generis* regime, on the other hand, recognises and protects the value of the human, technical and financial investment made by the maker of the database without consideration of whether or not the result was original or innovative.

3.1 Ownership of copyright / sui generis right

In determining whether a WHOIS database is worthy of copyright protection as an intellectual creation or whether its maker is entitled only to the recognition of a legitimate economic interest in protecting the investment, it is necessary to review some of the features of such a database.

A WHOIS database includes data about all the registrants of domain names under a certain TLD. Upon collection of the data, no distinction is made concerning which records will be included or not included in the database. Existing agreements impose the provision of this general service on all accredited registrars. Accurate records of all the registrants are to be maintained. The agreements also mandate the nature of the data to be collected about each registrant; thus, the data collected from registrars are similar regardless of the domain name. No creative selection of the contents occurs.

For the time being, the agreements do not mandate the display of WHOIS records in a standardised format. It is therefore still possible for the providers of WHOIS databases to use a certain degree of creativity as to the search and arrangement criteria of the records in the databases. Whether the degree of creativity in the arrangement of the contents is sufficient to entitle the maker to copyright protection is a matter for a court to assess in any given case. The recent initiatives of ICANN to ensure accuracy of WHOIS data, however, reveal an intention to reduce rather to stimulate the creativity of the database providers and a commitment to finding appropriate standardised solutions at least in making WHOIS data publicly available following individual queries.[110]

110 See announcement of 21.12.2007 at <http://www.icann.org/en/announcements/announcement-2-21dec07.htm>.

Although accurate assessments regarding the amount of "qualitative or quantitative" investments made in obtaining, verifying or presenting the contents of the WHOIS databases would necessitate more extensive studies exceeding the scope and purpose of this report, it may be estimated that such costs cannot be very great for the registries, but may be arguably greater for the individual registrars. The .no registry, for example, receives from the registrars already corrected registration data entered on application forms which they have only to feed into the WHOIS database. A computer-generated ID Handle is assigned to each informational set provided in relation to a certain role. This in itself may have required additional investment. However, according to the Database Directive, "the protection afforded shall not apply to computer programs used in the making or operation of databases accessible through electronic means" (Article 1(3)). It is therefore improbable that this "innovation" alone would qualify the .no WHOIS database for copyright protection.

Given the increasing number of Internet users in each domain,[111] it is nonetheless likely that each WHOIS database includes a substantial number of records.

Considering the specific requirements for affording the one or the other regime of protection to a WHOIS database, as well as the features of the database itself, it is doubtful that the controller of the database may claim a copyright for it. This is first and foremost because there is no original selection of the contents of the database made by the entity claiming copyright protection. None of the registrars or registries can claim that they made a selection concerning which data records were to be included or about which registrant.

Secondly, there is arguably little if any originality of the arrangement of the contents of the databases. The notion of "originality" in relation to the arrangement of a database has been interpreted loosely by courts and no harmonised threshold for originality has been set at European level.[112] The preparatory works for the Norwegian transposition of the Database Directive considered, however, that in highly functional databases where the main purpose is to provide the user with complete information on a certain topic, copyright protection will be seldom available.[113]

111 EURid's quarterly progress report for 2008 states: "Over the past quarter .eu registrations grew by more than 40% in eight countries when compared to the second quarter of 2007. The average growth for the EU as a whole was 15%." See <http://www.eurid.eu/files/Q2_08.pdf>. Similar growth trends are recorded for .no. See <http://www.norid.no/statistikk/domener/>.

112 See Beunen, *Protection for databases*, p. 76 *et seq*.

113 See Ot.prp. nr. 85 (1997–98), p. 13 ("Departementet antar at det ikke vil være vanlig at databaser som sammenstillinger fyller kravene til verkshøyde. For mange databaser vil hovedformålet være å gi brukeren en helt ut dekkende samling av informasjon innen et område.

According to the information displayed as a result of a WHOIS search in the .no WHOIS database, the registry for the .no domain claims their database is "kopibeskyttet", i.e., subject to "copyright".[114] Insofar as this claim is intended to mean that the WHOIS database satisfies the conditions for copyright protection (as opposed to protection under the *sui generis* or catalogue regime), its validity is dubious. It is at least questionable whether the claim would be upheld by a court, especially given the widely inclusive catalogue protection in section 43 of the Copyright Act (elaborated further below).

The .eu registry claims only that:

> *"it is explicitly forbidden to extract, copy and/or use or re-utilise in any form and by any means (electronically or not) the whole or a quantitatively or qualitatively substantial part of the contents of the WHOIS database without prior and explicit permission by EURid, nor in any attempt hereof, to apply automated, electronic processes to EURid (or its systems). You agree that any reproduction and/or transmission of data for commercial purposes will always be considered as the extraction of a substantial part of the content of the WHOIS database."*

The rights claimed by the .eu registry are those guaranteed to a database maker according to the sui generis regime, and no other reference to copyright in databases is made. Similar claims of legitimate interests in the investment made in WHOIS database are made by the registrars accredited under .com.

The US Copyright Act 1976 defines in section 101 the notion of "compilation" by focusing on similar criteria to those used by the Database Directive in defining the notion of "database". In order to assign copyright protection to a compilation, it is necessary that the resulting work as a whole be an original work of authorship. Copyright protection focuses on the original ways in which the pre-existing materials or data were selected, coordinated, arranged, and not on the data as such (see particularly section 103(b)).

The leading case on copyright protection for compilations is the decision of the US Supreme Court in *Feist Publications v. Rural Telephone Service Co.*[115]

Ofte vil da utvelgelseskriteriene i liten grad bære preg av noens individuelle, kreative valg. Det beror på en konkret vurdering om resultatet viser en slik kreativ innsats med hensyn til sammenstillingen at arbeidet må anses å være et åndsverk.").

114 See too English text at <http://www.norid.no/domenenavnbaser/whois/kopirett.en.html> and Norwegian text at <http://www.norid.no/domenenavnbaser/whois/kopirett.html>. See also Norwegian text on "Bruk av informasjon lagret i Norids kundedatabase", at <http://www.norid.no/domenenavnbaser/personvernpolicy.html> where it is stated that the database is "kopibeskyttet".

115 499 U.S. 340 (1991).

Rural Telephone Service (Rural) was denied copyright in a database with clear parallels to a WHOIS database. The database in question was a telephone directory that Rural was required to compile and update under the terms of a license agreement with the state regulator of telecommunication. Rural gathered the information from subscribers as part of the subscription to telephony services process, and as a result had monopoly over the data. The Supreme Court stated that although it acknowledged the possibility of compilations enjoying copyright protection, such protection was not available in this case since: (i) Rural did not choose what facts to include in the database (but acted in accordance with the requirements of the license); (ii) Rural did not make a creative call in deciding the order in which the data should be presented; (iii) the manner of arranging the collected data so that they could be effectively used by those accessing the database was not sufficiently original in the case at hand. The Supreme Court made it clear that a modicum of originality is a *sine qua non* for copyright protection: "copyright protects only those constituent elements of a work that possess more than a de minimis quantum of creativity".[116] The Court in Feist also underscored that copyright protection in a compilation of factual data is very thin. It will not prevent others from using the compiled facts once access has been obtained, as long as the new work does not display the same selection and arrangement features as the one from which it was extracted.[117]

Nonetheless, American database producers may be able to invoke several legal doctrines other than copyright to prevent unauthorized use of their databases. Of central importance is the doctrine of commercial misappropriation, the leading case on which is the decision of the US Supreme Court in *International News Service v. Associated Press*.[118] In that case, the Court held that International News Service was able to prevent a direct competitor from copying and distributing its news content when the competitor did not incur costs in gathering the news and when the competitor's activity "would render publication profitless, or so little profitable as in effect to cut off the service by rendering the cost prohibitive in comparison with the return".[119] The application of the doctrine is often cumbersome due to the cumulative conditions that must be fulfilled. According to Derclaye,[120] database producers can only prevent the copying of databases containing time sensitive information created

116 *Idem*, p. 363.
117 *Idem*, p. 349.
118 248 U.S. 215 (1918).
119 *Idem*, p. 241.
120 Estelle Derclaye, "Intellectual property rights on information and market power – comparing European and American Protection of Databases", *International Review of Industrial Property and Copyright*, 2007, vol. 38, pp. 275–98.

at some cost (investment), and there must be direct competition between the database producer and the one who copied the database. Moreover, free-riding by the defendant must reduce the database producer's incentive to create to such a degree that they would not produce the database, or the quality of the database would be significantly reduced in the absence of a sanction.

Turning back to Europe, it is doubtful that copyright protection is an objective worth pursuing in the case of WHOIS databases. One may question whether copyright for such databases affords a higher degree of protection to the database owner than application of the sui generis/catalogue right, particularly given that the owner cannot claim copyright over the factual content of the database anyway.

3.1.1 Individual queries

When a user makes a query to the WHOIS service, the registration data on one single domain name are displayed. According to the definitions provided by the Database Directive, this process would be an example of "*temporary or permanent reproduction by any means and in any form … in part*" of the contents of a database (Article 3(a); emphasis added) as well as an act of "*permanent or temporary transfer of … parts of the contents of a database to another medium by any means or in any form*" (Article 7(2)(a); emphasis added). Regardless of whether the database is protected by copyright or the database maker is afforded a sui-generis database right, the rights holder has an exclusive right to carry out or to authorise both acts of reproduction and the acts of extraction.

The lawful user of the database protected by copyright can, however, perform such acts of permanent or temporary reproduction if they are necessary for the purposes of *access* to the contents of the database and normal use of its contents. Moreover, lawful users may perform similar acts without authorisation, for the *purposes of public security or in the context of an administrative or judicial procedure* (Article 6(1)).

If a *sui generis* right alone is held by the maker of the database, a lawful user would still be allowed (with no possibility for stipulation to the contrary) to extract and to reutilise *insubstantial* parts of the database contents, *for any purposes whatsoever*, as long as such acts do not conflict with the normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database (Article 8(1)). However, repeated and systematic extraction and/or reutilisation of insubstantial parts of the contents is prohibited if the cumulative effect of such insubstantial intervention conflicts with the normal exploitation of the database or prejudices the legitimate interests of the maker of the database (Article 8(2); cf. Article 8(3)).

It is thus apparent that both regimes – copyright and sui generis right – allow legitimate users to perform certain acts without the express authorisation of the rightsholder. However, the Directive (as well as its various implementations) does not define what a legitimate user is. It is up to the rightsholders themselves to define the scope of legitimate use, either by defining permitted uses (functional criteria) or by defining authorised categories of users (role-based criteria).

The scope of the legitimate use of WHOIS databases has been defined in the Internet community to some extent, although consensus has yet to be reached. Therefore an interested party may use the functional criteria in order to determine with relative certainty whether a requestor should be regarded as a "legitimate user".

Direct and free access to individual public WHOIS records for any Internet user is mandated by the contractual agreements in force in the current WHOIS regime. Moreover, the accredited registrars in the .com domain cannot impose more restrictive conditions of access than those set down in the Consensus Policies mandated by ICANN.[121] It would therefore seem reasonable to conclude that the creation of a role-based access control mechanism, through which determined roles have access in varying degrees of detail to the contents of the WHOIS database, would only be possible if stipulated by a new WHOIS policy approved by ICANN for gTLDs. The use of a role-based criterion for determining whether a user is legitimate would involve major transformations in WHOIS policy for the gTLD and require the consensus of the international Internet community.

As long as the current WHOIS regime at gTLD level does not accommodate a role-based access mechanism which would subject the legitimacy of an access request to the role-dependent identity of a user, the rightsholders can arguably only define legitimate use by limiting the purposes for which access is granted.

In the light of the above considerations, legitimate use may be defined as the use of WHOIS records for the purposes indicated (allowed) by the rightsholder or in accordance with the imperative legal provisions.

It can, of course, be questioned to what extent access to individual records associated with a certain domain name qualifies as access to a "substantial" or an "insubstantial" part of the WHOIS database, for the purposes of the Database Directive. The main criterion in organising WHOIS data is the connection to one certain domain name. The information associated with one domain can be plausibly regarded as one single record in the database. As such, access to information about one domain name can be reasonably regarded as

121 Section 3.3.5 of the Registrar Accreditation Agreement.

access to an insubstantial part of a database, and therefore does not require the special authorisation of the database owner.

3.1.2 Multiple queries

In accordance with the Database Directive, the rightsholder may limit the access to the database when the provision of such access would involve a significant extraction or reutilisation of the contents of the database. This requirement is reflected in the WHOIS policy framework by the registrar's obligation to enter into written bulk-access agreements with third parties expressing the terms and conditions under which the whole WHOIS database may be released. Additionally, the bulk-access agreements should stipulate specific guarantees that the legitimate rights of either the registrar or the registrants will not be disregarded.[122]

A significant extraction or reutilisation may be the result of one single access (by virtue of a bulk-access agreement, where permitted) or the result of repeated and systematic access to individual records.

The burden of proof that the individual acts of extraction of insubstantial parts of the database amount to a substantial extraction is done through a case-by-case assessment by the database maker. In practice, the rightsholders have put in place mechanisms to restrict the maximum number of queries that can be sent repeatedly from a certain location during a certain interval of time. Although the restriction is mainly justified by the technical limitations of the network, it can also be argued that the rightsholder considers the cumulative effect of individual queries beyond this maximum threshold of queries to be detrimental to the normal exploitation of the database.

3.2 Limitations in the exercise of the database rights

The maker of the database is granted, according to the Database Directive, the right to prevent the extraction and/or reutilisation of a whole or a significant part of the database (Article 7). Additionally, they may decide whether or not to make the database public, the conditions under which access to the information is allowed, as well as when and how information is updated.

WHOIS databases which are created and maintained by the registrars and registries as vital components in the provision of the WHOIS service, afford

122 The terms of the Zone File Access Agreement (01.03.2006) can be consulted via <http://www.icann.org/en/tlds/agreements/verisign/appendix-03-01mar06.htm>.

the database makers the exercise of a more limited range of rights. In addition to the statutory limitations stipulated by the national laws transposing the Database Directive, supplementary limitations are imposed on the database makers via the contractual agreements entered into for the provision of the WHOIS service.

3.2.1 Statutory limitations of WHOIS database makers' rights

As the registry for the .no domain, Norid manages the registration of domain names under that domain and decides the conditions of access to and use of the .no WHOIS database in accordance with the principles set down by the law and the interests of the Norwegian Internet community.

An individual user querying the WHOIS database for .no is faced with the following claim:

> *"Except for use which falls under the intended use of the database or with written permission from Norid, it is forbidden to copy or imitate in any other way, store, download or transfer information or collection of information given in this database. This applies independently of how the information is rendered, stored etc., and independently of whether this is for temporary or permanent storage or use. This also applies independently of whether or not the intention is commercial use. Any commercial use of the registered information, targeted marketing including, is forbidden. Infringement may be in violation of the EU's database directive and Norwegian law concerning the protection of person information. Any violation is at one's own responsibility. Norid will prosecute any illegal rendering, downloading or other type of violation. Norid requests to be informed of violations or suspicion of violations".*[123]

In the following, the validity and enforceability of the above claims are analysed in the light of the provisions of section 43 of the Norwegian Copyright Act (transposing the Database Directive) and in the light of the obligations assumed by Norid as registry for .no ccTLD towards the Norwegian Internet Community. The analysis proceeds on the basis that the .no WHOIS database does not fulfil the conditions for *copyright* protection but falls within the protection offered under section 43. The most important provisions of section 43 in this respect are contained in paragraphs 1 and 2, which provide:

123 See <http://www.norid.no/domenenavnbaser/whois/kopirett.en.html>. This is a direct translation from the Norwegian text at <http://www.norid.no/domenenavnbaser/whois/kopirett.html>. The Norwegian text is expressed as having precedence over the equivalent English text in the event of conflict between the two. As far as I can see, though, the translation is accurate.

> *"A person who produces a formula, catalogue, table, program, database or a similar work in which a large number of items of information has been compiled, or which is the result of a substantial investment, shall have the exclusive right to dispose of all or a substantial part of the contents of the work through the producing of copies thereof or through making it available to the public.*

The exclusive right under the preceding paragraph applies correspondingly when insubstantial parts of works as mentioned, are repeatedly and systematically reproduced or made available to the public, if this constitutes acts conflicting with a normal exploitation of the work or which unreasonably prejudices the producer's legitimate interests."

As legal entity taking the initiative and bearing the risks of the investment in the WHOIS database, Norid has (following the wording of section 43 above) the exclusive right of disposition over the entirety or substantial parts of the contents of the database, by producing it and making it available to the public. Norid's exclusive rights over the WHOIS database therefore pertain to the database itself (or substantial parts of it), and not the information contained in it. By virtue of the specific object and scope of protection (*sui generis* database rights), the authorisation of the rightsholder is only required when the act of disposition (reproduction, copying, adaptation, distribution to the public), impacts on either the entirety of the database, or a part of it substantial enough to meet the criteria for protection in section 43. Admittedly, in the event an infringement is suspected, an ex post case-by-case assessment should be carried out in order to determine whether or not the act of disposition should have been authorised by Norid. In making such an assessment, one should bear in mind that the database protection afforded by section 43 of the Norwegian law and by the Database Directive, is aimed at safeguarding the database maker against acts of unfair competition and against acts that "unreasonably prejudice the legitimate interests of the database maker or conflict with the normal exploitation of the database".

Whenever access to the database is provided in return for a fee, or the restriction of access is a prerequisite for the maker to capitalise on their investment, it is obvious that the database maker has a legitimate economic interest in the database. However, in its role as ccTLD registry, Norid has an obligation to provide WHOIS service free of charge and to anyone. Despite not having copyright as such over the personal data contained in the database, Norid, as controller of personal data, can be said to have a legitimate interest in protecting the privacy and the personal data of the registrants from being used with disregard for the intended purpose when the information was collected and made available to the public. Given the investment of funds, time and human resources in managing the domain-related information, Norid can also be said

to have a legitimate interest in preventing another from earning unlawful profits through the exploitation of the WHOIS database for commercial purposes.

Norid can also oppose acts of disposition that conflict with the normal exploitation of the database. The scope of the "normal exploitation" of the WHOIS database is derived from the interpretation of the purpose of the WHOIS database. As discussed in Chapter 2, by exemplifying permitted uses rather than defining a more encompassing purpose for providing access to the database, Norid incurs the risk of costly case-by-case assessments and divergent interpretations to the detriment of legal certainty. It also risks restricting a broader range of legitimate uses for the database.

Given the considerations above, Norid's statement that "it is forbidden to copy or imitate in any other way, store, download or transfer information or collection of information given in this database" should be understood as limited in scope to the entirety of the database or a substantial part of it, and limited in content only to those acts of disposition that unreasonably prejudice the legitimate interests of the database maker or conflict with the normal exploitation of the database. In fact, Norid stipulates that it may grant "written permission" for the performance of otherwise restricted acts. Based on the information available until now, however, it is unclear who the beneficiaries of such written permissions are and under what terms and conditions such permissions are awarded. The statement may serve as an indication of Norid's future intention to enter into bulk-access agreements and extend third-party access to the entire WHOIS database.

To what extent is Norid entitled to prohibit individual acts of access to and disposition of insubstantial parts of WHOIS database? According to paragraph 6 of section 43 of the Norwegian Copyright Act,[124] agreements which extend the database maker's rights under paragraph 1 of the section over a database which had been made available to the public, shall be unenforceable. In other words, the statutory legal provisions represent the only source of limitations for the exclusive rights of the database makers, and any agreements that extend those rights to the detriment of the database users shall be considered null and void. Therefore, Norid cannot restrict individual acts of access to insubstantial parts of the database, for any purpose whatsoever. The statement made by Norid that "it is forbidden to copy or imitate in any other way, store, download or transfer information" should be amended or interpreted accordingly.

Although acts of disposition over insubstantial parts of the database fall outside the scope of the exclusive authorisation rights of the database maker, repeated and systematic extraction of insubstantial parts can be prohibited by the database maker in accordance with paragraph 2 of section 43. The

124 This paragraph transposes Article 15 of the Database Directive into Norwegian law.

central criterion for evaluating the cumulative effect of such acts of disposition is whether or not they unreasonably prejudice the legitimate interests of the database maker or conflict with the normal exploitation of the database, that is, whether they cumulatively lead to disposition over a significant part of the database. In this evaluation, the purpose for the extraction will have significant weight. For example, the repeated use of a database by a library or for research purposes cannot be said to produce a detrimental effect on the normal exploitation of the database as required by the law.[125]

What limitations are stipulated by the law on the exclusive rights of disposition of the database maker over the entirety or significant parts of the database? According to section 12 of the Norwegian Copyright Act,[126] copies of the entirety or of substantial parts of a database may be used for private, non-commercial purposes. The rightsholder will receive compensation through the state budget or as determined by the King. However, according to section 12(2)(c), the private use rights do not entitle one to produce electronic copies of an electronic database (only non-electronic copies are permitted). Thus, the statement made by Norid that "this [the restriction] also applies independently of whether or not the intention is commercial use" should be amended or reinterpreted accordingly.

Paragraphs 4 and 5 of section 39h of the Copyright Act transpose Article 6(1) of the Database Directive and extend its scope[127] to databases which are not deemed worthy of protection through copyright. The effect is that the lawful user of the WHOIS database can perform acts necessary in order to access the contents of the database without the possibility to restrict this right of access through individual agreements stipulating the contrary. This limitation of the freedom to contract presupposes that the database had previously been made public. Per a contrario, if the database has not been made public, or regarding those parts of the database which are not public, the rightsholder can decide for themself under which terms and to whom to give access to the unpublished data.

A license agreement between Norid and a user of the WHOIS database cannot stipulate that the user does not have disposition rights over insignificant

125 See too Ot.prp. nr. 85 (1997–98), p. 41 ("Hovedregelen er at råderetten ikke omfatter uvesentlige deler av innholdet i en database. Når et bibliotek gjør gjentatte søk og tar utskrifter av mindre deler av for eksempel referansedatabaser, til bruk for sine lånere, vil dette etter departementets syn falle utenfor slik utnyttelse som forslagets andre ledd tar sikte på, nettopp fordi dette ikke vil antas å stride mot rettighetshaverens legitime utnyttingsinteresser.").

126 Though originally drafted for copyrighted works, its applicability was subsequently extended by section 43(5) to catalogues and databases.

127 This extension is permitted by virtue of Article 13 of the Database Directive (see also Recital 52 of the preamble to the Directive).

parts of the database or that the database cannot be exploited in the private sphere. However, the law does not prevent the rightsholder from stipulating contractual limitations on the rights of the legitimate users out of concern for the protection of other legitimate interests (for example, privacy concerns).

3.2.2 Contractual limitations of WHOIS database makers' rights

As a matter of principle, contractual derogations from the rights and obligations guaranteed through statutory laws are permitted only to the extent and within the limits permitted by the laws.

In the layered contractual framework of the gTLDs, ICANN appears to be the beneficiary of the rights in WHOIS databases, deciding which data may be included in WHOIS databases at each level, to whom access to the collected data should be granted and under which conditions, as well as how rights in the database can be further assigned to third parties. These rights have been transferred to ICANN by the registrars via a compulsory and non-negotiable Registrar Accreditation Agreement (RAA) and by the registries through the Registry Agreement (RA). Both agreements stipulate the obligation of the registries – and, respectively, of the registrars – to create and maintain WHOIS databases, but they do not recognise the database makers' exclusive rights afforded in the European Union by the Database Directive. To the contrary, according to section 3.3.5 of the RAA, the registrars "shall not impose terms and conditions on use of the data provided, except as permitted by policy established by ICANN". Moreover, "the data accessible shall consist of elements that are designated from time to time according to an ICANN adopted specification or policy" (section 3.3.1). Similar obligations to abide only by ICANN adopted specifications or policies are imposed on the registries.[128]

Thus, it would appear that the registries and registrars act as agents of ICANN in providing a service within the limits of the prescribed parameters, rather than as database makers with legitimate interests in the value of their investments. One may argue, however, that the policies set by ICANN are the result of a consensus building process which ensures broad agreement among large categories of stakeholders, thus conferring legitimacy to ICANN's intervention within the limits of its mandate.

In this case, the .com registry is governed by US law. As explained in the previous section, the American law provides a weaker level of protection to the makers of unoriginal databases, who are left with the task of contractually defining the boundaries of their rights. While this situation allows the database

128 See, e.g., .com Registry Agreement (01.03.2006), Appendix 5 ("Whois specifications"), at <http://www.icann.org/en/tlds/agreements/verisign/appendix-05-01mar06.htm>.

maker a high degree of variation and customisation in the scope of protection, the provisions of the contract can normally be invoked only against the contractual partner and not against an infringing third party. It is relatively unlikely that an infringement of rights in the WHOIS database will come from the contractual party, which in the present case is ICANN, since the latter has already guaranteed by the RAA the contractual right to bulk access for the entire registrar WHOIS database.[129] More often, infringement will be the result of a third party's accessing the database for illegitimate purposes or in disregard of the legitimate rights of the registrars of the registrants.

On the other hand, the European registrars accredited to provide registration services under .com face the challenge of accommodating the scope of the statutory rights conferred by the Database Directive along with their obligations under the RAA. It is questionable to what degree the relevant provisions of the RAA are enforceable in the event they conflict with the Database Directive (or national laws transposing the Directive).

In the following, the limitations on the exercise of the database rights by the registry and the various registrars according to the RAA and the Database Directive are discussed.

A. The registry for the .com domain provides the "authoritative WHOIS service for all second level Internet domains registered in the .com TLD and for all hosts registered using these names".[130] In providing the service, the registry must set up a centralised WHOIS database and update it daily. The registry not only provides an access facility to the databases belonging to the registrars, but it receives data from the registrars and sets up its own databases including additional identification data about the registrars. The content and policies for access to the registry database are decided by ICANN as follows:

1. individual access to records connected to one domain name should be ensured for anyone via port 43 and via the registry Operator's site. The information to which access is provided has been collected by the registry from the registrars, rather than directly from the domain name holders.
2. bulk access to up-to-date data concerning the domain name, registrar data and name server registrations will be ensured by the registry on a daily schedule, to a third party designated at intervals by ICANN.

129 Section 3.4.3 of the RAA stipulates that "[…] during the Term of this Agreement and for three years thereafter, the registrar shall make these records available for inspection and copying by ICANN upon reasonable notice. ICANN shall not disclose the content of such records except as expressly permitted by an ICANN specification or policy".

130 See .com Registry Agreement (01.03.2006) in the introduction to Appendix 5 (Whois specifications).

Additionally, the registry must provide bulk access to ICANN, to updated data concerning the domain name, registrar data and name server registrations. The purpose of this access is to *ensure the operational stability of the registry services and DNS.*

3. the registry shall deposit into escrow all registry data (defined as data pertaining to the domain names registered, name servers sponsored, registrars, registrant data), entrusted to an escrow agent mutually approved by the registry and ICANN. The escrow data are intended to guarantee that data are not lost regardless of potential technical difficulties faced by the registry at any given time.

To my knowledge, the legitimacy and enforceability of these contractual provisions have hitherto not been challenged by the .com registry operator either in court or via ADR procedures. The above stipulations warrant two further comments. First, because the access to WHOIS records for individual queries is free of charge and unrestricted, it may reasonably be presumed that any query addressed to the WHOIS database is to be regarded as coming from a "legitimate user".[131] Secondly, considering the volume of data to which access is granted through bulk access, as well as the value of the investment in obtaining these data, it can be envisaged that bulk access to the data represents a right to extract and to reutilise a significant part (if not all) of the WHOIS database. The purpose for allowing access to this registry-collected information is the provision of *cross-domain look-up facilities* by a provider designated by ICANN. However, considering the technical challenge in controlling subsequent use of data to which legal access has been obtained, it is questionable to what extent the registry can effectively ensure that the third party uses WHOIS data only for the specified purposes.

B. Section 3.3.5 of the RAA stipulates that the registrar should make available WHOIS data to individual queries for any lawful purposes, except to:

- "Allow, enable or otherwise support the transmission by e-mail, telephone or facsimile of mass, unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing customers";
- "Enable high volume, automated, electronic processes that send queries or data to the systems of any registry Operator or ICANN Accredited registrar, except as reasonably necessary to register domain names or modify existing registrations".

131 Cf. Beunen, *Protection for databases*, *op. cit.*, p. 215 and references cited therein, noting that anyone who has free access to a website has lawful access to it unless this requires the circumvention of technological protection measures.

Individual queries to a WHOIS database may be regarded, in the language of the Database Directive, as extractions of an insubstantial part of the contents of the database. One set of records regarding one domain name represents a qualitatively and quantitatively insignificant part of a registrar's database. According to Article 8(1) of the Database Directive, the maker of a database cannot prevent a lawful user from extracting insubstantial parts of its contents for any purpose whatsoever. Moreover, according to Article 15, any contrary contractual provision shall be null and void.

The question arises is whether the provisions of section 3.3.5 of the RAA (stipulating restrictions on use of WHOIS records) are enforceable against a European registrar, in light of Articles 8(1) and 15 of the Database Directive. The answer, I believe, is affirmative. The exceptions stipulated by the RAA prohibit the use of the public WHOIS data records for the purpose of transmitting unsolicited commercial communications (as well as allowing, enabling or supporting similar acts) and for the purpose of automated data mining (or any other automated process that would hinder the normal functioning of the WHOIS service). According to Article 13 of the Database Directive, the provisions of the Directive do not prejudice existing legal provisions regarding, inter alia, "laws on restrictive practices". The behaviours restricted by the RAA are prohibited as well by statutory provisions applicable in Europe, and, by virtue of Article 13 of the Database Directive, should be considered in determining the scope of Article 8(1).

Moreover, according to Article 13(1) of the 2002 Directive on privacy and electronic communications,[132] "the use of automated calling systems for the purpose of direct marketing is only allowed in respect of subscribers who have given their prior consent". Where such prior consent was not given by the domain name registrant, the access and subsequent use of the registrant data for direct marketing purposes are prohibited, and such a restriction is not overridden by Article 8(1) of the Database Directive. If the damage it causes is sufficiently serious, the behaviour envisaged by the second restriction in section 3.3.5 of the RAA might also qualify as a criminal offence under the Council of Europe's Convention on Cybercrime.[133] Article 5 of the Convention considers the following as an offence of "system interference":

132 Directive 2002/58/EC of 12.07.2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (O.J. L 201, 31.07.2002, pp. 37–47).

133 ETS No. 185; adopted 23.11.2001; in force 01.07.2004.

"when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data".

Consequently, the enforceability of the exceptions in section 3.3.5 of the RAA by or against European registrars is dependent on whether the domestic law equally prohibits the same behaviours. In the event of the contrary, given the fact that Article 15 of the Database Directive prohibits contractual derogations from Article 8 (1), a user's access to insubstantial parts of a European WHOIS database cannot be contractually limited only to certain uses (such as, for example, to check the availability of a domain name).

Although the registrar does not have the right to prevent a lawful user from extracting insignificant parts of WHOIS database (such as single records about a domain name), it has the power to prevent repeated and systematic extraction of insufficient parts of the database, whereby the cumulative effect would amount to a substantial part and thus qualify as an infringement. This translates into the right of the registrar to introduce technological measures to limit the amount of queries that could be sent within a definite unit of time (usually one day) from the same IP address. Given the provisions of Article 10(3) of the Database Directive, which consider an updated database as qualifying for a renewed term of protection, it can be questioned whether an updated version of the database can be regarded as a new database (whereby repeated acts of extraction could be argued as affecting different databases and thus not constitute a significant cumulative extraction from one and the same database). Beunen cites case law in which the courts have interpreted Article 10(3).[134] The criterion used more often by the courts is whether the update is the result of a significant investment or not. Where only a few data records have been added during one day without a significant investment from the registrar, it can be considered that the WHOIS database held by a registrar remains a single database in a state of constant revision, and therefore it may be argued that a repeated extraction from the same source takes place.

Where a repeated and systematic extraction of insignificant parts of the database has occurred, the Directive requires in Article 7(5) a "harm test" as a condition for awarding financial relief to the rightsholder. In other words, in order to prevent the systematic and repeated extraction of insignificant parts of the database, the rightsholder must prove that the acts conflict with the normal exploitation of the database or prejudice the legitimate interests of the registrar.
By virtue of the RAA with ICANN, the registrar must provide not only individual access to single WHOIS records but also, in accordance with section

134 *Idem*, p. 199.

3.3.6, third-party bulk access for the downloading of a "complete electronic copy of the data available, at least one time per week". The access is governed by the terms of an agreement between the registrar and the third party. This act may be qualified according to the Database Directive as "an extraction of a copy of a significant part of the database". The remuneration which the registrar is entitled to claim for providing access is set by ICANN at a maximum of 10,000 Euro per year. ICANN further requires the registrar to restrict the purpose for which such bulk access may be granted, so that the receiving third party may not use the data for direct marketing purposes or for sending high-volume automatic queries to the registrar or registry. Moreover, further transmission of the data by the receiving party should be prohibited unless it is incorporated into a value-added product or service.

According to the Database Directive, the provision of bulk access to the entire WHOIS database is one of the prerogatives recognised as belonging to the maker of the database. However, the Directive stipulates in Article 9 that a lawful user can access significant parts (but not the entire database) of the database without authorisation for, among other things, public security or in the context of judicial procedures, even in the absence of a license agreement. Given this legal exception, it is questionable whether the database maker can invoke their right to claim remuneration from the beneficiaries of one of the exceptions in Article 9 (such as law enforcement). Given that restrictions on access can only be imposed by ICANN policies, the registrar is not in a position to introduce additional conditions for access. However, since ICANN sets only the maximum sum that can be claimed from the beneficiaries of the bulk access, the registrar could act upon the text of the Directive and allow free access to law enforcement authorities exercising their competence according to the law.

4 PROTECTION OF PERSONAL DATA IN WHOIS DATABASES

This chapter of the study focuses on the content of WHOIS databases. It aims at assessing the rights and the obligations of the registries and the registrars to lawfully process the personal data submitted by the registrants upon registration of domain names. The issues raised here constitute in many ways the Gordian Knot in the consensus-building process on WHOIS-related issues at ICANN level. The gTLD Policy Development Process aiming to optimize the public provision of data via the web-based WHOIS service and to improve the accuracy of the data has come to a halt, at the time of writing. Increased awareness of the data protection implications of the provision of WHOIS service, insufficient empirical data in support of the claims for "legitimate interests" of the various stakeholders and disagreement regarding the most appropriate compromise are among the factors that contributed to the current state of affairs. As a consequence, while awaiting a consensus to the contrary, the default rules stipulated by the Registrar Accreditation Agreement and the Registry Agreement still apply in the gTLD domains.

The ccTLD domains and their managers, however, now have the opportunity to reaffirm the application of national (and supranational) data protection legislation to the processing of personal data under the WHOIS regime. As noted earlier in this report, the principle of subsidiarity recognises that the "ccTLD policy should be set locally, unless it can be shown that the issue has global impact and needs to be resolved in an international framework". Moreover, it is recognised by the international community that most of the ccTLD policy issues are local in nature and should therefore be addressed by the local Internet Community, according to national law.

Given the above considerations, this chapter identifies the main requirements of European data protection law and the guarantees that should be paramount during the personal data processing carried out through WHOIS service. In the light of the existing practice at ccTLD level as well as the proposals that were submitted during the consensus-building process at the gTLD level, best practice examples of privacy-compliant implementations are identified and assessed.

4.1 Application of data protection legislation to WHOIS service

The provision of WHOIS service involves, as described in detail in Chapter 2 of this study, wholly or partially automated processes of collection, storage, publication and transfer to third parties of data relating to the domain name and to its registrant. The registry and the accredited registrars become involved in different stages of this process and, depending on the registration model adopted (thick or thin), have a higher or a lower degree of decision-making authority with regard to the means and purposes of the processing.

4.1.1 Nature of data processed

Several factors support the applicability of Directive 95/46/EC to at least some of the information processing involved in the provision of WHOIS service. The first concerns the nature of the data processed. In short, the provision of WHOIS service necessitates, at least to some extent, the processing of data that fall within the scope of the Directive.

To elaborate, the Directive applies, as a point of departure, to "processing of personal data wholly or partly by automatic means" (Article 3(1)).[135] In the understanding of the Directive, personal data designates "[…] any information relating to an identified or identifiable natural person (the data subject) […]".[136] At the same time, "the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable" (Recital 26 in the Directive's preamble). In assessing whether a set of data may lead to the identification of a natural person, "account should be taken of all the means reasonably likely to be used either by the controller or any other person to identify the said person" (Recital 26). The notion of "controller" is elaborated further below, but it suffices to note for present purposes that this denotes the person/organisation who/which determines the purposes and means of the data processing (Article 2(d)).

In the WHOIS context, it is clear that the data collected from a natural person registrant during the registration process (or subsequently, if updates are provided) are stored by the registrars (in the thin model) and by the registries (in the thick model) in such a way that the identification of the natural person

135 The rules of the Directive do not, however, apply to data processing that takes place in the course of an activity that falls outside the ambit of European Community law or that is carried out by a natural person in the course of a purely personal or household activity (Article 3(2)).

136 For a more extensive analysis of the "personal data" concept, see, e.g., Lee A. Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (The Hague /London/New York: Kluwer International Law, 2002), chapters 2 (section 2.4.1) and 18 (section 18.2).

is extremely easy. Although the ccTLDs are not under a statutory or contractual obligation to follow the gTLD WHOIS regime imposed by ICANN, there is currently a common practice[137] to request that the domain name applicants provide "accurate and reliable contact details"[138] as well as domain-related information. In the first category, the name, the address, telephone number, e-mail addresses and fax number of the registrants and their administrative and technical contact points are requested upon registration. Refusal or failure to provide accurate data constitutes grounds for refusal to register the domain name,[139] or for termination of the registration agreement and loss of the domain name.[140]

Data enabling identification of a *legal* person only (such as a corporation) fall outside the ambit of the rules laid down by Directive 95/46/EC – and, indeed, outside the ambit of the overwhelming majority of data protection laws, both in Europe and elsewhere. This means that WHOIS database operators usually need not apply the same data protection regime for data belonging to natural and legal person registrants alike; they may also distinguish between the two. In other words, a choice may be made between applying the same regime for both types of data or adopting different regimes for each. The first option would ideally lead to a homogenous processing of registrant data and eliminate the costs associated with the design and implementation of a reliable informational system that includes mechanisms for distinguishing between natural and legal person registrants and dissociated data-processing policies. However, the protection afforded to the data belonging to legal persons would not stem from the provisions of Directive 95/46/EC but, for the most part, from the contractual agreements between the data controller and the legal person data subject. A homogenous processing of WHOIS data would also provide a simple solution for the "grey area" situations where data identify at the same time the natural person and the legal person (employment relations)

137 See OECD's Working Party on Telecommunication and Information Services Policies, "Comparing Domain Name Administration in OECD Countries" (DSTI/ICCP/TISP(2002)11/FINAL; 08.04.2003), Table 8; available at <http://www.oecd.org/dataoecd/46/38/2505946.pdf>.

138 Section 3.3.7 of the RAA.

139 The .no Registrar Agreement stipulates the obligation of the registrar to check "before an electronic application is submitted to Norid, that it is correctly filled in, and that the applicant has signed a copy of the applicable declaration form which has been filled in correctly".

140 The .eu domain name WHOIS policy section 2.2 affirms that "[b]y deliberately submitting inaccurate information, the Registrant would also be in breach of the Terms and Conditions which could also lead to loss of the Domain Name." Similarly, section 11(1)(b) of the .no Domain name policy stipulates that if the "registration was based on incorrect information provided by or on behalf of the applicant", the domain may be deleted and made available to others.

or situations in which the legal and the natural person coincide (sole proprietorship). On the other hand, the second option would arguably better reflect the different needs and interests of the two categories and provide dissociated solutions to mitigate the risks arising from the use of the domain name for commercial purposes as opposed to personal, private purposes. Ultimately, the cost-benefit assessment of the WHOIS database operator must take into account the attractiveness of the domain towards each of the two categories, the history of use and abuse recorded in the given TLD for the two categories as well as the complaints received against/from either of the two.

Currently, the gTLD policy for the .com domain does not distinguish between natural and legal person registrants. At the same time – and as argued extensively by reform activists – it disregards many of the data protection principles for both registrant categories. By contrast, the WHOIS policy for the .no ccTLD stipulates a homogenous treatment of the .no registrants' data. Although that domain so far is open only to legal person registrants, it is recognized that some of the registrant data can also constitute personal data for the purposes of Norwegian (and EU) data protection law. Other ccTLD domains, such as .eu and .uk, stipulate different data protection rules for natural persons and legal persons respectively, in conformity with the data protection rules regarding data on natural persons and common practices regarding legal person registrants.

4.1.2 Operations involved in provision of WHOIS service

The provision of WHOIS service involves operations of collection, storage, making available, utilisation and transfer to third parties of registrant- and domain-related information. Directive 95/46/EC subjects to its regime the "processing" of personal data, meaning "any operation or sets of operations which are performed upon personal data, whether or not by automatic means, such as collecting, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" (Article 2(b)). It is clear that the processing of personal data during the WHOIS registration process and during the provision of WHOIS service is done either wholly or partly by "automatic means" – as indicated also in the relevant agreements with registrars and registries.[141]

The provisions of the Directive are applicable to partly automated data-processing operations regardless of how the data are structured. However, processing other than by automatic means (i.e., manual processing) may also

141 See, e.g., Article 7.1 of the .eu Registrar Agreement and section 3.4 of the RAA.

fall within the scope of the Directive if the data are part of a "personal data filing system". The latter notion is defined as "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis" (Article 2(c)). A WHOIS database may be regarded as such a system. It contains a "structured" data set which can be accessed "according to specific criteria" (in this case via the search words to be typed in the search field of the webpage functioning as a user interface to the database), and may also be "centralised" (in the case of a thick registration model), "decentralised" (in the case of a thin registration model) or "dispersed on a functional or geographical basis". In any case, as noted above, the scope of protection afforded by the Directive is not limited only to operations in relation to a personal data-filing system, but to any processing of personal data carried out at least partly through automatic means.

Given that the Directive defines "processing" as "any operation or set of operations which is performed upon personal data" (Article 2(b)), the entire design and provision of WHOIS service must fulfil the requirements of the Directive once the service first comes under the Directive's scope. While the greatest privacy-related concerns about the service arguably pertain to the actual publication of personal data relating to registrants, the collection, storage and transfer of the data independently of their publication should equally fulfil the criteria prescribed by the Directive.

4.1.3 Identity and roles of WHOIS service providers

Directive 95/46/EC identifies the rights and the obligations of the main actors involved in the processing of the personal data: the data subject, the data controller and the data processor. During the provision of WHOIS service, these roles are assumed respectively by the registrant, the registrar and the registry. However, the role distribution between registrars and registries is dependent on the model employed (thick or thin registry model) and may be difficult to determine in particular cases. Nevertheless, an accurate determination of the roles assumed by each of the participants in the provision of WHOIS service is a prerequisite for:

- determining the application of one or another of the national laws transposing Directive 95/46/EC to a particular data-processing operation;
- identifying which entity has the primary legal obligation to observe the data-processing principles laid down by the Directive and the corresponding rights of the data subjects thereunder.

According to the Directive, the data "controller" is the entity which "alone or jointly with others determines the purposes and means of the processing of personal data" (Article 2(d)). By contrast, a data "processor" is an entity that "processes personal data on behalf of the controller" (Article 2(e)). In elaborating who may be a controller, the Directive also states that, "where the purposes and means of processing are determined by national or community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or community law" (Article 2(d)). Thus, the Directive allows both a functional and a statutory determination of the data controller.

However, another possibility should also be recognised as being in line with the spirit of the Directive. This is that an entity expressly takes on the role of controller through contractual agreements and/or soft law instruments. This occurs, for example, in the case of the .eu domain, where both the data controller and data processor roles are designated in the accreditation agreement between the registry and the registrar. According to Article 9 paragraph 4 of the EURid Registrar Agreement, "the registrar is hereby appointed as a Data Processor with respect to the collection and transfer to EURid, acting as a Data Controller, of the Personal Data of the registrants requesting the Registration of a Domain Name or renewal of a Registration Period."

The legality of such designation is supported both by a legal and a factual argument. Firstly, EURid is entrusted by the European Commission with the organisation, administration and management of the .eu TLD, "including maintenance of the corresponding databases and the associated public query services",[142] and EURid is to do so "on the basis of principles of quality, efficiency, reliability and accessibility".[143] The Commission stipulates too that "'Who is'-type databases should be in conformity with Community law on data protection and privacy".[144] Thus, it can be argued that a clear allocation of responsibility between the registry and the registrars is in the field of competence of the designated registry and represents a measure to ensure the quality and reliability of the management of the .eu domain.

Secondly, the actual distribution of functions between the registry and the registrars in the processing of registrants' personal data supports the same role distribution. Similar to most ccTLDs, .eu follows a "thick" registration model where the registry has been assigned technical, administrative and policy-making competence for the given ccTLD, therefore determining the "purposes and means" of the data processing. All authoritative registrant-related information is kept within the registry, while the registrars are accredited only to intermediate

142 Regulation (EC) 733/2002 (referenced *supra* note 27), Article 2(a).
143 *Idem*, Article 4(2)(a).
144 *Idem*, Recital 12.

the relation between registrants and the registry. In carrying out this function, registrars are "processing data on behalf of the controller" within the limits of their accreditation. Under the .eu Registrar Agreement, the data-processing tasks of the registrar are limited to verification and data check ("ensure and document"), provision of information ("[i]nform each registrant of all information sent by EURid to the registrar") and data forwarding (Article 4). In fulfilling its tasks, the registrar "must respect the procedures developed by EURid to register, renew or manage a Domain Name" (Article 7.1) and must "use the access to EURid's software components in good faith" (Article 7.3). On the other hand, in its role as a data controller, the registry (EURid) "should comply with the relevant data protection rules, principles, guidelines and best practices, notably concerning the amount and type of data displayed in WHOIS database".[145] The registry shall also determine the procedure for the accreditation of registrars and set the technical requirements for the accreditation of registrars.[146] The registry has also drafted the ".eu Domain name WHOIS policy", along with the "Code of conduct for .eu registrars".

In conclusion, EURid has the legal right and the ability to set the "purpose and means of the processing", while the accredited registrars process personal data in the framework of their accreditation, as decided by the registry.

An express designation of the registry as data controller and of the accredited registrars as data processors has not been made for the .no domain, although the use of the thick registry model for .no would indicate a similar role distribution as the one in the .eu ccTLD. Under the .no Domain Name Regulation,[147] the registry is given the right to assign domain names under .no (Articles 2(b) and 3) and the role of the registrar is defined in terms of forwarding applications and updates on behalf of the registrants in accordance with the terms of their accreditation (Article 2(c)). The registry is to draft the domain name policy for .no based on general principles of domain name administration and taking into account the opinions of the local Internet community and authorities (Article 3). Parts of the registration process are entrusted by the registry to the registrar. One of these tasks is the forwarding of domain name applications to the registry, using the forms developed by Norid.[148] Further, in carrying out its administrative assignments, the "registrar is obliged to comply with the regulations in effect at any time, as well as the guidelines and routines that Norid has provided on its Web pages".[149] As such, it would appear that

145 Commission Regulation (EC) No. 874/2004, *supra* note 26, Recital 13.
146 *Idem*, Article 4.
147 Referenced *supra* note 25.
148 .no Domain name policy, paragraph 7(2).
149 Registrar Agreement, <http://www.norid.no/registrar/regavtale.en.html>, paragraph 3.3.

the registry in the .no domain assumes the role of data controller and has all the obligations that are assigned to controllers by Directive 95/46/EC, while the accredited registrars are data processors, in a thick registration model. Although the .no domain is currently open only to legal person registrants, the registry acknowledges[150] the application of data protection legislation to the processing operations leading to the publication of personal data of the designated contact persons or of one-person businesses (sole proprietorships). Furthermore, Norid is currently considering opening up .no for natural person registrants;[151] if it does permit such registration, the data protection requirements will become all the more applicable to the activity of Norid.

While both .eu and .no domains operate with thick registration models, .com operates with a thin registration model – i.e., the registry database contains only information about the domain name (such as the domain name, the nameserver used as well as addresses and the name of the registrar); the domain name registrant data as well as contact data are maintained by the registrar. What are the data protection implications of this model? More particularly, to what extent do European data protection rules apply in the .com domain and, to the extent these rules do apply, which legal entities should assume the respective roles of data controller and data processors?

Taking the question of applicability first, Article 4 of Directive 95/46/EC lays down certain criteria for resolving this. The principal criterion for determining which country's data protection law applies is the place of establishment of the data controller; one shall apply the data protection law of the Member State of the EU (or European Economic Area – EEA) to the processing of personal data when the controller of that processing is established in the said Member State (Article 4(1)(a)). However, even if a controller is established in a jurisdiction outside the EU or EEA – i.e., in a so-called "third country" – the data protection law of an EU/EEA member state may nevertheless apply if the controller "for the purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State" (Article 4(1)(c)).[152] In order to determine whether European data protection rules are applicable to the provision of WHOIS service in the .com domain, it is imperative, therefore, to determine first who the data controller is.

150 See "Bruk av informasjon lagret i Norids kundedatabase", at <http://www.norid.no/domenenavnbaser/personvernpolicy.html>.

151 See "Norske domenenavn for private personer", at <http://www.norid.no/regelverk/forslag/privatpersoner-2008/>.

152 For further analysis and criticism, see, e.g., Lee A. Bygrave, "Determining Applicable Law pursuant to European Data Protection Legislation", *Computer Law & Security Report* [now Review], 2000, vol. 16, pp. 252–7.

As stated above, the controller is the entity that "alone or jointly with others determines the purposes and means of the processing of personal data" (Article 2(d)). Given the centralised accreditation and designation procedure of ICANN, as well as the policy-making competence of GNSO at gTLD level, it would appear that ICANN determines the "purposes" of the data processing. ICANN, however, is not the principal decision-making authority in determining the means for processing. Instead, the .com registry as well as the different accredited registrars may determine on their own the means they choose to use in the provision of WHOIS service, in accordance with technical specifications agreed by the international community via the RFC documents, and in conformity with the policy aims and data specification requirements issued by ICANN. According to section 3.3.1 of the Registrar Accreditation Agreement, "[a]t its expense, registrar shall provide an interactive web page and a port 43 WHOIS service providing free public query-based access to up-to-date (i.e., updated at least daily) data concerning all active Registered Names sponsored by registrar for each TLD in which it is accredited" . Similarly, while the data specification is imposed by ICANN on the .com registry, the registry is left to decide the implementation model of the registry-level WHOIS service. It would appear from the .com model that one entity determines the purpose of the data processing while others are responsible for choosing the means by which to reach the objective. At a conceptual level, it may be argued that by dictating the purpose, one constrains at the same time the means to be used in fulfilling it. However, by not having direct control over the means, it may be difficult to be held accountable whenever the purpose is not reached or the means are misused.

Neither the Directive, its preparatory works, nor case law pursuant to it provides an authoritative answer pertaining to a hierarchy between the two functions of the controller; the assumption is that the two roles are fulfilled by the same entity. Nevertheless, the definition of "controller" explicity envisages that control can be shared, and it is reasonable to presume that such sharing may involve some inequality between the concerned parties in the level and kind of control exercised by each. As such, general legal principles of fairness and justice would support an interpretation where several controllers process personal data jointly in the .com domain. In this perspective, all relevant actors are joint controllers in the entire operation of the .com WHOIS service, while at the same time they are liable for the operations performed directly in their area of decision-making competence: policy-making (ICANN), coordination and control (the registry) and finally daily operation (the accredited registrar).

If all three actors are data controllers, and the Directive applies to them, they should only process data in accordance with the Directive. However, application of the Directive occurs only if they are "established" in a Member

State of the EU (or EEA) or they make use of "equipment" located in a Member State, as laid down in Article 4(1)(c). Both ICANN and VeriSign are corporations set up and headquartered in the USA and therefore "established" there. It could be argued that, for the purposes of Article 4, ICANN is also established in Belgium as it has offices in Brussels (in addition to offices in Marina del Rey, Washington DC and Sydney). Under EU law, a corporation can have multiple places of "establishment" in the sense of places where it conducts "effective and real exercise of activity through stable arrangements" (Recital 19 of the Directive's preamble).[153] Moreover, "the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect" (Recital 19). Nonetheless, it is doubtful that ICANN's Brussels office acts as controller in the WHOIS context; that role is most likely filled solely by ICANN's head office in Marina del Rey (California). For the purposes of the following analysis, it is therefore assumed that ICANN as controller is established outside the EU. It is also assumed that neither ICANN nor Verisign use "equipment" that would bring them within the scope of an EU (or EEA) Member State's data protection law on the basis of Article 4(1)(c).

As far as registrars are concerned, if they are established in an EU/EEA Member State, their registration practices shall follow, first and foremost, the relevant national rules on data protection (which transpose the Directive), and only afterwards, to the extent that they do not conflict with the law, shall those practices conform to the provisions of the contractual agreements to which the registrars are party. The potential for legal conflicts between the provisions of the agreements entered into with ICANN and the provisions of the national data protection laws is extremely high since ICANN accepts requests for accreditation from both European and non-European registrars. A similar conflict would occur in cases where the registry is established in a European jurisdiction.[154]

In an effort to mitigate such conflicts, the ICANN Board approved in May 2006 a "Procedure for Potential Conflicts between WHOIS Requirements

153 This builds on ECJ case law, in particular Case C-221/89, *The Queen v. Secretary of State for Transport, ex parte Factortame Ltd and others* [1991] ECR I-3905, paragraph 20.

154 This is, for example, the situation with the .tel gTLD, the registry for which – Telnic, Ltd. – is incorporated in England: see further <http://www.telnic.org/aboutus.html>. Telnic has successfully requested ICANN to adjust the .tel Registry Agreement in order to ensure compliance with the UK Data Protection Act. See further .tel Registry Agreement (30.05.2006), Appendix S, Part VI (04.02.2008), available at <http://www.icann.org/en/tlds/agreements/tel/appendix-s-04feb08.htm#Part6>.

and Privacy Laws", recommended by the GNSO.[155] That procedure was subsequently elaborated by ICANN staff in December 2006.[156] Basically, the procedure involves following six steps when there is conflict between national privacy laws and WHOIS requirements:

1. Notification that a conflict is present. A conflict is present when the registrar/registry is hindered from complying with the ICANN policies by an investigation, litigation, regulatory proceeding or other government or civil action.
2. Consultation, not only between ICANN and the registrar/registry concerned but also between ICANN and local/national enforcement authorities or other claimants (if practicable). The aim of the consultation is to find a compromise solution that would enable the registrar/registrant to comply to the largest extent possible with both national and ICANN requirements.
3. General Counsel analysis and recommendation. ICANN's General Counsel will analyse the conflict. While awaiting that analysis, ICANN may agree to a temporary exemption of the defendant from complying with the ICANN policy. The analysis will recommend how the issue should be resolved, including by introducing an exception for those categories to which the conflict applies.
4. Resolution of ICANN Board. Following the General Counsel's recommendation, the Board will reach a decision in which it will have to consider the expected impact of the recommendation on the operational stability, reliability, stability and interoperability of the Internet's unique identifier systems. Public comments may be scheduled in order to assess better the expected impact and the opinions of the stakeholders on the proposed actions.
5. Publication. The decision reached will be made available to the public.
6. Ongoing review. ICANN will annually review the effectiveness of the procedure, taking account of stakeholder input.

Conflict of law does not constitute the only possible legal basis for derogation from the policies set by ICANN. Under ICANN's Bylaws, the ccTLD manager may refrain from implementing a policy that would require them to breach custom, religion or public policy, as long as a failure to implement the policy would not impair DNS operations or interoperability (Article

155 The Board decision is at <http://www.icann.org/en/minutes/minutes-10may06.htm>. The procedure is at <http://gnso.icann.org/issues/tf-final-rpt-25oct05.htm>.

156 See "Draft ICANN Procedure for Handling Whois Conflicts with Privacy Law" (03.12.2006), at <http://gnso.icann.org/issues/whois-privacy/whois_national_laws_procedure.pdf>.

IX section 14(11)). In terms of possible sanctions for non-compliance, the Bylaws stipulate that "any individual relationship a ccTLD manager has with ICANN or the ccTLD manager's receipt of IANA services is not in any way contingent upon membership in the ccNSO" (Article IX section 4(3)). In other words, even in the case where, following a conflict, a ccTLD manager decides to withhold from or cease to be a part of the ccNSO, this conflict will not hinder the respective ccTLD from being part of the DNS[157].

The above-mentioned regulatory measures would seem to indicate that adherence to the substantive policies developed by ICANN for gTLDs, or implementation of similar policies at ccTLD level would be the result of a voluntary action from the ccTLD manager. Furthermore, the countries would be relieved from all responsibility of applying the ICANN policies that were not set globally through a ccTLD policy process in as much as this derogation does not impact upon the overall functioning and the stability of the DNS. In practice, however, this will more likely be an issue for negotiation between ICANN and the national Governments and will be highly dependent on the interpretation given to the terms of the ccTLD delegation agreements between ICANN and the national registry.

4.2 Legal basis for processing personal data when providing WHOIS service

As noted above, where the data-processing operations are carried out by a controller established on the territory of an EU/EEA Member State, the national provisions of that Member State (adopted pursuant to Directive 95/46/EC) shall apply.[158] Belgium, the country where the controller for the data processing taking place in the .eu ccTLD is established, has transposed the Directive into national law through amendments to its "Law of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data".[159] The provisions of that statute are clarified through a royal decree (Arrêté royal) from 2001.[160]

157 Further on the "IANA function" of ICANN, see <http://www.iana.org/domains/root/>.

158 According to Article 4(1)(a) of Directive 95/46/EC.

159 As modified by the Law of 11 December 1998 implementing Directive 95/46/EC (Belgian State Gazette, 3 February 1999, 3049) and the Law of 26 February 2003 (Belgian State Gazette, 26 June 2003). A consolidated version of the statute is available in French at <http://www.privacycommission.be/fr/static/pdf/wetgeving/loi_vie_privee.pdf>.

160 See Arrêté royal portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l' égard des traitements de données à caractère personnel, available at <http://www.privacycommission.be/fr/static/pdf/wetgeving/ar_vie_privee.pdf>.

In Norway, the country where the registry for the .no domain is established, Directive 95/46/EC is transposed by the "Act of 14 April No. 31 relating to the processing of personal data" (hereinafter termed "Personal Data Act").[161] The provisions of the Belgian and the Norwegian Acts are referred to in the following as the principal legal sources of the respective rights and obligations for the two ccTLD registries in connection with processing of personal data. In addition, reference is made to Directive 95/46/EC and to ICANN's Registrar Accreditation Agreement for analysis concerning the legal rights and obligations of the European registrars accredited to provide registration services in the .com gTLD.

Directive 95/46/EC stipulates (in Article 7) six alternative criteria for permitting the processing of personal data:

1. the freely given, informed and specific consent of the data subject;[162]
2. the need to perform the terms of a contract with the data subject or to take steps at the request of the data subject prior to entering into a contract with the data subject;
3. compliance with a legal obligation to which the controller is subject;
4. protecting the vital interests of the data subject;
5. performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller or in a third party to whom the data are disclosed;
6. the processing is necessary for the purposes of the legitimate interests pursued by the controller, and these interests override those of the data subject.

The Directive thus provides a wide range of justifications for virtually all data processing activities which the controller has an interest to pursue. According to Article 5, however, it is for the Member States to determine more precisely the conditions under which the processing of personal data is lawful.

The data-processing operations in relation to the collection of registrant details in the customer database and their further publication and processing for providing WHOIS service may arguably be justified by all of the above-listed legal bases provided by the Directive, excluding the criterion concerning protection of vital interests of the data subject. The processing operations are without

161 The Norwegian title of the Act is Lov om behandling av personopplysninger (personopplysningsloven). An unofficial English translation of the Act is available at <http://www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/lov-20000414-031-eng.pdf>. In the following, quotations (in English) from the Act are based on this translation.

162 According to Article 2(h) of the Directive, stipulating the qualities that the data subject's consent should fulfil.

doubt justifiable. However, depending on the reason invoked by the registry as a justification of the data processing envisaged, additional guarantees for the data subject should be in place. The extent to which these guarantees are in place and made available to the data subject is examined in the following.

4.2.1 The consent of the data subject

The Belgian data protection law stipulates (in Article 5) in a manner similar to the Directive, the six criteria for permitting data processing, without imposing any hierarchy among them or requiring the data controller to use the one more often than the other. Nonetheless, in its ".eu Domain name policy", the registry for the .eu ccTLD expresses its preference for collecting the informed and specific consent of the potential registrant, although it acknowledges additionally that the provision of WHOIS look-up service by the registry is also "required by the public policy rules" as set out in Commission Regulation (EC) No. 874/2004.

For consent to be valid, it should fulfil, according to the law, three cumulative requirements:[163]

- It should be freely given – that is, no pressure has been exercised on the data subject in order to agree to the processing;
- It should be specific – that is, it should concern a well-defined processing operation or set of operations;
- It should be informed – that is, the data subject has received all the relevant information about the processing.

In the current system, the data subject is asked to agree to have the personal data processed via WHOIS service simultaneously with agreeing with all the other terms and conditions of the registration. The .eu WHOIS policy stipulates that "by registering a Domain Name and accepting the .eu Domain Name Registration Terms and Conditions ("Terms and Conditions"), the registrant authorises the registry to process personal and other data required to operate the .eu Domain Name system". It is not possible for the registrant to agree to the terms of the registration agreement without agreeing to have the data made publicly available via WHOIS service and if the registry wishes so, transfer the personal data to third parties. This all-or-nothing situation leaves a lower degree of freedom of decision for the applicant, cornering them into the position of making a trade-off between their legitimate interest in having an Internet

163 Interpretation of the key requirements of a valid consent is provided by the Belgian Privacy Commission at <http://www.privacycommission.be/fr/lexicon/c/Consentement-indubitable.html>.

presence and their right to privacy. From the point of view of the registry, the option of all-inclusive consent may be justified by the fact that the registry itself is under a legal obligation to provide the service. However, the law does not impose on the registries which information to collect from the registrants, or under what terms and conditions they may make them public or transfer them to third parties. Neither do the international agreements with ICANN impose on the registries a particular configuration of WHOIS service for the ccTLD domain.

The impossibility to have a domain name registered without agreeing to the publication of personal data in a public directory (such as WHOIS) is also in tension with the provisions of Directive 2002/58/EC (Privacy in Electronic Communications Directive) which stipulates that the subscribers (to a public electronic communications service) should be recognised a right "to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data" (Article 12(2)). Moreover, "[n]ot being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge" (*idem*). Although it may be problematic for a registry alone to take the initiative of reforming the domain name registration system by introducing a voluntary participation in the WHOIS directory for the domain names registered under the ccTLD it manages, the registries should be aware that in not giving the registrants a clear possibility to opt-out from being included in a public directory they may face sanctions for contravention of the provisions of national laws implementing Directive 2002/58/EC.

It may be argued that WHOIS service is such an essential part of the Domain Name System and that the security of the latter is so dependent on provision of WHOIS service, that domain names may not be registered and managed properly without it. As such, requesting the applicants to consent to all the terms and conditions of the Registration at the same time is justified by the fact that they are inseparable parts in the provision of one and the same registration service. This argument cannot be accepted, however, without reservations. Firstly, despite the fact that the inclusion of domain information and registrant data in WHOIS database was initially voluntary, domain names could still be registered and managed adequately.[164] Secondly, WHOIS service provides nowadays a broader spectrum of arguably legitimate purposes, facilitating operability being only one of them. If WHOIS service is seen as limited only to its technical function, then this should be considered as the only purpose of collection. The display of personal data (and the amount of data collected)

164 See Chapter 2 (section 2.1) of this Report.

should then be restricted to what is necessary for the attainment of that purpose. If subsequent uses are to be made of the data collected, then they should be the subject of a renewed consent. Given these reservations, it is imperative that a valid consent from the domain name applicant be based on specific and sufficient information provided by the registry about the data processing – that is, a high standard should be kept in mind in the interpretation of the two remaining conditions of an informed consent (dealt with next).

One of those conditions is that the consent should be specific – that is, it should concern a well-defined operation or set of operations. While the first requirement for a valid consent imposes a negative obligation on the data controller (not to constrain), fulfilment of the other two requirements depends on the active involvement of the controller: the provision of information to the data subject. The information rights of the data subject are analysed in section 4.3 below. For the purposes of the present discussion, it is relevant to highlight that the consent (and implicitly the processing operations) should have a well-defined scope.

The registry for the .eu domain complies with this obligation by affirming as follows: "The registrant explicitly agrees that the registry can use the data for operating the system (which will include attribution of the Domain Name, transfer of a Domain Name to a new registrant, transfer of one Domain Name or a portfolio of Domain Names to a new registrar) and can after the unambiguous consent of the registrant transfer the data to third parties but only … [conditions for transfer follow]". The registry takes also upon itself the obligation to request a specific consent from the data subject when the transfer of data to third parties is envisaged. Furthermore, "[w]hen registering a Domain Name, the registrant is required to accept the registry's Terms and Conditions which authorises the registry to make some personal data accessible on its web site, along with some other technical data, in order to guarantee the transparency of the domain name system towards the public." Thus, the scope of the envisaged data processing is clearly revealed.

The final condition of a valid consent is that the data subject is informed about all the relevant aspects of the processing. Article 9 of the Belgian Data Protection Law stipulates the obligation of the controller to inform the data subject, "no later than the moment on which the data are obtained", about:

a. name and address of the controller and, if such is the case, of his representative;

b. the purposes of the processing;

c. the existence of a right to object on request and free of charges against the intended processing, if personal data are obtained for purposes of direct marketing;[165]
d. other additional information, in particular:

- the recipients or categories of recipients of the data,
- whether or not replies to the questions are obligatory as well as possible consequences of a failure to reply,
- the existence of the right of access to and the right to rectify the personal data concerning him.

The data controller may be exempted from providing this information in two situations: either where the data subject already has this information; or where the additional information is not necessary to guarantee fair processing towards the data subject, taking into account the specific circumstances in which the data are obtained.

The .eu registry provides the information required by the law either in its WHOIS policy, or in its ".eu Domain Name Registration terms and conditions". Both documents are available on the registry's website but the applicant is also required to agree with their terms and conditions upon registration. The applicant therefore has the opportunity to obtain prior comprehensive information about the terms of the registration and must additionally certify that the terms and conditions have been read and understood as part of the domain application process. It can therefore be argued that the registrant of a .eu domain makes an informed decision based on information concerning: (i) the identity of the registry,[166] in its role as data controller; and (ii) the purposes of the processing (i.e., "to provide reasonably accurate and up-to-date information about the technical and administrative points of contact administering the domain names under the .eu TLD").[167] While the registry fails to expressly explain why the latter information is necessary, the reason can be inferred from the statement, "[i]f the registry is holding false, incorrect or outdated information, the registrant will not be contactable and may lose the name" – i.e., that the information will ensure a communication channel between the registry and the registrant. The registrant is also informed that the use of WHOIS data for marketing purposes is prohibited. The registry is actively involved

165 This part of the provision transposes Article 14(b) of Directive 95/46/EC.

166 Specified as "EURid vzw/asbl, a nonprofit organisation duly incorporated and validly existing under the laws of Belgium, with a registered office at Park Station, Woluwelaan 150, 1831 Diegem (Belgium)". See <http://www.eurid.eu/files/trm_con_EN.pdf>.

167 See, though, Chapter 2 (section 2.2) for a discussion about the inadequacy of the purpose definition in the .eu WHOIS policy.

in preventing misuse of public WHOIS data, both through legal means and through technical means, as specified in section 2.5 of the .eu Domain Name WHOIS policy.[168]

Although it is not expressly required by the law, in the spirit of a fair and transparent provision of WHOIS service, the registry provides additional information to the potential applicants: They include:

- the registrant's right to access his own personal data and to request that the data be amended;
- the types of information collected only for internal use, for what reason, and under which circumstances / to whom it may be disclosed;
- the distinctive regimes for publication of personal data applied to natural and to legal person registrants;
- the conditions under which third parties who claim a legitimate interest in the unpublished personal data of the registrant may gain access to this data;
- Internet accessibility facilities for the visually impaired.

In conclusion, despite the limited freedom to decide whether or not their personal data will be included in WHOIS public directory, the applicants for a domain name under the .eu ccTLD have the possibility to give specific and informed consent to the processing.

The Norwegian Personal Data Act stipulates in section 8 that personal data may be processed only if "the data subject has consented thereto, or there is statutory authority for such processing, or the processing is necessary in order:

- to fulfil a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into such a contract,
- to enable the controller to fulfil a legal obligation,
- to protect the vital interests of the data subject,
- to perform a task in the public interest,
- to exercise official authority, or
- to enable the controller or third parties to whom the data are disclosed to protect a legitimate interest, except where such interest is overridden by the interests of the data subject".

Although the criteria for permitting data processing follow those in Directive 95/46/EC, they are drawn up as three main groups: (i) consent; (ii) statutory authority; and (iii) necessity for achieving particular goals and/or interests. On their face, these three groups of criteria have equal normative weight – as they supposedly do under the Directive. However, in Norway, both in theory and, to

168 See <http://www.eurid.eu/files/whois_en.pdf>.

some extent, practice, the criterion of consent has been given normative priority over the other criteria such that a data controller must ordinarily obtain the data subject's consent to the processing unless there are reasons for waiver that are grounded in more than just considerations of cost and convenience.[169]

Section 3.1 of the memorandum on "Use of information stored in Norid's customer database"[170] describes the legal grounds invoked by Norid for the personal data processing operations it pursues. The .no registry invokes four legal conditions under which the registry is entitled to process the personal data of the registrants:

- the consent of the data subject;
- the need to fulfil a contract to which the data subject is party;
- to protect the interests of the subscriber;
- to perform a task in the public interest.

In the following, each of these grounds for processing is examined more closely, in the light of their interpretation in the legal literature.

A central aim of Directive 95/46/EC, as expressed in its Article 1, is to protect the fundamental right to privacy with respect to the processing of personal data of the natural persons. The right to privacy embraces the right to informational self-determination – i.e., the right of individuals to decide, to the largest extent possible, when, how, and to what extent, information about them is communicated to others.[171] Consent represents the most evident manifestation of the data subject's will to agree to the processing of data about themself, and it is therefore one of the most important concepts of data protection laws as well as the major legal rationale legitimising data-processing operations. In balancing the data subject's privacy interests with the legitimate commercial interests of the controller, the will of the data subject, manifested via the refusal to consent to the processing, should be given significant consideration.[172]

---

169 See decisions of the Norwegian Privacy Appeals Board (*Personvernnemnda*, a quasi-judicial body handling appeals from decisions of the Norwegian Data Inspectorate (*Datatilsynet*)) in cases 2004-01, 2004-04 and 2005-08. See too Dag Wiese Schartum & Lee A. Bygrave, *Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger* (Bergen: Fagbokforlaget, 2004), pp. 131, 135.

170 As noted earlier, the original title is "Bruk av informasjon lagret i Norids kundedatabase". The memorandum is in Norwegian only. See <http://www.norid.no/domenenavnbaser/personvernpolicy.html>.

171 For a broader discussion about the values and interests safeguarded by data protection laws, see Bygrave, *Data Protection Law*, *op. cit.*, chapter 7.

172 See too the preparatory works to the Norwegian Personal Data Act: Ot.prp. nr. 92 (1998–1999), p. 109 ("Generelt må hensynet til privatlivets fred tillegges betydelig vekt i avveiningen mot kommersielle interesser. Dersom en registrert gir den behandlingsansvarlige beskjed

The law imposes strict requirements on what can be regarded as a valid consent. According to section 2(7) of the Norwegian Personal Data Act, consent represents a "freely given, specific and informed declaration by the data subject to the effect that he or she agrees to the processing of personal data relating to him or her". As expected, the requirement for a "free, specific and informed" consent is identical with the requirement found in the Belgian Data Protection Law – discussed above.

The requirement of a "free" manifestation of will has also been discussed above. Authoritative academic commentary on the Norwegian law considers that refusal to consent to the data processing should not result in negative consequences or sanctions.[173] Consent should not be mandated by someone in a position of superiority, such as an employer or a public authority. Moreover, the Data Protection Tribunal has held that the requisite freedom of consent did not exist in a case where bank loan applicants were forced to "consent" to their personal data being registered in a central "loan registry".[174] The requirement should not, however, be interpreted as a prohibition against attaching an advantage to the consent, such as, for example, the possibility of benefiting from an Internet presence via the registration of a domain name.

The consent should also be specific. There should be no doubt that the consent was in fact given (regardless of any prerequisite about its form) and what scope it has. The applicant for a domain name under .no gives consent by signing and submitting a "self-declaration form" ("egenerklæring"), which becomes part of the ensuing contract with Norid.[175] The text linked with the consent given by the applicant for collection of personal data and the provision of WHOIS service states: "the contact information and the time for registration of the domain will be made public among others through WHOIS database of Norid. Access could also be given through other Internet technologies".[176]

om at han eller hun ikke vil at behandlingen skal gjennomføres eller fortsette, bør dette tillegges vesentlig vekt").

173 Dag Wiese Schartum & Lee A. Bygrave, *Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger* (Bergen: Fagbokforlaget, 2004), p. 131.

174 Case 2003-01.

175 As noted earlier, the applicant for a .no domain name can only be a legal person (as of the time of writing). Thus, strictly speaking, such an applicant does not have to be accorded the consent-related and other safeguards mandated by the Personal Data Act. Nevertheless, data on some applicants (particularly small companies) may well qualify as data on natural/physical persons, thus bringing the processing of the data under the ambit of the Act.

176 Translation made by NORID and available at <http://www.norid.no/navnepolitikk.en.html#link15>. The Norwegian text states: "Kontaktinformasjon og registreringstidspunkt for domenet gjøres offentlig tilgjengelig på internett, blant annet gjennom Norids WHOIS-database. Tilgang vil også kunne bli gitt via andre internett-teknologier".

Simply comparing the manner in which the determination of scope of consent is made in the .eu WHOIS policy, it is apparent that the .no policy is much broader and looser. If public access is given "among others" via the WHOIS database and that "access could be given through other Internet technologies", one may wonder how, to whom and for what purposes the access is given. The specificity requirement is also not fulfilled considering that the provision of WHOIS service , as discussed in Chapter 2 (section 2.2) of this report, does not have a very clear purpose (being expressed as a non-exhaustive list of possible legitimate uses of the data). In the current formulation, the applicant's consent may encompass a broader range of activities than an applicant in good faith may foresee. Although some clarification can be obtained from the information published by Norid on the website, the documents are intended only to provide information and are not included in the binding agreement between the registry and the registrant. Since it is the registry that "determines the purposes and the means of the processing", a more explicit and a more transparent formulation of the consent would not only validate and legitimise the processing, but it would also contribute to the overall goal of a fair data-processing activity.

The third prerequisite of a valid consent is that it should be informed. As discussed above, Directive 95/46/EC imposes on the data controller the obligation to provide information to the data subject. This obligation is transposed in section 19 of the Norwegian Data Protection Act. The controller must provide "on its own initiative" information about:

a) the name and address of the controller and of his representative, if any
b) the purpose of the processing,
c) whether the data will be disclosed and if so, the identity of the recipient,
d) the fact that the provision of data is voluntary, and
e) any other circumstances that will enable the data subject to exercise his rights pursuant to this Act in the best possible way, such as information on the right to demand access to data, cf. section 18, and the right to demand that data be rectified, cf. sections 27 and 28.

Information regarding the name of the data controller is provided to the registrant in the Domain Name Policy for .no. The purpose of the data processing in the .no policy has already been discussed in Chapter 2 of this study. Norid's choice to exemplify legitimate uses rather than formulate an overall purpose of the database represents a hindrance to a proper assessment of whether the potential applicant is truly informed about the scope of the data processing involved in the provision of WHOIS service. The registry maintains that the consent is given in order to make the domain and the associated information

publicly available on the Internet.[177] It can be argued, however, that making information publicly available on the Internet represents a means by which to achieve a purpose (for example, to guarantee that technical problems are rapidly resolved), but not a purpose in itself.

Although the law does not require a particular degree of detail in the specification of purpose, a high information threshold should be considered. This is in light of the fact that the aim is to provide the applicant with all data relevant for giving informed consent, and that, due to the specificity of the processing, this information is not available elsewhere.

Although the registry mentions the need to collect data in an internal database and the fact that this database is only accessible to Norid and "ensures efficiency and quality to the registration services it provides",[178] it is not at all clear what this information will be used for and under what terms the data will be transferred to third parties.[179] The evaluation of whether all the information is necessary and sufficient cannot be made in a satisfying way without the purpose of the collection being clearly stated.

The registry provides information about how the information collected will not be used – i.e., it will not be used for "sale, transfer to third parties, marketing and other commercial purposes". The data in the WHOIS database, however, will be made publicly available and this entails a high risk of misuse. In addition, given that the registry will admittedly give access to registrant data "through other Internet technologies", the registry provides information about the technical measures in place to prevent misuse of the public WHOIS data.[180] However, as long as there is uncertainty about the circumstances in which the personal data will be released, it is difficult to assess whether these technical measures are sufficient.

177 The relevant part of the policy states: "I samtykket som avgis ligger at formålet er å gjøre domenet samt tilhørende informasjon offentlig tilgjengelig på Internett".

178 The Norwegian text states: "Databasen er nødvendig for å sikre effektivitet og kvalitet i driften av Norids registreringstjeneste".

179 The Norwegian text states simply that the database is used "til å holde oversikt over samtlige registrerte domenenavn under .no-domenet samt annen teknisk og praktisk informasjon tilknyttet disse".

180 The Norwegian text states: "Hvert søk logges med informasjon om hvor søket foretas fra. Dersom en adresse som det søkes fra har en oppslagsaktivitet som overstiger definerte grenser, blokkeres eller begrenses videre søk fra adressen inntil aktiviteten avtar et nivå som kan aksepteres".

4.2.2 Other legal grounds

Although consent is the central and, to the extent that it is valid, sufficient means to permit data processing, the registry for the .no domain lists three other reasons justifying its right to process registrant data. These are: (i) "the need to fulfil a contract to which the data subject is party"; (ii) "to protect the interests of the subscriber"; (iii) "to perform a task in the public interest". They all fall under the category of "necessary processing" according to the Norwegian Personal Data Act. As Schartum and Bygrave point out, these alternatives are so broadly formulated by the law that at least one of them will justify almost any processing activity.[181] Since the majority of processing operations do not necessitate a prior license from the Data Inspectorate, it will be up to the controller in most cases to claim convincingly that the foreseen processing operations are "necessary".

Firstly, there is an intrinsic element of consent in the existence of a contract between the data subject and the data controller. However, where the contract is brought in to legitimise a data-processing operation, the data processing must be intrinsic and essential to the contractual obligations assumed by the parties – for example, if data processing is necessary in order to ensure payment for services that the processor provided to the data subject. The object of the contract between the registrant and the registry is registration of the domain name and provision of registration services. The WHOIS service is provided not only in the interest of the data subject and in the framework of the registration contract,[182] but also with regard to other, extra-contractual interests of third parties. In this perspective, although the terms of the contract bind the registrant (because he/she/it has agreed to it) by virtue of contractual law principles, the contract does not necessarily legitimise a processing activity carried out in disregard of the data processing principles. In effect, even though the registrant agreed via binding contract to have the personal data processed "for any purpose the controller may find appropriate", the processing would still not be legitimate according to the data processing principles.

Secondly, the .no registry maintains that the data-processing operations are legitimised by the interest "to protect the interests of the subscriber" ("for å ivareta abonnentenes interesser"). It is unclear whether Norid in this respect invokes the provisions of section 8(c) of the Personal Data Act, referring to the "vital" interests of the data subject. The notion of "vital" may mean "necessary for the continuation of life" or "having or affecting life". Recital 31 in the preamble to Directive 95/46/EC refers in this context to "processing carried out in order to protect an interest which is essential for

181 Schartum & Bygrave, *Personvern i informasjonssamfunnet*, *op. cit.*, p. 135.

182 See the explanations given in the discussion about the freedom of consent in Belgian law.

the data subject's life". Despite the advantages the registrant may have from registering a domain name and from having their data made available on the Internet, it is nevertheless obvious that section 8(c) does not apply here, being more suited for data processing in a medical or health services context.

Finally, the .no registry claims that the "performance of a task in the general interest" (viz. section 8(d) of the Personal Data Act) legitimises the data-processing operations it carries out. While the wording of section 8(d) is, on its face, broad, the intention of the legislator was that it is only meant to apply to processing activities carried out for archiving, statistical, historical or scientific purposes.[183]

To sum up, given the nature of the data processing envisaged by Norid in providing WHOIS services, the valid consent of the applicants represents the necessary and sufficient legal ground for permitting the processing.

4.3 The features of a legally compliant processing of personal data via WHOIS service – a best practice framework

The registries for the .no and the .eu domains legitimise their data processing operations in the context of the provision of WHOIS service through having obtained a valid consent from the applicant, through the claim of fulfilling the terms of a contract with the registrant, or through the claim of carrying out a task in the public interest. Irrespective of which motives represent the legal basis for the processing, the operations carried out by the registry from the moment data are collected until they are deleted or made anonymous must fulfil a series of requirements. Directive 95/46/EC lays down these requirements, among others, in Article 6 (data quality), Article 12 (access rights), Article 14 (right to object), Article 17 (security of processing), and Article 18 (notification of supervisory authority). The requirements embody (at least) eight core principles of data protection law. These principles may be summed up in terms of "fair and lawful processing", "minimality", "purpose specification", "information quality", "data subject participation and control", "disclosure limitation", "information security" and "sensitivity".[184] Considering the analytical and pragmatic approach of this report, and the basic distinction between legal basis (which legitimises data processing) and legal requirements for processing (which dictate how the processing operations should be organ-

183 Ot.prp. nr. 92 (1998–99), p. 109.

184 See further Bygrave, *Data Protection Law*, *op. cit.*, chapters 3 and 18.

ised in accordance with the law), this section aims at presenting and assessing the conditions imposed by the applicable law on:

- the processing routines defined by the data controller in achieving the envisaged purpose (treatment of personal data);
- the interaction of the controller with the data subject throughout the processing (treatment of the data subject); and
- the automated information system (security).

Admittedly, the three classification criteria overlap in many instances. For example, the analysis of the personal data management requirements is indirectly also an analysis of the functioning of the information system which is implemented in order to put into practice the requirements. The treatment of the data subject is indirectly reflected by the manner in which the controller processes the personal data. However, in the opinion of the author, the classification reflects the three main types of interactions entailed by a processing activity: interactions among legal subjects (i.e., the data controller and the data subject),[185] interactions among the controller and the personal data which is entrusted to it by the data subject, and interactions of the controller with its own systems, which it designs for the purposes of processing the personal data in accordance with the targeted goal.

Subsequent to mapping the relevant legal obligations, current WHOIS policies are examined in order to identify some best practices in the main processing operations specific for the provision of WHOIS service: collection, use for internal purposes, public display, access by and transfer to third parties. While the best practice analysis is not exhaustive, it may serve as a starting point in building a common European view about the provision of WHOIS service, with an increased power of persuasion in relevant international fora such as ICANN.

4.3.1 Personal Data Management

4.3.1.1 Legal requirements

Article 6(b) of Directive 95/46/EC requires that personal data be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". Moreover, processing "for statistical, historical or scientific purposes" will not be regarded as incompatible, provided the national law stipulates adequate safeguards. Furthermore, according to article 6(c)

185 Considering that the data processor interacts with the data subject within the limits of its mandate from the controller, this interaction is only incidentally discussed in this context.

of the Directive, personal data shall be "adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed".

The need to identify a specific, explicit and legitimate purpose of the processing has been analysed in two other sections of this study: firstly, in the context of identifying the purpose of WHOIS service; secondly, in the context of identifying what constitutes a valid consent that may permit data processing. This section discusses further the correspondence between the "declared" (i.e., not yet implemented) purpose of personal data processing and the collecting, use and transfer practices implemented by the controller in order to achieve the purpose.

The requirements of Article 6 of the Directive have been transposed into the Norwegian Personal Data Act in section 11(b), (c) and (d) and into the Belgian Privacy Law in Article 4(1) paragraphs 2 and 3. While the Belgian implementation reproduces the letter of the Directive, the Norwegian Act adds elements which facilitate the interpretation of the otherwise broad terms used by the Directive, setting more specific obligations for the controller during the personal data processing. The relevant provisions of section 11 of the Norwegian Act read:

> *The controller shall ensure that the personal data processed: […]*
>
> *b) is used only for explicitly stated purposes that are objectively justified by the activities of the controller,*
>
> *c) is not used subsequently for purposes that are incompatible with the original purpose of the collection, without the consent of the data subject,*
>
> *d) is adequate, relevant and not excessive in relation to the purpose of the processing, ….*

The three paragraphs of section 11 introduce a twofold relation of logical coherence: on the one hand between the purpose to be achieved and the processing operations carried out in the attainment of the purpose (storage, publication, transfer to third parties) and, on the other hand, between the stated purpose of the processing and the personal data requested from the data subject.

Purpose of processing operations

As noted above, section 11(1)(b) of the Norwegian Act requires that personal data be processed "only for explicitly stated purposes that are objectively justified by the activities of the controller". A controller cannot therefore process personal data for reasons that are objectively outside the scope of its activity. According to Norid's memorandum on "Use of information stored in

Norid's customer database",[186] the WHOIS database is to be used "for example by rightholders interested in controlling who is allegedly misusing their rights, or by the police, who can collect information in the context of investigations". Although these are legitimate uses of the database, they do not come under the object of activity of the registry. This does not mean that the interested stakeholders may not receive access via private agreements with the registry, upon justifying legitimate interests in specific data, or by virtue of the provisions of other laws. It does mean, however, that Norid cannot justify its processing of the personal data by invoking the possible usefulness of this information for third parties, because Norid does not have as a purpose of its activity to serve as an intermediary data provider between the data subject and a third party. The storage, publication and transfer of the personal data collected by Norid (via the registrars) from the domain name registrants should concern Norid's object of activity, that is, domain name administration and allocation under .no.

It may be argued that by consenting to the data processing, the registrant grants the registry permission to carry out processing operations which are not necessarily circumscribed to its own field of activity. It may be said that consent from the data subject in general may legitimise any kind of processing. However, in the case of WHOIS service, the registrant has in practice no possibility to opt out of having their data displayed publicly in the database. Given the low degree of freedom of the registrant in choosing to give this consent, I believe in this particular case that the consent of the data subject alone does not entitle the registry to carry out processing operations which are not necessarily circumscribed to its own field of activity.

Another issue to be assessed here is whether the processing operations are effective for achieving the desired purpose(s). More precisely, the issue involves the extent to which the collection and provision of free and unrestricted query-based access via the web serve the intended purposes of the WHOIS service. WHOIS service is provided, according to Norid, "in order to accommodate the legitimate interests of others, for example by allowing others:

- To check whether the domain name is available or registered;
- To find out information about who is responsible for a certain registered domain
- To check whether one's own registered information is correct or updated,
- To allow rightsholders to verify whether an infringement of their rights has occurred,
- To allow law enforcement actions by the police".

186 Referenced *supra* footnote 170.

The limitations of this definition are discussed in Chapter 2 (section 2.2) of this study. Following a query addressed to the WHOIS database, the following main clusters of personal data are displayed:

- Organisation handle;
- Legal contact handle;
- Technical contact handle – including a "person handle".

Every handle contains information about the name, the address, telephone number and e-mail address of the person in charge for the respective roles. In addition, other operational information is provided about the domain name and the servers used.

Up to the present, Norid only accepts applications for registration from legal persons. Arguably, the roles of legal, technical or organisational point of contact for a legal person may be regarded as limited to one's professional obligations and regulated by the employment agreement. Even so, considering that making available information in a public database with free and unrestricted access may represent the most privacy-invasive processing practice, devoid of adequate guarantees and exposing the personal data to the broadest possible range of uses and misuses, it would be advisable for the registry to provide a clearer justification for why the maximum amount of information collected is displayed regardless of who requests such access and why it is requested.

If a layered access model were implemented, the information provided by the registry could be customized according to the needs of the requestor and would give full effect to the requirement of the Personal Data Act that the minimum necessary and sufficient personal data be processed in the least privacy intrusive manner. The possible legitimate purposes of the WHOIS database, identified in Chapter 2 (section 2.2) of this report, are, in summary, to facilitate operability, transparency and accountability. Each of these functions may be adequately served by automated and free access to only a limited amount of personal data about the registrant, registrar or the domain servers. For example, the operative function of the WHOIS database justifies the publication of information about the technical contact point as well as information about the domain name servers, registrar, registration and expiration dates, but not necessarily about the domain name owner or the legal contact point. Law enforcement in a free and democratic society requires adequate guarantees for due process and rule of law. These could be better served if the information identifying the alleged perpetrator were made available to the enforcement authority and the request for additional, unpublished information were addressed directly to the registry and above all through mechanisms other than WHOIS. The registrant may check and request the update of their own personal data through a simple username and a password mechanism,

but this legitimate use of the database does not justify making all the personal information available to everyone. Similarly, those interested primarily in finding out whether the domain name is available (or possibly when the current registration is expected to expire) may not always have an interest (or, better yet, a claim) in finding out what the contact details of the different administrative, legal, technical contact points are.

In principle, according to section 11(1)(c) of the Personal Data Act, personal data collected for specific purposes cannot be used for other purposes than those initially given. Exceptionally, a change in the purpose may be accepted as long as the new purpose is not incompatible with the initial one. Given this rule, it is not advisable that the registry for .no specifies only a non-exhaustive list of possible interests that may be served by the publication of personal data via WHOIS service, as this choice would limit the possibility to process the data for other, unspecified uses. If the already collected personal data must be used for a new purpose, this purpose should be within the reasonable expectations of the data subject.[187] For example, whenever the controller has collected personal data in order to provide the data subject a benefit or an advantage, the use of the same data in a way that brings disadvantages to the data subject is arguably not in compliance with the rule in section 11(1)(c).[188]

Purpose of processing – need for personal data

The principles of minimality and purpose specification require that the personal data collected be adequate, relevant and not excessive in relation to the purpose of the processing. In other words, the data controller must be able to justify, at any point, the need for certain personal data in order to achieve one or more of the purposes for processing. For example, the information about the technical contact point facilitates an interested party's obtaining information that would make possible the technical co-ordination and inter-operation of specific delegations within the registration and the DNS. While it is true that the assignment of responsibilities and the distribution of roles within a legal entity exceed the scope of competence of the domain name registry, the latter has – in its role as policy and decision maker in the relevant ccTLD – the competence to define in very clear terms the scope of the roles of legal, technical or administrative points of contact. Moreover, the registry is the only actor

187 See further Bygrave, *Data Protection Law*, *op. cit.*, p. 340.

188 See too Schartum & Bygrave, *Personvern i informasjonssamfunnet*, *op. cit.*, p. 137. It should be admitted, however, that law enforcement purposes are exempted from this limitation.

with enough information about, and overall view of, the functioning of the ccTLD to provide guidance as to what kind of queries fall within the scope of each of the roles, by reference to the purposes it aims to have achieved through collecting that particular information from the applicants. Such guidance from the registry would prove useful to both the registrants and their designated representatives, and it may arguably create a more standardised and predictable response to inquiries from the relevant contact point, increasing the reliability of contacting it. What may also be achieved through this approach is a more informed consent of the applicant to the data processing as well as a more customised access of, and display to, the information resource needed by a certain requestor.

Once the necessary and sufficient data have been collected, the Personal Data Act requires the controller "to ensure" that the data are "accurate and up-to-date, and are not stored longer than is necessary for the purpose of the processing" (section 11(1)(e)). The registrar (as data controller) could fulfil this obligation, for example, by sending regular reminders about what data are registered in the database and with an affirmative confirmation that the data are still accurate, as well as by implementing (or requesting the registrars to implement) economically reasonable checks on the accuracy of the data provided upon registration, for example by cross-referencing the data with information stored in other public databases. In this way, the registry has a constructive approach by facilitating the provision of accurate data rather than merely applying sanctions for provision of incorrect data. Nonetheless, it will necessarily be the registrant that has the main responsibility for providing accurate contact information in the first place and for providing updates to the registered data – as is the case under the Domain Name Policy for .no (sections 14.3 and 14.4).

According to the Personal Data Act, in respect of inaccurate or incomplete data, "the controller shall on his own initiative or at the request of the data subject rectify the deficient data" (section 27(1)). Section 14.5 of the Domain Name Policy for .no stipulates the obligation of the applicant to "reply to queries from Norid regarding the continued accuracy of the registered information. The applicant must then document the information provided". The provision introduces another possible type of active control by the registry of the accuracy of the data provided by the registrant. Such a control could take place when the registry receives a complaint of inaccuracy, or at regular intervals.
According to the Domain Name Policy for .no, the sanction for a non-responsive contact or for providing incorrect information by or on behalf of the applicant is the compulsory deletion of the domain name. Deletion of incorrect data, however, is not the only possible remedy for inaccurate personal data pursuant to the Personal Data Act. Paragraphs 2, 3 and 4 of section 27 lay

down other measures that can be implemented in the event the data processed are incomplete or inaccurate. The law indicates that the "rectification of inaccurate or incomplete personal data which may be of significance as documentation shall be effected by marking the data clearly and supplementing them with accurate data" (section 27(2)). Alternatively, "if weighty considerations relating to protection of privacy so warrant, the Data Inspectorate may … decide that rectification shall be effected by erasing or blocking the deficient personal data" (section 27(3)). Moreover, "[e]rasure should be supplemented by the recording of accurate and complete data. If this is impossible, and the document which contained the erased data therefore provides a clearly misleading picture, the entire document shall be erased" (section 27(4)).

According to section 28(1) of the same legislation, personal data collected by the registry should not be stored "longer than is necessary to carry out the purpose of the processing. If the personal data shall not thereafter be stored in pursuance of the Archives Act or other legislation, they shall be erased". The subsequent storage of personal data, however, may be justified for "historical, statistical or scientific purposes, if the public interest in the data being stored clearly exceeds the disadvantages this may entail for the person concerned" (section 28(2)). In such a case, "the controller shall ensure that the data are not stored in ways which make it possible to identify the data subject longer than necessary" (section 28(2)).

The registry for the .no domain declares in its memorandum on "Use of information stored in Norid's customer database" that although the WHOIS database publishes only the information last updated at the moment of the request, all the data which were provided to it at a certain point will be stored in its *internal* database(s) for an indefinite period. The registry justifies the retention of "historical information about the domain name and the corresponding (personal) data" by referring to, *inter alia*, the need to "be able to document the history of the domain name in case disagreement should occur about the right to a domain name". The registry also refers to the retention as occurring for "statistical purposes". The registry further claims that the permanent storage of personal data and domain-related information is in conformity with the purpose of the database. However, as noted above, section 28(2) of the Personal Data Act requires that such data (insofar as they are "personal data" under the Act) be stored in a form which does not allow identification of the data subject(s).

It would be advisable for the registry to explain why the permanent storage of personal data serves the purpose of the database – that purpose being stated as one of "making the domain and the corresponding information publicly available on the Internet" – where, admittedly, only the information that is valid (updated) is made available by the WHOIS database. Where a

contractual relation exists, the personal data may be retained for as long as the contractual relation exists. The general rule is that personal data should be deleted when they no longer serve the purpose for which they were collected.

As already noted, the registry justifies its choice for a permanent retention of the personal data through invoking first of all the need for evidentiary documentation where a conflict may occur. The general rules of evidence would seem, though, to indicate that the party making a claim must also provide the evidence on which it bases the claim. Should such a need occur for the registry, the general three-year time limitation ("foreldelsesfrist") for claiming rights limits the need for documenting rights which were not exercised during that time.[189]

The permanent retention of the personal data is also justified by the need to maintain statistical evidence about the evolution of the domain name system over time. It may be useful for the registry to provide information – either on its own initiative or following requests for access – on the the routines it has implemented in order to hinder the identification of the data subject based on the data.

Registries are not the only actors processing the registrant's personal data. In agreement with a registry, a multitude of accredited registrars may receive applications for registration from individuals and companies interested in having an internet presence. The domain name policies for .no and .eu do not restrict the possibility of registrars being located abroad (including outside Europe). As a consequence, it is possible that a domain name registration involves transfer of personal data to a country outside the EU/EEA – i.e., a "third country" in the understanding of Chapter IV of Directive 95/46/EC. According to Article 25(1) of the Directive, "the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if … the third country ensures an adequate level of protection". However, Article 26(1) and (2) provides a number of alternative derogations from the adequacy requirement in Article 25.

The Directive does not directly clarify the meaning of the term "transfer" of personal data in such a context. Neither does the Norwegian Personal Data Act, which transposes the requirements of Articles 25–26 in its Chapter V. A question arises whether a transfer of personal data occurs during the registration of a domain name when registrant/applicant data are sent to registrars located in a third country without an adequate level of data protection. Although technically speaking a transfer does take place, it is arguable that Articles 25–26 should be read down to concern only the situation when transfer is facilitated by a controller (or processor acting on behalf of a controller) as opposed to the

189 See Limitation Period for Claims Act 1979 (Lov av 18.05.1979 nr. 18 om foreldelse av fordringer (foreldelsesloven)).

data subject (the domain name registrant/applicant being the latter). Certainly, the bulk of authoritative commentary on these rules seems to presume that they pertain primarily if not exclusively to data export by controllers.[190] Even if they do not, the transfer may be permitted under one or more of the criteria provided under Article 26 of the Directive, particularly Article 26(1)(a) ("the data subject has given his consent unambiguously to the proposed transfer") or 26(1)(b) ("the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request") or 26(1)(c) ("the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party").

As for the subsequent transfer of registrant data from the registrar to the registry, this involves transfer of personal data from a third country to an EU/EEA state. Such transfer is not caught by the rules in Articles 25–26 as those rules deal only with transfers *from* EU/EEA states *to* third countries.

However, how is one to treat the publication by the registry of the registrant data in its WHOIS database? Does such publication amount to a transfer of personal data to a multitude of third countries, given that the database – being accessible via the Internet – can be potentially accessed by entities based all over the world? The European Court of Justice has held, in the case of *Lindqvist*, that publication of personal data on an Internet website that is potentially accessible from around the globe does not necessarily amount to a transfer of personal data falling under the rules in Articles 25–26.[191] In such a situation, it would seem that there will only be a transfer (in terms of Articles 25–26 and national rules transposing these provisions) if the controller posting the data to the website does so with the intention of actively transmitting the data to entities in third countries. Kuner argues persuasively that "the best and safest interpretation of *Lindqvist* is that making personal data available on the Internet can be viewed as a kind of data transfer if it involves granting access to the data of other parties (such as employees, customers, etc) on a large scale and for business purposes".[192] Arguably, such access is facilitated by the WHOIS services of European-based registries. Thus, there are strong grounds for treating, say, EURid's WHOIS database on .eu registrants as involving data

190 See, e.g., Chris Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford: Oxford University Press, 2007, 2nd ed.), chapter 4; Peter Blume, *Retlig regulering af internationale persondataoverførsler* (Copenhagen: Jurist- og økonomforbundets forlag, 2006), espec. p. 35.

191 Case C-101/01, *Bodil Lindqvist*, European Court Reports 2003, I-12971, especially paragraphs 61, 68 and 70. Note that the court restricted its decision on this particular point to the situation where the server hosting the website is located in the EU/EEA.

192 Kuner, *European Data Protection Law*, *op. cit.*, p. 156.

transfers falling under the Article 25–26 regime. Nevertheless, such transfers might still be justified under one or more of the derogations provided in Article 26. There are two possibly pertinent derogations here. One is based on data subject consent (Article 26(1)(a). However, such consent must be unambiguous, informed and voluntary. Some of these criteria may be difficult to fulfil. The criterion of "informed" undoubtedly requires the data subject to be given information that the data registered on them in the WHOIS database may be transferred to jurisdictions without adequate levels of data protection.[193] Given the limited amount of information made available on the .no registry's website (and the associated documents) on whether/to what extent and under which guarantees personal data are transferred to third countries, it is questionable whether the consent given by an applicant for a .no domain may be considered sufficiently informed and specific.

Another possibly pertinent derogation is when the transfer "is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public or by any person who can demonstrate legitimate interest ...." (Article 26(1)(f)). However, the latter derogation may not be relevant if it means that the register must have been established pursuant to statute or regulations – WHOIS databases do not usually have a statutory basis. If, though, the provision is to be construed as requiring only that the actual public access to the register be statutorily permitted – for example, under general legislation on access to information – then it might cover access to WHOIS databases. It is not certain which way the provision is to be construed. This uncertainty pertains also to the equivalent provision in the Norwegian Personal Data Act which formulates the derogation in terms of the situation where "there is statutory authority for demanding data from a public register" (section 30(1)(h)).

Regarding the other grounds for processing, reference should be made to Section 2 of this Chapter, explaining their scope and clarifying their meaning.

4.3.1.2 Best practices

Various ccTLDs provide adequate solutions of compliance with the legal requirements identified in this section. Although the local conditions may differ from one ccTLD to the other, the examples provided below may serve as a best practice model for other interested ccTLDs. The examples provided in this section are, of course, not exhaustive.

193 See also Dag Wiese Schartum & Lee A. Bygrave, *Utredning av behov for endringer i personopplysningsloven* (Oslo: Justis- og politidepartementet, 2006), chapter 8 and references cited therein.

In describing the legal requirements for the management of personal data collected in the WHOIS database, the benefits of a layered access to WHOIS data were exemplified. Currently, the layered access to the public, web-based WHOIS database is implemented either by distinguishing between most frequent purposes of access (for example, to check whether the domain name has been registered before) or for distinguishing the nature of the registrant (natural/ legal person).

In the first category, Nominet, the registry for .uk, provides several types of services allowing different types of queries to its WHOIS database:

- WHOIS search:[194] This displays the information collected about domain names that are currently registered, including registrant's details, registration date and current status, registrant's agent and the name servers associated with the domain name. The basic WHOIS search can be used for checking the availability of a domain name or for finding out the registrant's details for a domain name that is already registered.
- WHOIS 2 service:[195] This enables WHOIS gateways/proxies to query WHOIS database without being blocked for excessive use. It is only to be used as a gateway for end users who are making a live WHOIS query. It is designed in such a way that anti-abuse mechanisms can recognise and block users attempting to abuse the systems by using multiple gateways. The interested parties may use an online application form and must accept specific terms and conditions before being allowed to use the service.
- Domain Availability Checker (DAC):[196] This is available to Nominet registrars who are also members (subscription-only basis). The service enables one to make high–volume queries about the availability of domain names. Once connected to the DAC, one or many domain name queries may be sent to the system. The DAC is able to accept high volumes of queries because it reduces the amount of information it returns to the requester and it authenticates only once, at the point of connection.
- Public Register Search Service (PRSS):[197] This allows one to search the register for domain names that are registered to a particular legal entity and/ or of a similar name. The PRSS is accessible via a web interface and allows searches using wildcards. A maximum of 21,000 results can be viewed per week. These results can be viewed in batches.

194 See <http://www.nominet.org.uk/other/WHOIS/>.
195 See <http://www.nominet.org.uk/other/WHOIS2/>.
196 See <http://www.nominet.org.uk/other/dac/>.
197 See <http://www.nominet.org.uk/other/prss/>.

For each service, the registry for .uk domain specifies the eligibility criteria, the fees, application procedures and their terms and conditions and, of course, the activities for which the service may useful.

Another example is the .name gTLD for which the WHOIS service supports two types of free queries (no password required) and two types of password protected queries.[198] In the first category:

- Summary WHOIS queries provide very limited information, such as whether a domain name exists and its registration status;
- Standard WHOIS queries about domain-name registrations provide more information, including registrar ID, registrant ID, admin ID, technical ID, billing ID, Nameserver ID, Creation Date, and Expiration Date. No personally identifiable data relating to the registrant are available from this query.

In the second category, the following types of queries are restricted to those who have received a user-name and a password from the .name registry:

- Detailed WHOIS queries will return more extensive contact information (not including e-mail addresses or phone and fax numbers) about registrants. Administrative, technical, or billing contacts that are the same as the registrant contact will not be separately displayed. Upon completing an application for Detailed WHOIS searches, an applicant will receive five passwords, each of which is effective for one Detailed WHOIS search only. A fee of USD 2 may be charged for the five passwords. To acquire a password, users must agree (via a click-through license) not to use the data for marketing purposes, spamming, or other improper or unlawful purposes.
- Extensive WHOIS queries will return more extensive contact information than Detailed WHOIS queries. Information about e-mail forwarding registrations may be obtained only through Extensive WHOIS queries. To receive a persistent password and continuous, free access to the Extensive WHOIS data, a requestor must enter into a written contract with registry Operator.

Other ccTLD registries manage the registrant's personal data by providing different public display options for registrants who are natural persons and those that are legal persons. For example, clause 2.4 of the .eu WHOIS policy specifies:

198 See .NAME Agreement Appendix 5: Whois Specifications (15.08.2007), at <http://www.icann.org/en/tlds/agreements/name/appendix-05-15aug07.htm>.

> *"Where the registrant is a private individual (natural person) the registrant contact information published is restricted to the e-mail address, unless they request otherwise. Natural persons who apply for a .eu Domain Name will be explicitly informed by their registrars of the possibility to create and use a specific functional email address for publication in WHOIS as an alternative to the use of their personal e-mail address. All other information collected will only be kept for internal use."*

The policy states too that this information will not be disclosed to third parties unless the registry is ordered by a judicial authority within the European Community to grant such access. Access to third parties will also be provided following an individual request for the disclosure of these data through filing a special application form.

Other ccTLD registries allow the display of a smaller amount of data for both natural and legal person registrants if certain special circumstances apply. For example the .nl registry allows the registrants to request that their personal data be exempted from inclusion in the public part of WHOIS database.[199] They are asked to justify the request by identifying a concrete and real interest compelling them to opt out. This real interest may be documented, for example, by showing that a report has been filed with the police or that other precautions have been taken to protect their own identity, or that the same personal data are protected by other bodies or organisations. A case-by-case evaluation will be made by the registry following the receipt of a "special circumstances" opt-out request.

The principles of minimality and purpose specification require that the minimum amount of personal data that is necessary for the fulfilment of the stated purpose is collected from the data subject. Delegates of the main Internet stakeholder groups, represented in the GNSO, have long attempted to reach consensus on defining the scope of WHOIS databases. Additionally, extensive debates took place on how this purpose could be achieved while displaying a lesser amount of personal data than now required by the Registrar Accreditation Agreement. After the decision of the GAC to restrict the purpose of the WHOIS database to the provision of information "sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS nameserver", two proposals were submitted in order to minimise the amount of information displayed by WHOIS database.

---

199 See General Terms and Conditions for .nl Registrants (version 14.07.2008), clause 22.3, available at <http://www.sidn.nl/ace.php/p,728,5693,368340178,AV_houders_UK_pdf>.

The one proposal, termed the "Operational Point of Contact Proposal" (OPoC) suggests that every registrant be required to designate a new operational contact which would replace the administrative and technical point of contact. Following a request, WHOIS service would display the full contact details (name, address, telephone, e-mail address etc.) of the operational point of contact but only the name and the country of the registrant. The role of Operational Point of Contact could be filled by the registrant self, by the registrar or by a third party in a consensual relation with the registrant. The role would be associated with three functions:

- to relay a request to the registrant;
- to reveal unpublished data about the registrant;
- subject to the prior agreement of the registrant, to provide a remedy.

In the event the OPoC does not fulfil its functions, the requestor may contact the registrar to reveal the registrant's WHOIS data, to suspend the domain name record or website, to lock the domain for transfer.

Requestors with a legitimate interest may obtain data directly from the registrars. Regular query-based access to un-displayed data records would be provided only upon reasonable evidence of actionable harm. Law enforcement agencies investigating or prosecuting illegal activity may receive full access to both the displayed and undisplayed data records.

Despite some support for this proposal,[200] the level of agreement necessary for turning it into a consensus policy was not reached. Nonetheless, for the purposes of the present discussion, the proposal reveals important points of reflection for ccTLD registries that are trying to design a privacy-compliant WHOIS policy:

- the need to display less information about the registrant;
- the need to define clearly the purpose of WHOIS service;
- the need to define clearly and to provide guidance regarding the status and the obligations of the point of contacts designated by the registrant as well as mechanisms for remedy in case the points of contact do not fulfil their obligations;
- the need to provide mechanisms for access to un-displayed data records upon proof of legitimate need.

The other proposal suggested during the consensus-building process at gTLD level was the Special Circumstances proposal. The proposal is based on the idea that there are indeed few registrants who are using the domain names for

200 See *Final Outcomes Report of the WHOIS Working Group 2007* (20.08.2007), <http://gnso.icann.org/drafts/icann-whois-wg-report-final-1-9.pdf>.

purely non-commercial purposes or who have a legitimate need for private registration due to the nature of the service they provide (shelters for abused women, drug rehabilitation centres). Given proper notice of special need, these categories of registrants may benefit from private registrations.

The disadvantage of this proposal is that it makes the data protection system optional rather than imposing a general rule of fair and justifiable processing of personal data. The proposal, however, acknowledges that special groups of registrants may require a different regime for processing personal data.

The reform of WHOIS database policy, in my opinion, should not necessarily involve the replacement of the existing contact points and the definition of new ones. The effectiveness of the database in responding to the legitimate needs for information of the stakeholders could be achieved as well via a proper definition of the existing contact points and through reaching agreement as to the type of response that is expected of them following a request.

A best practice example of an attempt to explain the role of the designated contact points is the .de ccTLD.[201] It defines the contact points in addition to displaying their personal data:

- "The domain holder is DENIC's contractual partner and hence holds the material rights to the domain".
- "The administrative contact (admin-c) is the natural person appointed by the domain holder to act as his/her authorized representative and who also has the duty towards DENIC of taking binding decisions in all matters concerning the domain access.de".
- "The zone administrator (zone-c) supports the name servers of the domain access.de".

Difficulties may arise where the registration of the domain name involves transfer of personal data from the registrant to a registrar located in a country which does not ensure an adequate level of protection of the data (but is nevertheless accredited by the registry). Article 9 (Privacy Policy) of the .eu Registrar Agreement stipulates the obligation of the registrar to "maintain a clear privacy policy, compliant with all applicable national, European and international data protection regulations, and to inform his registrants thereof." Since the registrar may be located anywhere, the registry provides clarifications as to which country's privacy rules should be followed by the registrars in their data-processing activities:

a) if established within the European Economic Area, the registrar must comply with the applicable data protection legislation in force in the Member State in which the registrar is established and indemnify and

201 See <http://www.denic.de/webWHOIS/info>.

hold EURid harmless against any third party action due to violations of such data protection laws in relation to the performance of this Agreement.

b) if established within a country outside the European Economic Area which has been declared as ensuring an adequate level of protection by reason of its domestic law or of the international commitments it has entered into by a European Commission decision taken under Article 25(6) of Directive 95/46/EC, must comply with the applicable data protection legislation in force in the jurisdiction where the registrar is established and indemnify and hold EURid harmless against any third party action due to violations of such data protection laws in relation to the performance of this Agreement.

c) if based within a country which does not meet the conditions set out in (a) or (b) above, must comply with the standard contractual clauses adopted under the European Commission Decision 2002/16/EC of 27 December 2001 and indemnify and hold EURid harmless against any third party action due to violations of such contractual provisions in relation to the performance of this Agreement.

d) if based in the United States of America the registrar must:

- adhere to the Safe Harbor Privacy Principles issued by the US Department of Commerce, giving adequate information thereof to EURid, and indemnify and hold EURid harmless against any third party action due to violations of such provisions in relation to the performance of this Agreement; or
- adopt the contractual provisions set out in (c) above, and indemnify and hold EURid harmless against any third party action due to violations of such contractual provisions in relation to the performance of this Agreement.

4.3.2 Data subject management

A core principle of data protection laws is that persons should be able to participate in, and have a measure of influence over, the processing of data on them by other individuals or organisations.[202] The principle manifests itself through: (a) rules which aim at making people aware of data processing activities generally; (b) rules aimed at making people aware of the basic details of the processing of data on themselves; and (c) rules which allow persons to object to others' processing of data pertaining to them and to demand that

202 See further Bygrave, *Data Protection Law*, *op. cit.*, chapters 3 (section 3.6) and 18 (section 18.4.5).

these data be rectified or erased insofar as the data are invalid, irrelevant or illegally held.[203]

4.3.2.1 Legal requirements

Ultimately, the principle requires the data controller to permit the data subject to become an active and aware participant in the processing of data about themself. The data subject's active involvement may translate as their right to have information about the processing and as their right to influence, under certain conditions, how the processing of information about them takes place.

In accordance with section 18 of the Norwegian Personal Data Act, any person has the right to obtain general information about the identity of the controller, the purposes of the processing, whether personal data will be disclosed, and if so to whom. The information is usually available on the website of the controller, easily accessible to any party interested in finding it. However, in addition to this general right of access, the data subject has in accordance with section 24 of the Personal Data Act, a right to demand that the data controller inform them in writing no later than 30 days after receipt of the (written and signed) inquiry, about (a) the categories of data concerning the data subject that are being processed, and (b) the security measures implemented in connection with the processing insofar as such access does not prejudice security. The data subject may demand that the controller elaborate on the general information provided by the data controller online, to the extent that this is necessary to enable the data subject to protect their own interests.

Norid stipulates in section 14.1 of the Domain Name Policy for .no that it is the duty of the applicants to familiarize themselves with the relevant legislation and with the rules that describe the registration process and policies. Moreover, in assisting the domain name applicants with completing the registration application, the registrar is given the responsibility to inform them about the applicable rules and policies. Usually the registrars only provide a link to Norid's web pages containing the Domain Name Policy for .no; the registrar cannot, therefore, be regarded as a source of additional information for the registrant.

No reference is made in the Domain Name Policy, however, about the possibility of a registrant's request for more information from the registry directly (as data controller) about the processing operations involving its data, as required by section 18 of the Norwegian Personal Data Act, and the obligation of the registry to reply to such queries. Queries may occur especially where the

203 *Idem.*

registry facilitates transfers of personal data to third parties or while storing personal data beyond the duration of the registration agreement.

The obligation to provide upon request information about the processing operation involving data about the data subject represents a prerequisite for a relation of trust between the controller and the data subject. The individual right of access may be used by the data subject as a starting point for a request for deletion, correction or update of the data according to section 27 of the Personal Data Act. In the event the processing is based on the consent of the data subject, and the data subject has doubts about the necessity of the data collected for the purposes specified or has doubts about the processing practices, the data subject may choose to withdraw the consent or request that the extent of the processing be reduced.

4.3.2.2 Best practices

The information consulted concerning the registration policies and practices of the ccTLD and gTLD registries up until the present time has not revealed best practice examples of the obligation to respond to data subjects' requests for supplementary information about the processing operations involving their own personal data. It may be assumed that the registrants may contact the registry directly by using the contact details provided on the website or by directing their requests via the registrars for any claims or requests.

4.3.3 Confidentiality and security of processing

4.3.3.1 Legal requirements

Article 17 of Directive 95/46/EC states that controllers "must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing". These measures are to be taken "both at the time of the design of the processing system and at the time of the processing itself" (recital 46). Furthermore, controllers should "ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected" (recital 46; cf. Article 17).

Sections 13 and 14 of the Norwegian Personal Data Act transpose the above provisions with some elaborations. They require both the data con-

troller and the data processor to implement "planned, systematic measures" in order to ensure a "satisfactory" level of confidentiality, integrity and accessibility in processing personal data (section 13). Moreover, any controller who allows other persons to have access to personal data (e.g., a processor or other persons performing tasks in connection with the data system) shall ensure that the said persons fulfil the same requirements that the controller himself must fulfil according to the law. The security measures taken shall be documented by both the data processor and the data controller and the documentation shall be made available to their own employees and to the Data Inspectorate and the Privacy Appeals Board (section 14). A similar obligation of documentation is imposed with respect to measures to ensure the quality of personal data (section 14).

The Belgian Data Protection Act contains similar provisions regarding the obligation of the data controller to ensure the confidentiality, integrity and accessibility of the personal data. Neither that Act nor the Norwegian Act is very specific about the kind of initiatives (organisational, technical) that should be taken in compliance with the law. The Belgian legislation, however, stipulates that the measures should cover protection against "accidental or unauthorised destruction, accidental loss, as well as against alteration of, access to and any other unauthorised processing of personal data" (Article 16(4)). And the security requirements of the Norwegian statute are elaborated in Chapter 2 of the Regulations issued pursuant to the Personal Data Act.[204] Furthermore, both the Norwegian Data Inspectorate and the Belgian Privacy Commission have issued documents explaining the standards of security that should be respected by the data controllers and by those processing data on their behalf.[205]

Without analysing in detail these documents, it is important to emphasise in the present context the scope of the controller's obligations to ensure the security of the systems used for processing personal data. The Norwegian Data Inspectorate underscores that, in accordance with section 13 of the Personal Data Act, the controller is responsible not only to safeguard its own systems, but also to make that the information security of its "communication partners" ("kommunikasjonspartnere") and "suppliers" ("leverandører") is satisfactory. The notion of information security is here broadly understood

204 Regulation No. 1265 of 15.12.2000 on processing of personal data (Forskrift om behandling av personopplysninger), available in English at <http://www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/POF_eng_v2.pdf>.

205 The explanatory comments of Norway's Data Inspectorate (issued December 2000) are available at <http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/SV100_00.pdf>. The Belgian Privacy Commission has released in 2001 reference measures on information security, available in French at <http://www.privacycommission.be/fr/static/pdf/mesures-de-r-f-rence-vs-01.pdf>.

as encompassing confidentiality, integrity and availability of the data. The Inspectorate states that a "satisfactory level of information security" is obtained whenever planned and systematic measures are taken in accordance with the state of the art. Although it is not possible to make an *a priori* assessment of what the specific security measures should be, they should be put in place following an objective evaluation of the security threats that may be present, given the nature and the purposes for which personal data are processed. The document describes in detail the obligation of the controller to make and document risk assessments in order to identify security threats, the likelihood and possible consequences of their occurrence, to reconsider this assessment periodically and to document situations where the policies, organisational measures and technical mechanisms were used in disregard of the agreed routines. Routines for ensuring confidentiality and availability are also set as the responsibility of the controller. Similar routines and rules are formulated by the Belgian Privacy Commission.

According to the self-declaration which must be signed by the applicant for a .no domain, the applicant consents to the fact that the registry cannot be held accountable by the applicant for any direct or indirect prejudice resulting from system errors or system interruption at Norid which is caused by circumstances or relations that are not under its control.[206] The scope of the .no registry's limitation of liability would be better understood by the applicant if had been accompanied by clear information regarding what circumstances or relations are indeed under the control and responsibility of the registry. According to the Domain Name Policy for .no, "Norid denies all responsibility for misuse of the information which is made public via WHOIS database". However, the provisions of the Personal Data Act, analysed in this section, would seem to indicate otherwise. In its capacity as a data controller, the registry has the legal obligation and the technical ability to implement adequate measures to prevent or to hinder, to the best of its abilities, the misuse of the data entrusted to it for the specifically agreed purposes.

By publishing the personal data of the domain name registrant and of its contact points, the registry exposes those data to a multitude of possible uses and misuses. While the registry cannot be held directly liable for a third party's misuse of the data, the registry has the stipulated obligation to implement technological and organisational measures in its systems so that all those with a legitimate interest in the data can access these data while the risk of misuse

206 The Norwegian text is as follows: "Søkerorganisasjonen aksepterer herved at Norid ikke kan holdes ansvarlig overforsøkeren for noen direkte eller indirekte skade som følge av driftsfeil eller driftsstans hos Norid som er forårsaketav forhold eller omstendigheter som Norid ikke kontrollerer".

of the data is minimised to the extent made possible by the state of the art, in the light of a systematic risk analysis.

In 2007, ICANN's Security and Stability Advisory Council completed an empirical study of four TLDs (.com, .info, .de and .org) in an attempt to find out whether WHOIS data are a source of spam and if so, which technical measures would best prevent the misuse of WHOIS data for spam purposes.[207] To accomplish this task, the SSAC conducted an experiment to see the effects of two services offered currently by registrars to protect registrant e-mail addresses from publication and abuse. SSAC found that the data collected from the WHOIS database were, indeed, one of the many sources for spam. However, technical measures implemented by the database owner could significantly reduce the misuse of the data. SSAC distinguished between two classes of technical measures currently used by the registrars to prevent the automatic collection of WHOIS data:

- Forms of protection that they term "Protected-WHOIS", including measures through which "web user interfaces challenge the querying party with a visual display and prompt for a response that is not easily automated" (CAPTCHA, anti-scripting, IP rate limiting);[208]
- Forms of protection that they term "Delegated-WHOIS" and that focus on protecting the email addresses of registrants, including measures through which the registrars substitute their own address details in the registrant fields when the domain name is queried using WHOIS.[209]

The findings of the SSAC study reveal both the need and the usefulness of an active involvement by WHOIS database owners in the protection of the personal data published via WHOIS. Among the findings:

- For an e-mail address that is not published anywhere other than WHOIS, the volume of spam delivered to e-mail addresses included in registration records is significantly reduced when Protected-WHOIS or Delegated-WHOIS services are used. Moreover, the greatest reduction in the delivery of spam to e-mail addresses included in registration records is realized when both of the protective measures are applied.
- Of the two forms of protective measures registrants can obtain through registries/registrars, the Delegated-WHOIS appears to be somewhat more effective than Protected-WHOIS.

207 SSAC, *Is the WHOIS Service a Source for email Addresses for Spammers?* (SAC023, October 2007), available at <http://www.icann.org/en/committees/security/sac023.pdf>.

208 *Idem*, p. 17–18.

209 *Idem*, pp. 18–20.

4.3.3.2 Best practices

The above-mentioned SSAC study represents to date the only reliable empirical study testing the effectiveness of implementing security measures in the WHOIS database and in the provision of WHOIS service. The study examines the practices currently employed by a number of registrars to protect the public WHOIS data against illegitimate use and especially automated collection. The SSAC

> *"observes that registrars offer a variety of "protection" services including "WHOIS Spam Catcher" service, e-mail masking, and proxy registration services. Evidently, a market exists for the sale of services that protect e-mail addresses from open publication in various locations, including WHOIS. Registrars also offer anti-abuse and anti-spam measures to registrants who purchase these services".*[210]

The study revealed that the volume of spam received by e-mail addresses displayed by WHOIS databases which were neither protected by "Delegated-WHOIS" nor "Protected-WHOIS" measures was "extraordinarily large compared to all study cases where one or multiple protection services were used".[211] When a domain name is registered at a registry/registrar that offerred "Protected-WHOIS" without "Delegated-WHOIS", the study indicated it was possible to achieve two orders of magnitude enabling better defence against spam.[212] When a domain name is registered at a registry/registrar that did not offer "Protected-WHOIS" but offered "Delegated-WHOIS", the study indicated it was possible to achieve three orders of magnitude enabling better defence against spam.[213] When a domain name is registered at a registry/registrar that offered "Protected-WHOIS" and "Delegated-WHOIS", the study indicated it was possible to achieve nearly four orders of magnitude enabling better defence against spam.[214]

Currently, neither the .eu nor the .no ccTLDs give registrars the possibility of offering "Delegated-WHOIS" services, despite the proven benefits. According to the .eu Registrar Agreement, during the registration process, the registrar must

---

210 *Idem*, p. 20 (footnote references omitted).
211 *Idem*, p. 25.
212 *Idem*, p. 26.
213 *Idem*, p. 27.
214 *Idem*, p. 28–29.

"always submit (including but not limited to any submission in WHOIS database) the data of the registrant who made the initial request for the Registration of the Domain Name(s) concerned and not his own data. The email address submitted in the contact information will be that of the registrant only and not that of the registrar, unless the registrant expressly requests that the registrar's email address be submitted. After the Registration process, the registrar must ensure that the data in WHOIS database is at all times the data of the registrant, and not his own data."

However, the WHOIS Policy for the .eu domain includes several safeguards for preventing misuse of WHOIS data. According to section 2.5 of the Policy,[215]

(i) All who submit a WHOIS query will be provided with an automatically generated random code which they must type in before receiving the answer to their query. Providing the code in the form of a picture rather than text will prevent easy automation of the system for data mining. Without entering the correct code, the only information available following a query will be whether the domain is available for registration or not.
(ii) E-mail addresses, and if published, postal addresses, telephone and fax numbers are displayed as images (pictures) rather than text making it difficult to automate capture of the data.
(iii) Multi-criteria searching and other search facilities to search by name, e-mail address, postal/street address, fax or telephone numbers will not be possible.
(iv) All those who submit a query to WHOIS database will first be required to read and agree to the 'WHOIS legal statement and terms and conditions' which will inform the user that:
a. WHOIS services are provided for information purposes only;
b. by submitting a query the user agrees not to use the information to:
1. allow, enable or otherwise support the transmission of unsolicited, commercial advertising or other solicitations whether via email or otherwise;
2. target advertising in any possible way;
3. cause nuisance to the registrant in any way by sending messages to them.

Given the fact that the .no ccTLD will be opened for natural person registrants, it would be advisable that one or several of these measures be implemented for that domain as well.

215 Available at <http://www.eurid.eu/files/whois_en.pdf>.

5 EFFECTIVE LAW ENFORCEMENT THROUGH A PRIVACY-FRIENDLY WHOIS DATABASE

For the past five years, the international Internet community has been struggling to reach consensus on the most appropriate policies for the provision of WHOIS service, policies that would replace an inertia regulation of WHOIS service with a system of norms and practices acknowledging and taking due account of the interests of the users, providers of domain name services, of the international IP associations, governments and law enforcement. Some progress has been reached at gTLD level throughout this period by agreement on the "WHOIS marketing restriction policy" and "WHOIS data reminder policy" – each of which is dealt with earlier in this report. Intensely debated issues such as the purpose of the WHOIS database, the amount of personal data to be publicly displayed, and the procedures for access to un-displayed WHOIS data, have remained controversial and the subject of considerable disagreement. The general lack of consensus at gTLD level, however, has resulted in the preservation of the regulatory status quo. In other words, the existing WHOIS specification policy imposed by ICANN on the gTLD registries and accredited registrars through bilateral agreements remains in force, despite numerous objections to its provisions raised by international fora.[216]

In parallel, the ccTLD managers face the challenge of trying to adapt a policy similar to the gTLD model to the realities of their national legal framework and to the needs of the local internet community. As described earlier in this report, the various ccTLD managers (registries) have implemented several models for the management of the WHOIS database that are applicable within the limits of their territorial competence. This approach has nevertheless resulted in a fragmented reflection of the European Internet stakeholders' interests, arguably to the detriment of the persuasiveness of their arguments during negotiations with their non-European counterparts.

One of the major hindrances in reaching international consensus about WHOIS service is the perceived antithesis between privacy and accountability. Given the increase in frequency and in scope of the misuses of the domain

---

216 See, e.g., EU Article 29 Data Protection Working Party, *Opinion 2/2003 on the application of the data protection principles to the Whois Directories* (10972/EN/final, WP76, 13.06.2003); ICANN's Non-Commercial Users Constituency, *Comments to ICANN from Commissioners and Organizations Regarding WHOIS and the Protection of Privacy* (not dated), <http://www.ncdnhc.org/policydocuments/whois-ncuc-backgrounder.pdf>.

name system, it is strongly claimed that an absolute transparency of the system users would arguably deter further attempts at abuse and would ensure a more rapid and effective intervention of law enforcement agencies in identifying and prosecuting those who infringe the law.[217] The supporters of this claim opine that since the European data protection framework argues for the reduction of the amount of personal data collected and displayed publicly to the minimum necessary and sufficient for reaching specified purposes, law enforcement would suffer an undue hindrance, especially where cross-jurisdiction enforcement actions are needed. This "zero-sum game" would require either the safeguarding of the interests of society by sanctioning unlawful behaviour or the protection of the interests of private individuals in benefitting from an internet presence without incurring the risk of overexposure of their personal data to an unlimited number of receivers and as many potential uses.

The lesson learned from the past five years of intense and considerably unfruitful debate is that by arguing only one side of the two interests, both end up being inadequately safeguarded. The central aim of WHOIS reform should be to ensure that the individual's privacy is dully attended to while at the same time allowing law enforcement agencies a possibility to exercise their authority and accomplish their duties in an efficient manner. Rather than pitting these two against one another as antithetic goals, more emphasis should be placed on a privacy-friendly WHOIS policy that will increase the accuracy of the WHOIS database and at the same time minimise the possibility for abuse of the data made available to the public.

Directive 95/46/EC encourages EU/EEA Member States to introduce rules for the processing of personal data "with the view of facilitating the data flow between them" (Recital 8 in the preamble). The privacy rules, therefore, should not be regarded as a hindrance to the communication of personal data, but rather as a facilitator of such flows, obviously within the scope of the legal guarantees examined in Chapter 4 of this study.

Law enforcement may have an interest in the data publicized in the WHOIS database because the information contained in it might reveal the link between an online behaviour or activity and the natural or legal person bearing the legal responsibility for it. In some cases, legal rules may apply to require that certain actors reveal their identity when interacting with clients or consumers. This is the case, for example, with providers of information society services pursuant to Article 5 of the E-Commerce Directive.[218] In some instances, a

217 The claim typically put forward by ICANN's Commercial and Business Users Constituency and its Intellectual Property Interests Constituency.

218 Article 5 of the E-Commerce Directive (Directive 2000/31/EC, referenced *supra* note 78) requires the service provider to "render easily, directly and permanently accessible to the

domain name is registered for speculative or law-infringing purposes or it is subsequently used to the detriment of IP rights holders, consumers, or society as a whole. Provided that the information in it is accurate, the WHOIS database may be the only source providing the necessary evidence between the online activity and the offline identity of the responsible party. It is, therefore, in society's interest that criminals do not find in online activities a safe haven for behaviour that would otherwise expose them offline to liability. Additionally, cross-jurisdictional law enforcement should be facilitated by rapid access to information and rapid exchange of relevant intelligence between the competent enforcing authorities.

The privacy framework does not impede the processing of personal data for law enforcement purposes. According to Article 13 of Directive 95/46/EC, EU/EEA Member States may introduce derogations from the data protection regime where such measures are necessary to safeguard, inter alia, "(a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions".

This exception constitutes the legal basis for organising the processing of personal data by the competent law enforcement authorities, in accordance with the material and procedural national rules. However, Article 13 should not be interpreted expansively so as to permit extensive processing operations by bodies other than law enforcement agencies, in the general "public interest". While law enforcement agencies may process (have access to, transmit, collect, use) personal data under a preferential regime, other data controllers should

---

recipients of the service and competent authorities, at least the following information:
(a) the name of the service provider;
(b) the geographic address at which the service provider is established;
(c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;
(d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;
(e) where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority;
(f) as concerns the regulated professions:
- any professional body or similar institution with which the service provider is registered,
- the professional title and the Member State where it has been granted,
- a reference to the applicable professional rules in the Member State of establishment and the means to access them;
(g) where the service provider undertakes an activity that is subject to VAT, the identification number referred to in Article 22(1) of the sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonisation of the laws of the Member States relating to turnover taxes - Common system of value added tax: uniform basis of assessment(29)."

abide by the letter of the national laws transposing the Directive. According to Jay, public interest will not necessarily justify widespread publication:

> *"The obligation to the particular individual may be set aside by reason of an overriding public need. Even when disclosures have been held to be in the public interest this would not permit publication of information to the world, but only to the appropriate authorities who investigate the matter".*[219]

The access of law enforcement agencies to personal data (as well as their processing of personal data within the scope of their authority) must, however, respect fundamental human rights. Article 8(2) of the European Convention of Human Rights stipulates that there "shall be no interference by a public authority with the exercise of" the right to respect for private life (laid down in Article 8(1)) "except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

Since the national criminal procedure laws become applicable when crimes are committed through or against a data system,[220] in designing policies for access and use by the law enforcement to the data WHOIS database, the ccTLD managers must take due account of the national laws. While the general issue of access by law enforcement to personal data (or to registries containing personal data) exceeds the scope of this report, selected aspects of this issue are taken up in this chapter due to the guidance they provide for registries in designing effective routines for access by the competent enforcement authorities to unpublished WHOIS data.

A fundamental distinction should be made concerning whether the request for access for law enforcement purposes comes from a public law enforcement authority (such as the police) or from a private or rightsholder organisation interested in claiming rights directly from the alleged infringer without recourse to the state enforcement authority. In the former case, the enforcement authority has, by virtue of its statutory mandate, a general right to investigate and prosecute unlawful behaviour, which may argue in favour of implementing a general right of query-based access for enforcement authorities. In the latter case, the interest in protecting the privacy of the domain name registrant may

219 Rosemary Jay, *Data Protection Law and Practice* (London: Sweet & Maxwell, 2007, 3rd ed.), p. 214.

220 See generally Bert-Jaap Koops & Susan W. Brenner (eds.), *Cybercrime and Jurisdiction – A Global Survey* (The Hague: T.M.C. Asser Press, 2006).

argue in favour of a case-by-case evaluation of the concrete circumstances in which the request is made as well as of the supporting documentation brought in as justification for the access request.

Regardless of the chosen implementation of the special right for access for law enforcement purposes, the request should be subjected to a proportionality test based on three criteria. First, it should be evaluated to what extent the initiative of request for additional information is appropriate in reaching the purported goal. Secondly, information motivating the recourse to this database should be provided. If the requestor already has access to the same information from other sources, then the request for access may not be justified. Thirdly, it should be assessed whether the importance of the goal to be achieved reasonably justifies access to the information. This assessment involves a weighing of different interests (the economic interest of the registry as private entity who is under an obligation to provide the information, the interest of the data subject in privacy as well as the interest of law enforcement). In this assessment it will be relevant to determine, inter alia, how invasive the obligation to provide information would be for the data subject.

These considerations can be elaborated using Norwegian law and practice as the point of departure. According to section 199a of the Norwegian Criminal Procedure Act,[221] "[w]hen conducting a search of a data-processing system, the police may order everyone who is dealing with the said system to provide the information necessary for gaining access to the system". Under section 199, therefore, the registries may be under an obligation to provide, upon request, the necessary information to the law enforcement authority. The scope of this legal provision may be determined by providing an answer to the following questions:

1. Which authority, according to the national law, is competent to impose an obligation to provide information?
2. What elements ensure that such a request is legitimate?
3. What and how much information must be provided?
4. What sanctions do the registries face if they refuse to fulfil their obligation?

In relation to the first of these questions, in Norway it is the police who are competent to mandate an obligation to provide information. According to Norway's Official Reports (Norges Offentlige Utredninger (NOU)) No. 27

221 Act No. 25 of 22.05.1981 (as amended). The Norwegian title is Lov om rettergangsmåten i straffesaker (straffeprosessloven). An unofficial English version of the legislation is available at <http://www.ub.uio.no/ujur/ulovdata/lov-19810522-025-eng.pdf>. In the following, quotations (in English) from the Act are based on this translation.

of 2003, the decision to designate this authority as competent was dictated by practical reasons: the need for information arises in most cases during police investigations.[222] When the object of the search is a computer system, it is imperative to intervene without delay in order to prevent relevant data from being lost, destroyed or prevent the suspect from getting time to obliterate traces of activity and abandon, for example, the domain name. On the one hand, the obligation to provide information is in tension with the general right against self-incrimination as laid down in section 230 of the Criminal Procedure Act.[223] However, a court of law (which might be considered as a possible alternative to impose the same obligation) does not have enough overview of the logistics of the investigation to be able to anticipate the need for additional information. Unnecessary delay could be envisaged in a situation where the court may be expected to reach a decision on the request to provide additional information.

Regarding question 2, a request from the police to provide information in support of an ongoing investigation is legitimate only if made in accordance with the law. The criteria for making the request for information legitimate are similar in principle with those legitimising any data processing. From the perspective of the nature and general purpose of police work, however, these criteria may be broadly interpreted.

The obligation of any data controller to process data only for the purposes for which they were/are collected (or for compatible purposes)[224] should be broadly interpreted in the context of law enforcement. According to Norway's Official Reports No. 21 of 2003, the various processing activities undertaken by the police on the information collected should be regarded as compatible with the initial purpose of collection as long as those purposes remain within the scope of their field of competence and attributions.[225] This interpretation would allow, for example, the information collected for investigative purposes in a concrete case to be used for the more general purpose of crime prevention.

Furthermore, in the context of police work, the minimality rule in Article 6(1)(c) of the Data Protection Directive[226] should be interpreted in accordance

222 See generally NOU 2003:27, *Lovtiltak mot datakriminalitet*, chapter 3.

223 *Idem*, section 3.4.3.2.

224 Cf. Article 6(1)(b) of Directive 95/46/EC which stipulates that "[p]ersonal data must be … collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes".

225 NOU 2003:21, *Kriminalitetsbekjempelse og personvern – politiets og påtalemyndighetens behandling av opplysninger*, chapter 4.

226 Article 6(1)(c) stipulates that "[p]ersonal data must be … adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed".

with the context in which the request for information was made: the relevance of the information to an ongoing investigation may be more narrowly determined than when information is collected as a preventive measure in the general context of crime prevention. In any case, though, despite wide latitude in interpretation of the somewhat discretionary criteria of the law, the constraint to provide information imposed by the police should be regarded as a last resort in the case when alternative, less intrusive measures could not be taken. This follows too from the proportionality principle – elaborated further below.

In the specific context of this analysis (namely, the extent to which the police may impose on a registry or registrars an obligation to provide information), it may be argued that the police may obtain at least part of the information registered in the WHOIS database from other databases, with a higher degree of accuracy than WHOIS. In addition to making full use of their own registries, the police have the competence and authority to search in many other registries which are not directly under their control. In Norway, the most important external registries to which the police have access are:

- The National Register (Folkeregisteret (FREG))[227] which includes names, dates of birth, current addresses, places of birth, citizenship as well as previous entries in the same fields, for all Norwegian residents. Moreover, the identities of the parents, children and spouse as well as, if applicable, previous spouses are connected to each of the entries. There is no electronic coordination or exchange of information between FREG and the police registries. However, the Central Criminal Record Registry (Det Sentrale Straffe- og Politiopplysningsregisteret) is continually updated with information from FREG about deceased persons.
- The Driver and Vehicle Licensing Agency (Biltilsynets Autosys) includes information about all registered motor vehicles in Norway and their owners. Information is supplied electronically to Autosys from the Search registry (Etterlysningsregisteret (Elys) and the Schengen Information System (SIS) about vehicles which have been reported as stolen.
- The police also have access to some of the Brønnøysund registers, including the European Register of Business Enterprises (Foretaksregisteret) and the national Property Register (Eiendomsregisteret). However, no information is electronically transferred from one registry to the other.

Given the already broad access rights of the police to external databases, it may be questioned to what extent police access to the information in the WHOIS registry is imperative for the investigations when the same information may be obtained more reliably from other sources. Whether the registry

227 FREG – tidligere Det sentrale personregister (DSP)).

should introduce routines allowing a case-by-case evaluation of each request for access or whether it should introduce an access mechanism through which the police may access all the information recorded about a certain domain name depends on a concrete cost-benefit evaluation at the registry level. This evaluation should take into account historical data about the volume or the likelihood of receiving such requests from law enforcement authorities during a given interval of time.

Regarding the third question, section 170a of the Norwegian Criminal Procedure Act lays down a general proportionality principle with respect to coercive police measures: such a measure "may be used only when there is sufficient reason to do so. The coercive measure may not be used when it would be a disproportionate intervention in view of the nature of the case and other circumstances". This principle applies also to the obligation to provide information under section 199a. Thus, a person may only be required to provide the information sufficient to obtain access to the data system (and implicitly to the information it contains). In Norway's Official Report No. 27 of 2003, it is submitted that it would be sufficient to provide the access codes enabling the police to access the information searched, and that it should not be necessary to provide (or legal to request) a means by which to access the exact data sought after by the police. Furthermore, it cannot be required to provide information which does not concern the data system (or the part of it which is under the scope of the search warrant).[228]

Finally, regarding question 4, the refusal of a registry to provide the police with the information requested would be sanctioned with a fine, according to section 339(1) of the Norwegian Criminal Code. It is relevant, however, to underscore that the sanction applies only when the request for information comes from a competent law enforcement authority (in this case the police) and not from private entities (e.g., rightholders' organisations). In contesting the access control routines implemented by the registry, the latter should be advised to employ the usual routines for law enforcement, with the notification of the competent state authorities.

At the EU level, legislation has recently been adopted that lays down special data protection provisions for the police and judicial sector. This legislation takes the form of the Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[229] Due to limitations of time and other resources, it has not been possible to analyse the provisions of this new instrument in detail. It suffices to note that its legislative history has been

228 NOU 2003:27, *Lovtiltak mot datakriminalitet*, section 6.2.
229 O.J. L 350, 30.12.2008, pp. 60–71.

protracted and marked by a great deal of controversy and disagreement.[230] The basic purpose of the Framework Decision is to provide, for the EU, a comprehensive, coherent and common set of data protection rules for the processing of personal data by police and judicial authorities in criminal matters – such rules having been hitherto absent given that the general Data Protection Directive (95/46/EC) does not cover that sector. While the Framework Decision is directed primarily at EU Member States, it is also relevant for the EEA Member States and Switzerland insofar as it develops and elaborates the provisions of the Schengen acquis (to which the latter states are party).[231]

The basic data protection rules laid down by the Framework Directive build on the standards set by Directive 95/46/EC and the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data,[232] without seeming to depart significantly from them. Of greatest importance for this study are the provisions of Article 3 which lay down the criteria for law enforcement agencies to gain access to, and further process, personal data held by private parties. Article 3 is as follows:

1. Personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected. Processing of the data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected.
2. Further processing for another purpose shall be permitted in so far as:
   (a) it is not incompatible with the purposes for which the data were collected;
   (b) the competent authorities are authorised to process such data for such other purpose in accordance with the applicable legal provisions; and
   (c) processing is necessary and proportionate to that other purpose. […].

230 For an overview of the legislative history, see <http://www.europarl.europa.eu/oeil/file.jsp?id=5279032>.

231 See Recitals 45–7 in the preamble to the Framework Decision. However, the Framework Decision is stated as not affecting the relevant set of data protection provisions governing the functioning of Europol, Eurojust, SIS (Schengen Information System), CIS (Customs Information System) as well as those introducing the direct access for the authorities of Member States to certain data systems of other Member States (Recital 39).

232 ETS No. 108; adopted 28.01.1981; in force 01.10.1985.

On its face, Article 3 would seem not to introduce rules that will fundamentally change the current ability of European law enforcement agencies to access data in a WHOIS database. The same would seem to pertain for the other provisions of the Framework Decision. However, as indicated above, there has not been sufficient time to carry out an extensive and detailed analysis of these provisions, so the assessment offered here is necessarily tentative.

Finally, while the registry and the registrars accredited to provide registration services under .com make available on the Internet all the personal data collected about the domain name registrants (therefore special access control mechanisms for law enforcement purposes are not necessary to be implemented), the entity (public or private) interested in acquiring more information than publicly displayed about a natural person registrant in the .eu ccTLD must fill out a special request form.[233] This form should be submitted by the interested party to the registry via one of the accredited registrars. In fact, as described in Chapter 4, the ccTLD registries that have implemented layered access to their respective WHOIS databases provide public and private entities the opportunity to enter into a registration agreement and receive access for legitimate reasons to supplementary data in addition to information provided freely within WHOIS database.

Although the implementation of such policies consumes more resources for the registry and more time for the entity making a claim against a registrant, they do attend to the privacy interests of the majority of law-abiding registrants. They are thus considered as another instance of best practice in this area.

233 http://www.eurid.eu/files/request_form_disclosure_personal_data_en.doc.

6 CONCLUSIONS

The main purpose of this research project on the WHOIS database has been to analyse and assess the workings of the WHOIS service against the backdrop of well-established legal rules in the fields of contract law, intellectual property, criminal procedure, and privacy and data protection.

Although the WHOIS service is provided for all national and generic TLDs, significant variations in the service exist. These variations partly reflect the fact that the service is supposed to serve a broad range of functions and respond to the legitimate interests of different groups of stakeholders. The analysis in this report shows that, according to current practices, the WHOIS service fulfils the following main functions:

1. it facilitates the operability of the DNS by allowing the network operators to contact each other in order to ensure efficient connectivity among networks;
2. it creates transparency about the domain name registrant and the domain (status, servers, registration and expiry dates, last update);
3. it facilitates accountability by providing to the law enforcement authorities evidence about the link between an unlawful behaviour and its legally responsible party.

These functions have been identified through examining the explanations given by different domain name administrators as well as by examining the claims of third parties with legitimate interests in receiving access to the information stored in WHOIS databases.

The domain name policies for the domains that are the focus of this analysis reveal great disparities in clearly defining the purpose of the WHOIS database. The domain name policy for .eu stipulates that the purpose of the WHOIS database is to "provide reasonably accurate and up to date information about the technical and administrative points of contact administering the domain names under the .eu TLD". Disclosure of personal data beyond what are made freely available through the WHOIS service may be justified for "legitimate purposes"; these, however, are not explicitly defined. The registry for the .no domain, Norid, defines its WHOIS database as "a searchable database which contains contact information about .no domains." Norid subsequently provides a non-exhaustive list of legitimate uses that can be made with the data published via WHOIS. The .no WHOIS policy exemplifies rather than defines the purpose of the service. At .com level, the impossibility to reach a consensus

about the purpose of WHOIS database has led to the compromise of introducing a functional definition which emphasises only the technical purpose of the database and its role in facilitating DNS operability.

Regardless of the manner in which the purpose of WHOIS service is defined, and irrespective of its components, it is essential that there is a high degree of accuracy of the data in the WHOIS databases. By examining the responsibilities of the registries, the registrars and the registrants in the examined domains, the report has identified several hindrances towards the achievement of accurate WHOIS databases. Firstly, there is a lack of clarity in the relevant rules as to what steps should be undertaken by registrars/registries in checking the accuracy of WHOIS data. Secondly, although registrants bear the primary responsibility for providing complete and accurate WHOIS data, they do not currently bear the costs of non-compliance, except in the event that the registration is cancelled and the domain is lost. Thirdly, access to WHOIS databases is free of charge. Consequently, registrars/registries bear the costs of any implementation of WHOIS service as well as the management policies for the WHOIS database. In the interest of maintaining a competitive business they have to transfer the incurred costs to the registrants, and their incomes are dependent on the number of registrants choosing their registration services over those of competitors. Their interest, therefore, is to provide an attractive service to the registrants, while keeping the costs for the provision of WHOIS service to a minimum. As noted above, the language of the relevant rules on accuracy is loose, and in the absence of any substantial best practice guidance, registrars have a high degree of discretion in terms of the measures to apply in investigating accuracy complaints. Given competition, a registrar with relatively strict policies on accuracy runs the risk of losing future profits from a registrant that they have chosen to exclude, without having an opportunity to compensate this loss through a better reputation.

In determining whether WHOIS databases qualify for copyright protection as an intellectual creation or whether their makers are entitled only to the acknowledgement of their legitimate economic interest in protecting the investment, certain factual elements have been underscored in Chapter 3 of the study.

- WHOIS databases include data about all registrants of domain names under a certain TLD. In this sense, upon collection of the data, no selection is made regarding the records to be included or not included in the database. Existing agreements impose the provision of this general service by all the accredited registrars, and accurate records of all the registrants should be maintained.
- The nature of the data to be collected about each registrant is mandated via agreements, and in this sense the information collected from registrars

and included in the database is similar regardless of the domain name. No creative selection of the contents occurs.

- The agreements do not mandate, for the time being, the display of WHOIS records in a standardised format. It is, therefore, still possible for the providers of WHOIS databases to use a certain degree of creativity as to the search and arrangement criteria of the records in the databases. The degree of creativity in the arrangement of the contents, however, would have to be determined by a court of law in each given case. The recent initiatives of ICANN aimed at ensuring the accuracy of WHOIS data nevertheless reveal a tendency to reduce rather than to encourage the creativity of the database providers, and to find appropriate standardised solutions at least in making WHOIS data publicly available following individual queries.

These elements would seem to indicate that the maker/controller of a WHOIS database may not claim copyright in the database, but only a *sui generis* protection in accordance with the national implementation of the Database Directive, if applicable.

At the same time, it is arguable whether in the specific case of WHOIS databases, copyright protection is an objective worth pursuing. It may not afford a higher or more sophisticated level of protection to the database owner than the *sui generis* / catalogue right. This thesis is supported by the fact that a lawful user of the database may perform both individual acts of access and multiple queries to the database under the same conditions in both regimes and that in all the three TLDs analysed here, access to the WHOIS database is free. In accordance with this thesis, several improvements of the copyright claim published by the domain name registry for the .no domain have been suggested.

The most extensive part of the research has been devoted to the analysis of the routines implemented by WHOIS database administrators in the protection of personal data processed during or as part of the provision of WHOIS service. Chapter 4 has examined the privacy policies issued by the registries for the .no and the .eu domains, as well as those imposed by ICANN on the accredited registrars. The analysis has focused on the main requirements of the European data protection laws and illustrated how they can be understood as guarantees that should remain paramount during the provision of WHOIS service. Irrespective of how the registry chooses to formulate the legal basis for the processing, the operations carried out by the registry from the moment data are collected until they are deleted or made anonymous must fulfil a series of requirements. The study suggests improvements in the practices for personal data management, data subject management as well as the maintenance of confidentiality and security of processing, based on examples which, in the opinion of the author, represent best practice models from selected ccTLDs.

Although the local conditions may differ from one ccTLD to the other, the examples provided may serve as a starting point in building a common European view about the provision of WHOIS service, increasing the clarity and power of persuasion of the layered access paradigm in relevant international fora.

Finally, Chapter 5 provides arguments in support of creating a layered access to WHOIS database, which would ensure that the individual's interest in privacy is dully accounted for while at the same time granting law enforcement agencies the opportunity to exercise their investigative authority and fulfil their duties in an efficient manner. Rather than setting legitimate access up against privacy preservation as separate, antithetical goals, more emphasis should be placed on the development of a privacy-friendly WHOIS policy that concurrently increases the accuracy of the WHOIS databases and minimises potential abuse of publicly available WHOIS data.

To sum up, the overarching argument of this report is that a clear definition of the purpose of data collection, rather than an identification of the individuals who may benefit from the data once they are made publicly available, is a prerequisite for formulating effective collection, access and transfer policies for such data. Furthermore, a clear definition would prevent uses different from or incompatible with the purpose for collection. Strict policy requirements can be derived from an explicit, well-defined purpose specification, so as to protect data from abuse.

While the attempt here to provide a multi-faceted view of the legal requirements for the management of WHOIS service has resulted in a series of conclusions and practical recommendations, it has only revealed the "tip of the iceberg" in the matter. It is desirable that similar studies be pursued in the near future and extended to other TLDs than simply .no, .eu and .com. Further research should be focused on contractual provisions and other legal mechanisms that may lead to a higher degree of accuracy of WHOIS databases as well as on the need, legitimacy and usefulness for access of law enforcement agencies to the personal data stored in the databases.

7 SELECT BIBLIOGRAPHY

Books, reports and journal articles

Beunen, A., *Protection for databases. The European Database Directive and its effects in the Netherlands, France and United Kingdom* (Nijmegen: Wolf Legal Publishers, 2007).

Blume, P., *Retlig regulering af internationale persondataoverførsler* (Copenhagen: Jurist- og økonomforbundets forlag, 2006).

Bygrave, L.A., "Determining Applicable Law pursuant to European Data Protection Legislation", *Computer Law & Security Report* [now Review], 2000, vol. 16, pp. 252–7.

Bygrave, L.A., *Data Protection Law: Approaching its Rationale, Logic and Limits* (The Hague /London/New York: Kluwer International Law, 2002).

Bygrave, L.A. & Bing, J. (eds.), *Internet Governance: Infrastructure and Institutions* (Oxford: Oxford University Press, 2009).

Derclaye, E., "Intellectual property rights on information and market power – comparing European and American Protection of Databases", *International Review of Industrial Property and Copyright*, 2007, vol. 38, pp. 275–98.

Edelman, B., "Large-Scale International Invalid WHOIS Data: A Case Study of 'NicGod Productions' / 'Domains for sale'" (02.06.2002), <http://cyber.law.harvard.edu/archived_content/people/edelman/invalid-whois/>.

EU Article 29 Data Protection Working Party, *Opinion 2/2003 on the application of the data protection principles to the Whois Directories* (10972/EN/final, WP76, 13.06.2003).

International Working Group on Data Protection in Telecommunications, *Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet*

(May 2000), available via <http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group>.

Jay, R., *Data Protection Law and Practice* (London: Sweet & Maxwell, 2007, 3rd ed.).

Koops, B-J. & Brenner, S. W. (eds.), *Cybercrime and Jurisdiction – A Global Survey* (The Hague: T.M.C. Asser Press, 2006).

Kuner, C., *European Data Protection Law: Corporate Compliance and Regulation* (Oxford: Oxford University Press, 2007, 2nd ed.).

OECD, *Cybersquatting: The OECD's Experience and the Problem it Illustrates with Registrar Practices and WHOIS System* (2002), <http://www.oecd.org/dataoecd/46/53/2074621.pdf>.

OECD Working Party on Telecommunication and Information Services Policies, *Comparing Domain Name Administration in OECD Countries* (DSTI/ICCP/TISP (2002)11/FINAL; 08.04.2003), <http://www.oecd.org/dataoecd/46/38/2505946.pdf>.

OECD Working Party on Telecommunication and Information Services Policies, *Evolution in the management of Country-Code Top-Level Domain Names (ccTLDs)* (DSTI/ICCP/TISP(2006)6/FINAL; 17.11.2006), <http://www.oecd.org/dataoecd/8/18/37730629.pdf>.

One World Trust, *Independent Review of ICANN's Accountability and Transparency – Structures and Practices* (London, March 2007), <http://www.icann.org/en/transparency/owt-report-final-2007.pdf>.

Schartum, D.W. & Bygrave, L.A., *Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger* (Bergen: Fagbokforlaget, 2004).

Schartum, D.W & Bygrave, L.A., *Utredning av behov for endringer i personopplysningsloven* (Oslo: Justis- og politidepartementet, 2006).

ICANN documents

Draft ICANN Procedure for Handling Whois Conflicts with Privacy Law (03.12.2006), <http://gnso.icann.org/issues/whois-privacy/whois_national_laws_procedure.pdf>.

Governmental Advisory Committee, "Principles and guidelines for the delegation and administration of country code top level domains" (Mar del Plata, 05.04.2005), <http://gac.icann.org/web/home/ccTLD_Principles.rtf>.

GNSO WHOIS Task Force, *Final Report on Accuracy and Bulk Access* (06.02.2003), <http://www.icann.org/en/gnso/whois-tf/report-19feb03.htm>.

GNSO Whois Task Force, *Final Task Force Report on the Purpose of WHOIS and of WHOIS Contacts* (15.03.2006), <http://gnso.icann.org/issues/whois-privacy/tf-report-15mar06.htm#0.1>.

GNSO Whois Task Force, *Whois Study Group Report to the GNSO Council* (22.05.2008), <http://gnso.icann.org/issues/whois/gnso-whois-study-group-report-to-council-22may08.pdf>.

GNSO Whois Task Force, *Final Task Force Report on WHOIS Services* (16.03.2007), <http://gnso.icann.org/issues/whois-privacy/whois-services-final-tf-report-12mar07.htm>.

GNSO Whois Working Group, *Final Outcomes Report* (20.08.2007), <http://gnso.icann.org/drafts/icann-whois-wg-report-final-1-9.pdf>.

ICANN's Whois Data Accuracy and Availability Program: Description of Prior Efforts and New Compliance Initiatives (27.04.2007), <http://www.icann.org/en/whois/whois-data-accuracy-program-27apr07.pdf>.

Security and Stability Advisory Committee, *WHOIS Recommendation* (SAC003, February 2003), <http://www.icann.org/en/committees/security/sac003.pdf>.

Security and Stability Advisory Council, *Is the WHOIS Service a Source for email Addresses for Spammers?* (SAC023, October 2007), <http://www.icann.org/en/committees/security/sac023.pdf>.

Requests for comments (RFCs)

RFC 812: NICNAME/WHOIS (March 1982), <http://www.faqs.org/rfcs/rfc812.html>.

RFC 954: NICNAME/WHOIS (October 1985), <http://www.faqs.org/rfcs/rfc954.html>.

RFC 1580: Guide to Network Resource Tools (March 1994), <http://www.faqs.org/rfcs/rfc1580.html>.

RFC 1591: Domain Name System Structure and Delegation (March 1994), <http://www.ietf.org/rfc/rfc1591.txt>.

RFC 3912: Whois Protocol Specification (September 2004), <http://www.faqs.org/rfcs/rfc3912.html>.

EARLIER REPORTS IN THE COMPLEX SERIES

CompLex er Senter for rettsinformatikks skriftserie. Serien startet i 1981, og det har blitt utgitt mer enn hundre titler. Bøkene i CompLex-serien kan bestilles fra Akademika (se bestillingsskjema bak i boken eller www.akademika.no).

2009

1/09 **Åpen programvare – noen rettslige problemstillinger**
Odd Randgaard Kleiva ..... *NOK 225,-*

2008

8/08 **Rett og rimelighet i moralsk belysning og andre grunnproblemer i norsk rettsliv**
Jens Petter Berg..... *NOK657,-*

7/08 **Vern av tekniske beskyttelsessystemer etter åndsverkslovens §53a**
Andreas Norum *NOK156,-*

6/08 **Grunnloven § 100 (4) som hinder for bruk av midlertidige forføyninger mot ytringer – med spesielt fokus på forestående, antatte opphavsrettskrenkelser**
Frederik Langeland..... *NOK132,-*

5/08 **Telekirurgi i et rettslig perspektiv – med spesiell vekt på etikk, samtykke og ansvar**
Bjørn Ivar Christie Østberg ..... *NOK 201,-*

4/08 **IT-støtte for arbeid med lovsaker**
Dag Wiese Schartum..... *NOK 144,-*

3/08 **Juristopia: Semantic Wiki for Legal Information**
Ole Christian Rynning ..... *NOK 243,-*

2/08 **Electronic Contracting in Europe. Benchmarking of national contract rules of United Kingdom, Germany, Italy and Norway in light of the EU E-commerce Directive**
Maryke Silalahi Nuth ..... *NOK 192,-*

1/08 **Internet search engines' collecting and processing of web pages – from the perspective of copyright law**
Ingvild Jørgensen ..... *NOK 165,-*

2007

5/07 **Gjennomgang av arkivretten**
Martin Rødland. ..... *NOK 129,-*

4/07 **Privacy & Identity Management**
Thomas Olsen, Tobias Mahler, et al. ..... *NOK 234,-*

3/07 **Personvern og transportsikkerhet**
Dag Wiese Schartum ..... *NOK 306,-*

2/07 **ZEBLEX 06 - Tre avhandlinger om fildeling, IT-sikkerhet og e-postkontroll**
Ida Otterstad, René Stub-Christiansen & Cecilie Wille Søvik ..... *NOK 348,-*

1/07 **Kontraktsregulering av domstolens kompetanse ved elektronisk handel**
Vebjørn Krag Iversen ..... *NOK 186,-*

2006

6/06 **Lover - fra kunngjøring til hyperstrukturer: to avhandlinger**
Per Marius Slagsvold & Kirill Miazine ..... *NOK 222,-*

5/06 **Retten til eget bilde**
Maria Jongers ..... *NOK 198,-*

4/06 **Legal, Privacy, and Security Issues in Information Technology Vol. 2**
Kierkegaard, Sylvia Mercado (editor) ..... *NOK 783,-*

3/06 **Legal, Privacy, and Security Issues in Information Technology Vol. 1**
Kierkegaard, Sylvia Mercado (editor) ..... *NOK 918,-*

2/06 **Rettslige reguleringer av informasjonssikkerhet**
Are Vegard Haug ..... *NOK 420,-*

1/06 **Anti-spam Legislation Between Privacy And Commercial Interest. An overview of the European Union legislation regarding the e-mail spam**
Dana Irina Cojocarasu..... *NOK 155,-*

2005

1/05 **Renessansen som unnfanget Corpus Iuris Civilis. Keiser Justinians gjenerobring av Romerriket**
Halvor Manshaus..... *NOK 249,-*

2/05 **Personvern og ytringsfrihet. Fotografering av siktede i straffesaker – et vern for ytringsfrihet?**
Anette Engum ..... *NOK 132,-*

3/05 **Rettigheter til geografisk informasjon. Opphavsrett, databasevern og avtalepraksis.**
Steinar Taubøll..... *NOK 206,-*

4/05 **"The Answer to the Machine is in the Machine" and Other Collected Writings**
Charles Clark..... *NOK 401,-*

5/05 **Digital Rights Management - Promises, Problems and Alternative Solutions**
Kristian Syversen..... *NOK 201,-*

6/05 **DRM og Demokrati. Argumentasjoner, rettferdiggjøringer og strategier bak endringen av åndsverksloven 2003-2005**
Jan Frode Haugseth ..... *NOK 224,-*

2004

1/04 **Opphavsrettslige problemstillinger ved universitetene og høyskolene. Innstilling fra immaterialrettsutvalget, oppnevnt av Universitets- og Høgskolerådet 31. januar 2000. Avgitt til universitets- og høgskolerådet 8. oktober 2003**
Immaterialrettsutvalget ..... *NOK 341,-*

2/04 **Ansvarsfrihet for formidler ved formidling av informasjonssamfunnstjenester**
Bård Standal ..... *NOK 311,-*

3/04 **Arbeidsgivers adgang til å kontrollere og overvåke sine ansatte med hovedvekt på grunnvilkårene for behandling av personopplysninger i arbeidslivet**
Stefan Jørstad..... *NOK 191,-*

4/04 **Elektroniske spor fra mobiltelefoner – om politiets bruk og teleoperatørenes lagring av trafikkdata.**
Christian Dahlgren ..... *NOK 117,-*

5/04 **International Jurisdiction and Consumers Contracts – Section 4 of the Brussels Jurisdiction Regulation.**
Joakim S. T. Øren ..... *NOK 172,50*

6/04 **Elektronisk dokumentfalsk.**
Lars Christian Sunde..... *NOK 60,502003*

2003

1/03 **IT i domstolene. En analyse av norske domstolers teknologianvendelse fra 1970 til 2001**
Even Nerskogen..... *NOK 330,-*

2/03 **Hvorfor vokser Norsk Lovtidend? En empirisk analyse av veksten**
Martin Støren..... *NOK 87,-*

3/03 **Etableringslandsprinsippet. En analyse av e-handelsdirektivet art 3 og prinsippet om fri bevegelighet av tjenester ved elektronisk handel**
Jon Christian Thaulow..... *NOK 213,-*

4/03 **The Law of Electronic Agents. Legal contributions to ALFEBIITE – A Logical Framework for Ethical Behaviour between Infohabitants in the Information Trading Economy of the Universal Information Ecosystem, IST-1999-10298**
Jon Bing and Giovanni Sartor (eds) ..... *NOK 351,-*

5/03 **LEA 2003: The Law and Electronic Agents Proceedings of the Second LEA Workshop, 24th June 2003, in connection with the**

ICAIL 2003 Conference (Ninth International Conference on Artificial Intelligence and Law), Edinburgh, Scotland, UK
Seminarrapport).....*NOK 228,-*

6/03 **Opphavsrettslige aspekter ved nettbasert formidling av musikk**
Stig Walle .....*NOK 153,-*

7/03 **Sceneinstruktørens opphavsrettslige stilling**
Edle Endresen.....*NOK 119,-*

8/03 **User-Centred Privacy Aspects In Connection With Location Based Services**
Christian B. Hauknes.....*NOK 203,-*

2002

1/02 **Koblingshandel og forholdet til fysisk og teknologisk integrasjon i relasjon til EØS-avtalens art.54(d)**
Ole Jacob Garder.....*NOK 180,-*

2/02 **To opphavsrettslige arbeider:**
Bjarte Aambø – Opphavsrettslige rettsmangler
Erlend Ringnes Efskind – Skjermbildets rettslige natur
Aambø / Ringnes Efskind.....*NOK 201,-*

3/02 **Arbeidstakeroppfinnelser ved universiteter og høyskoler. Innstilling fra et utvalg oppnevnt av universitets- og høgskolerådet 31 januar 2000. Avgitt til universitets- og høgskolerådet i oktober 2001**
.....*NOK 213,-*

4/02 **Utøvende kunstneres direkteoverføringer på Internett – med hovedvekt på kringkastingsbegrepet**
Irina Eidsvold Tøien .....*NOK 225,-*

5/02 **Administrasjon av radiofrekvensspekteret. Rettslige problemstillinger knyttet til telemyndighetenes forvaltning av frekvensressursene**
Øyvind Haugen .....*NOK 177,-*

6/02 **Overføring av personopplysninger til tredjeland. Kravet til tilstrekkelig beskyttelse etter EU-direktivet om personvern art. 25**
Mona Naomi Lintvedt og Christopher J. Helgeby.....*NOK 198,-*

7/02 **Digitale mellomledds ansvar for videreformidling av ytringer. E-handelsdirektivet art. 12-14**
Just Balstad.....*NOK 186,-*

8/02 **Platekontrakten. Eksklusive overdragelser av utøverens rettigheter til eksemplarfremstilling og spredning**
Øyvind Berge.....*NOK 237,-*

9/02 **Varemerkerettslige konflikter under .no. I hvilken grad kan registrering og bruk av et domenenavn medføre inngrep i en varemerkerett? Hvordan løses konflikter under .no i dag, og hva kan være en mer hensiktsmessig tvisteløsningsmekanisme i fremtiden?**
Silje Johannessen.....*NOK 192,-*

10/02 **Vegard Hagen – Pekeransvar. Spørsmålet om ansvar for publisering av pekere på verdensveven (World Wide Web)**
Hans Marius Graasvold – Pekeransvaret. Straffe- og erstatningsansvar for publisering av pekere til informasjon på Internett
Vegard Hagen / Martin Grasvold.....*NOK 234,-*

11/02 **Personopplysningsloven § 7. En analyse av forholdet mellom personvern og ytringsfrihet slik det er uttrykt i person-opplysningsloven § 7**
Karen Elise Haug Aronsen.....*NOK 198,-*

12/02 **Databasevern. Sui generis-vern av sammenstillinger etter gjennomføringen av databasedirektivet i åndsverkloven § 43**
Lisa Vogt Lorentzen.....*NOK 210,-*

2001

1/01 **Internet and Choice-of-Law – The International Sale of Digitised Products through the Internet in a European Context**
Peter Lenda.....*NOK 275,-*

2/01 **Internet Domain Names and Trademarks**
Tonje Røste Gulliksen.....*NOK 227.-*

3/01 **Internasjonal jurisdiksjon ved elektronisk handel – med Luganokonvensjonen art 5 (5) og elektroniske agenter som eksempel**
Joakim S. T. Øren ..... *NOK 204.-*

4/01 **Legal issues of maritime virtual organisations**
Emily M. Weitzenböck ..... *NOK 164.-*

5/01 **Cyberspace jurisdiction in the U.S. – The International Dimension of Due Process**
Henrik Spang-Hanssen ..... *NOK 685.-*

6/01 **Norwegian border control in a Europe without Internal Frontiers – Implications for Data Protection and civil liberties**
Stephen Kabera Karanja ..... *NOK 252,-*

2000

1/00 **Klassikervernet i norsk åndsrett**
Anne Beth Lange ..... *NOK 268.-*

2/00 **Adgangen til å benytte personopplysninger. Med vekt på det opprinnelige behandlingsformålet som begrensningsfaktor**
Claude A. Lenth ..... *NOK 248.-*

3/00 **Innsyn i personopplysninger i elektroniske markedsplasser.**
Line Coll ..... *NOK 148.-*

1999

1/99 **International regulation and protection of Internet domain and trademarks**
Tonje Røste Gulliksen ..... *NOK 248.-*

2/99 **Betaling via Internett**
Camilla Julie Wollan ..... *NOK 268.-*

3/99 **Internett og jurisdiksjon**
Andreas Frølich Fuglesang & Georg Philip Krog ..... *NOK 198.-*

1998

1/98 **Fotografiske verk og fotografiske bilder, åndsverkloven § 1 og § 43 a**
Johan Krabbe-Knudsen ..... *NOK 198.-*

2/98 **Straffbar hacking, straffelovens § 145 annet ledd**
Guru Wanda Wanvik ..... *NOK 238.-*

3/98 **Interconnection – the obligation to interconnect telecommunications networks under EC law**
Katinka Mahieu ..... *NOK 198.-*

1997

1/97 **Eksemplarfremstilling av litterære verk til privat bruk**
Therese Steen ..... *NOK 158.-*

2/97 **Offentlige anskaffelser av informasjonsteknologi**
Camilla Sivesind Tokvam ..... *NOK 175.-*

3/97 **Rettslige spørsmål knyttet til Oppgaveregisteret**
Eiliv Berge Madsen ..... *NOK 170.-*

4/97 **Private pengespill på Internett**
Halvor Manshaus ..... *NOK 160.-*

5/97 **Normative Structures in Natural and Artificial Systems**
Christen Krogh ..... *NOK 255.-*

6/97 **Rettslige aspekter ved digital kringkasting**
Jon Bing ..... *NOK 178.-*

7/97 **Elektronisk informasjonsansvar**
Tomas Myrbostad *NOK148.-*

8/97 **Avtalelisens etter åndsverksloven § 36**
Ingrid Mauritzen ..... *NOK 120.-*

9/97 **Krav til systemer for forvaltning av immaterielle rettigheter**
Svein Engebretsen ..... *NOK 168.-*

10/97 **American Telephony: 120 Years on the Road to Full-blown Competition**
Jason A. Hoida ..... *NOK 140.-*

11/97 **Rettslig vern av databaser**
Harald Chr Bjelke.....*NOK 358.-*

1996

1/96 **Innsynsrett i elektronisk post i offentlig forvaltning**
Knut Magnar Aanestad og Tormod S. Johansen.....*NOK 218.-*

2/96 **Public Policy and Legal regulation of the Information Market in the Digital Network Enviroment**
Stephen John Saxby .....*NOK 238.-*

3/96 **Opplysning på spill**
Ellen Lange.....*NOK 218.-*

4/96 **Personvern og overføring av personopplysninger til utlandet**
Eva I. E. Jarbekk .....*NOK 198.-*

5/96 **Fjernarbeid**
Henning Jakhelln .....*NOK 235.-*

6/96 **A Legal Advisory System Concerning Electronic Data Interchange within the European Community**
Andreas Mitrakas.....*NOK 128.-*

7/96 **Elektronisk publisering: Utvalgte rettslige aspekter**
Jon Bing og Ole E. Tokvam .....*NOK 186.-*

8/96 **Fjernsynsovervåking og personvern**
Finn-Øyvind H. Langfjell.....*NOK 138.-*

1995

1/95 **Rettslige konsekvenser av digitalisering: Rettighetsadministrasjon og redaktøransvar i digitale nett**
Jon Bing.....*NOK 368.-*

2/95 **Rettslige spørsmål i forbindelse med utvikling og bruk av standarder innen telekommunikasjon**
Sverre Sandvik .....*NOK 178.-*

3/95 **Legal Expert Systems: Discussion of Theoretical Assumptions**
Tina Smith ..... *NOK 278.-*

4/95 **Personvern og straffeansvar – straffelovens § 390**
Ole Tokvam ..... *NOK 198.-*

5/95 **Juridisk utredning om filmen «To mistenkelige personer»**
Johs. Andenæs ..... *NOK 138.-*

6/95 **Public Administration and Information Technology**
Jon Bing and Dag Wiese Schartum ..... *NOK 348.-*

7/95 **Law and Liberty in the Computer Age**
Vittorio Frosini ..... *NOK 158.-*

1994

1/94 **Deon'94, Second International Workshop on Deontic Logic in Computer Science**
Andrew J. I. Jones & Mark Sergot (ed) ..... *NOK 358.-*

2/94 **Film og videogramrett. TERESA (60)**
Beate Jacobsen ..... *NOK 318.-*

3/94 **Elektronisk datutveksling i tollforvaltingen – Rettslige spørsmål knyttet til TVINN**
Rolf Risnæs ..... *NOK 225.-*

4/94 **Sykepenger og personvern – Noen problemstillinger knyttet til behandlingen av sykepenger i Infotrygd**
Mari Bø Haugestad ..... *NOK 148.-*

5/94 **EØS, medier og offentlighet. TERESA (103)**
Mads Andenæs, Rolf Høyer og Nils Risvand ..... *NOK 148.-*

6/94 **Offentlige informasjonstjenester: Rettslige aspekter**
Jon Bing *NOK148.-*

7/94 **Sattelittfjernsyn og norsk rett. MERETE (3) IV**
Nils Eivind Risvand ..... *NOK 138.-*

8/94 **Videogram på forespørsel. MERETE (14) IV**
Beate Jacobsen (red) ..... *NOK 158.-*

9/94 **«Reverse engineering» av datamaskinprogrammer. TERESA (92) IV**
Bjørn Bjerke.....*NOK 198.-*

10/94 **Skattemessig behandling av utgifter til anskaffelse av datamaskinprogrammer. TERESA (75)**
Gjert Melsom.....*NOK 198.-*

1993

1/93 **Artificial Intelligence and Law. Legal Philosophy and Legal Theory**
Giovanni Sartor.....*NOK 148.-*

2/93 **Erstatningsansvar for informationstjenester, særlig ved databaseydelser**
Connie Smidt.....*NOK 138.-*

3/93 **Personvern i digitale telenett**
Ingvild Hanssen-Bauer.....*NOK 178.-*

4/93 **Consumers Purchases through Telecommunications in Europe. – Application of private international law to cross-border contractual disputes**
Joachim Benno.....*NOK 198.-*

5/93 **Four essays on: Computers and Information Technology Law**
Morten S. Hagedal.....*NOK 218.-*

6/93 **Sendetidsfordeling i nærradio MERETE (3) III**
Marianne Rytter Evensen.....*NOK 148.-*

7/93 **Essays on Law and Artificial Intelligence**
Richard Susskind.....*NOK 158.-*

1992

1/92 **Avskriving av mikrodatamaskiner med tilbehør – en nordisk studie TERESA (87)**
Beate Hesseltvedt.....*NOK 138.-*

2/92 **Kringkastingsbegrepet TERESA (78)**
Nils Kr. Einstabland.....*NOK 208.-*

3/92 **Rettskilderegistre i Helsedirektoratet NORIS (94) I & II**
Maria Strøm.....*NOK 228.-*

4/92 **Softwarepatent – Imaterialrettens enfant terrible. En redegjørelse for patenteringen af softwarerelaterede opfindelser i amerikansk og europæisk ret**
Ditlev Schwanenfügel.....*NOK 158.-*

5/92 **Abonnementskontrakter fro kabelfjernsyn TERESA (78II)**
Lars Borchgrevink Grindal.....*NOK 248.-*

6/92 **Implementing EDI – a proposal for regulatory form**
Rolf Riisnæs.....*NOK 118.-*

7/92 **Deponering av kildekode«escrow»-klausuler TERESA (79)**
Morten S. Hagedal.....*NOK 128.-*

8/92 **EDB i juridisk undervisning – med en reiserapport fra England og USA**
Ola-Kristian Hoff.....*NOK 228.-*

9/92 **Universiteters ansvar for bruk av datanett TERESA (94)**
Jon Bing & Dag Elgesem.....*NOK 198.-*

10/92 **Rettslige sider ved teletorg**
Andreas Galtung.....*NOK 148.-*

EARLIER REPORTS

The reports can be ordered from Akademika:

Number / year: _____
Title: _____

Number / year: _____
Title: _____

Number / year: _____
Title: _____

Number / year: _____
Title: _____

Number / year: _____
Title: _____

Name: _____
Adress:_____
Zip code: _____
Telephone number:_____

The reports can be ordered from Akademika:

akademika
Avd. juridisk litteratur Aulabygningen
Karl Johansgt. 47, 0162 Oslo
Telefon: 22 42 54 50
Telefaks: 22 41 17 08
(www.akademika.no) or Unipub (www.unipub.no)