

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

DGI(2014)12

Updated version 04 Oct 2014

ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values

by¹

Dr Monika Zalnieriute
Fellow at the Centre for Internet & Human Rights
European University Viadrina
Germany

and

Thomas Schneider
Deputy Chair of the Council of Europe's Steering Committee
on Media and the Information Society (CDMSI)

¹ The opinions expressed in this document are personal and do not engage the responsibility of the Council of Europe. They should not be regarded as placing upon the legal instruments mentioned in it any official interpretation capable of binding the governments of member states, the Council of Europe's statutory organs or the European Court of Human Rights.

Contents

FOREWORD	5
EXECUTIVE SUMMARY	7
INTRODUCTION	9
CHAPTER 1 HUMAN RIGHTS OBLIGATIONS BY GOVERNMENTS & INTERPRETATIVE DOCTRINES.....	13
CHAPTER 2 NEW GENERIC TOP LEVEL DOMAINS AND RIGHT TO FREEDOM OF EXPRESSION, FREEDOM OF ASSOCIATION, FREEDOM OF RELIGION, AND PRINCIPLE OF NON-DISCRIMINATION.....	15
2.1. Introduction.....	15
2.2. ICANN Procedures and Human Rights Considerations.....	17
2.2.1. String Review – Security & Sensitive Expression.....	17
2.2.2. GAC ‘Early Warning’ & ‘Advice’ Procedure	18
2.2.3. Public Objection and Dispute Resolution Procedures.....	18
2.2.4. String Contention Procedures	19
2.2.4.1. <i>Community Applicants</i>	20
2.2.4.2. <i>Auctions</i>	20
2.3. Human Rights Framework Applicable to gTLD	20
2.3.1. Free Expression and Internet	21
2.3.2. Relevant Provisions	21
2.3.3. Sensitive Expression: from Hate Speech to Protected Disturbing Speech... ..	24
2.3.4. Protected Expressions: From Political Expression to Religious Expression.. ..	26
2.4. Human Rights Analysis of the gTLD Application Procedures.....	27
2.4.1. Problematic and Sensitive Applied-For Strings	27
2.4.2. Freedom of Expression and Trademarks.....	29
2.4.3. Sensitivities and Varying Levels of Acceptable Criticism.....	29
2.4.4. Case Study on String Contention Procedures: Community Applications.....	30
2.4.5. Auction Procedures: Equality & Non-Discrimination	34
2.5. Conclusion.....	35
CHAPTER 3 WHOIS & RAA VS. DATA PROTECTION & PRIVACY	37
3.1 Introduction	37
3.2 ICANN Policy on Personal Data Retention & Public Access	37
3.2.1 Data Retention Specification.....	37
3.2.2 Public Access to Data on Registered Names	38

3.3.	HUMAN RIGHTS FRAMEWORK APPLICABLE TO RAA	38
3.4.	Human Rights Analysis of WHOIS and RAA	41
3.4.1.	Prescribed by Law/In Accordance with Law	41
3.4.2.	Legitimate Aim	42
3.4.3.	Necessary & Proportionate in a Democratic Society	43
3.4.4.	Purpose Limitation	43
3.5.	Conclusion.....	46
	CONCLUSION AND RECOMMENDATIONS	49
	Roles & Responsibilities – ICANN & GAC.....	50
	Recommendations	51

Foreword

The Internet is an aggregate of a vast range of ideas, technologies, resources and policies developed on the assertion of freedom and through collective endeavours in the common interest. States, the private sector, civil society and individuals have all contributed to build the dynamic, inclusive and successful Internet that we know today. The Internet provides a space of freedom, facilitating the exercise and enjoyment of fundamental rights, participatory and democratic processes, and social and commercial activities.

As the Internet is becoming ever more essential for individuals' everyday activities, the technological architecture and design choices embedded in them have ever greater consequences for human rights and shared values. Therefore, it is crucial that the Internet is managed in a sustainable and people-centered fashion and in harmony with human rights and fundamental freedoms, democracy and the rule of law. An open, inclusive, safe and enabling environment must go hand in hand with a maximum of rights and services subject to a minimum of restrictions and a level of security which users are entitled to expect. The existing framework of international law, including human rights law, is, as a matter of principle, equally applicable on-line as it is off-line.

The NETmundial Statement adopted in Sao Paulo on 24 April 2014 recognized that the Internet is a global resource which should be managed in the public interest. Its outcome document further held that governments have primary, legal and political accountability for the protection of human rights. Additionally, the High Level Panel on Global Internet Cooperation and Governance Mechanisms recognized in its report of May 2014 the NETmundial principles as being "fundamental for the operationalization of a 21st century, collaborative framework of governance for a unified Internet that is unfragmented, interconnected, interoperable, secure, stable, resilient, sustainable, and trust building".² The panel further held that the internet governance ecosystem should respect human rights and shared values.

The Council of Europe is an international organization, promoting co-operation between 47 member states and beyond, in the areas of human rights, rule of law and democracy. The Council of Europe fully supports the multi-stakeholder model of Internet governance which ensures that the Internet remains universal, open and innovative, and continues to serve the interests of users throughout the world.

The purpose of this report is to contribute to a more thorough discussion on global governance in the field of the Internet and its impact on human rights. It tries to raise awareness and improve knowledge on ICANN's impact on fundamental human rights, such as the right to freedom of expression or the right to privacy. It is clear that these are topics of paramount importance and demand serious public debate. The authors encourage ICANN to be part of global governance as an ethical process that bases itself on human rights.

² Panel on Global Internet Cooperation and Governance Mechanisms, 'Towards a Collaborative, Decentralized Internet Governance Ecosystem', May 2014

This report is intended specifically for ICANN and the GAC and all those who seek expert guidance on human rights and Internet governance. It provides both ICANN and the GAC with action-based recommendations to enhance human rights, fundamental freedoms, democracy and the rule of law online. The authors remind us that all who participate in internet governance are to shape the evolution in a manner that ensures human rights based approach.

I would like to thank the authors Monika Zalnieriute and Thomas Schneider for this timely report. I would also like to express thanks to Kinanya Pijl, member of the secretariat of the Internet Governance Unit at the Council of Europe, for her support.

Jan Kleijssen
Director
Information Society and Action against Crime
Directorate General Human Rights and Rule of Law
Council of Europe

Executive summary

This report focuses on the meaning of ICANN's global public interest responsibilities from an international human rights perspective. The report aims at clarifying the role and responsibilities of states in securing human rights in ICANN mechanisms and procedures; and how States can support this multi-stakeholder model in a way that better guarantees to serve the global public interest.

The concept of serving the global public interest is vague, providing neither clear guidance nor constraint on ICANN's action. It is therefore important to flesh it out in order to strengthen accountability and transparency in ICANN's multi-stakeholder model.

ICANN's current standards on 'sensitive applied-for new gTLD's' do not fully comply with the right to freedom of expression. The disagreement and confrontation raised by terms such as '.sucks' – even when expressed in strong terms – ordinarily come within the scope of the protection offered by the right to freedom of expression. ICANN should therefore exercise its role with due regard for fundamental rights and freedoms and in full compliance with international standards.

In the light of the positive obligations of states to reach out to specific types of groups who for various reasons are vulnerable, it is desirable that the people-centeredness of ICANN's policy development is further improved. A balance must be struck between economic interests and other objectives of common interest, such as pluralism, cultural and linguistic diversity. A less restrictive and formalistic approach in dealing with communities, in particular one that is promoting pluralism and that is better respecting special needs of vulnerable groups is recommended. As a result of this restrictive approach of the applied mechanisms for community priority evaluation, the application of auctions may risk to become the wide-used approach for allocating the scarce resource of attractive TLDs. This may be an efficient way of allocation from an economic point of view but not from a view of respecting plurality and diversity.

Law enforcement considerations seem to have been dominating in the elaboration of the new data retention provisions in the 2013 RAA at the expense of privacy considerations. States bear responsibility to take reasonable steps to ensure that the RAA complies with human rights, and that the right to privacy and personal data protection are effectively protected. Increased emphasis on safeguarding the right to privacy is therefore highly desirable, inter alia, in the light of the UN Resolution on *Privacy in the Digital Age* that might include sufficient agreement for the purpose of formation of a rule of customary international law on the right to privacy in a digital age.

As has been put forward by many experts in the field, public access to personal information in the WHOIS database is not fully consistent with international human rights law. National and international data protection instruments establish high standards for accessing and processing personal information by third parties. GAC members have the responsibility to protect the human rights of their citizens and should therefore make sure that ICANN includes provisions governing the disclosure and third party use of data.

The historically grown establishment of ICANN as a private corporation under Californian law may not be a sustainable solution for systematically taking into account international human rights law. New innovative solutions may be explored for the future development of ICANN in this regard.

As the role of ICANN in the field of Internet governance is increasing, its responsibility and accountability have to grow. A more attentive approach towards human rights could help to create an accountable and transparent way of doing business. Therefore the authors recommend to:

- Include reference to human rights in ICANN's Bylaws
- Define public interest objectives
- Improve the human rights expertise and early engagement in the GAC
- Develop an early engagement mechanism for the safeguard of human rights
- Review ICANN's legal basis and explore innovative solutions for developing an international or quasi-international status of ICANN.

Introduction

1. ICANN's remit is to take care of the technical coordination of the Internet's domain name and addressing system (DNS) in the global public interest. By means of a multi-stakeholder, private sector led, bottom-up policy development model for DNS technical coordination it has shown to flexibly meet the changing needs of the Internet and of the Internet community.
2. When technical and non-technical issues and outcomes concern matters of public policy, it is the role of the Governmental Advisory Committee (GAC)³ to provide advice on the activities of ICANN as they relate to concerns of governments.⁴ ICANN's Bylaws specifically entrust this to national governments, while other stakeholders, such as the At-Large Committee⁵ can give advice on ICANN's activities and policy. The GAC is not a decision making body, but has an important advisory task on matters where there may be an interaction between ICANN's policies and various laws and international agreements and public policy objectives.⁶
3. ICANN is a unique bottom-up multi-stakeholder model that came into life by means of a mandate from the United States government to improve the technical management of Internet names and addresses. It developed and became an institution that aims to serve the global public interest. Over the past years, ICANN has increased dramatically in size mostly due to the introduction of new generic top-level domains (gTLDs). It has grown and matured over time and expanded its areas of activities.⁷
4. ICANN's development has an impact on the scope and meaning of 'serving the global public interest'. Is it in the interest of the Internet community to block sensitive and problematic strings? Who has the right to own or should be entitled to exploit a TLD in case of multiple competing applicants and in whose interest? Is there a risk of making decisions presently that prejudice future developments taking into account all competing interests? Under what circumstances do community applicants prevail over other applicants? And what WHOIS information should or should not be publicly available? ICANN has to determine what it means to operate in the public interest with regard to an increasing variety of issues. And also taking into account that the public interest may evolve and change over time. There are

³ "The GAC's key role is to provide advice to ICANN on issues of public policy, and especially where there may be an interaction between ICANN's activities or policies and national laws or international agreements. The GAC usually meets three times a year in conjunction with ICANN meetings, where it discusses issues with the ICANN Board and other ICANN Supporting Organisations, Advisory Committees, and receives updates on process and policy from ICANN staff. Membership of the GAC is open to all national governments and distinct economies as recognised in international fora. Multinational governmental organisations and treaty organisations may join the GAC as observers. Currently, the GAC is regularly attended by approximately 50 national governments, distinct economies, and global organisations such as the ITU, UNESCO, the World Intellectual Property Organisation (WIPO), INTERPOL and regional organisations such as the OECD, Asia Pacific Forum, and Council of Europe". See: ICANN, 'About the GAC' <<https://gacweb.icann.org/display/gacweb/About+The+GAC>> accessed 17 April 2014

⁴ ICANN, 'Bylaws for Internet Corporation for Assigned Names and Numbers', Section 2, § 11 <<http://www.icann.org/en/about/governance/bylaws>> accessed 10 April 2014.

⁵ "The At-Large Advisory Committee (ALAC) is the primary organizational home within ICANN for individual Internet users. The role of the ALAC shall be to consider and provide advice on the activities of ICANN, insofar as they relate to the interests of individual Internet users". See: ICANN, 'Bylaws for Internet Corporation for Assigned Names and Numbers' <<http://www.icann.org/en/about/governance/bylaws>> accessed 10 April 2014.

⁶ ICANN-GAC, 'GAC Operating Principles' (2011), Article I – Scope of the Governmental Advisory Committee, principle 1 and 2 <<https://gacweb.icann.org/display/gacweb/GAC+Operating+Principles>> accessed 21 May 2014.

⁷ See: Fadi Chehadé, 'Balancing the Tasks At Hand' (12 March 2014) <<http://blog.icann.org/2014/03/balancing-the-tasks-at-hand/>> accessed 21 May 2014.

different publics and different and inevitably divergent interests.⁸ It is a great challenge to find the right balance.

5. This report aims at supporting the multi-stakeholder model, by providing guidance on how to live up to the expectations of the internet community. Human rights are the point of departure, since those rights must always be at the centre when serving the public interest. Internet users have a legitimate expectation that Internet services be accessible and affordable, secure, reliable and ongoing, as part of the public service value of the Internet.

6. To catalyze community discussion, this paper explores: How can we support the multi-stakeholder model in a way which more efficiently guarantees serving the public interest? This study will pay close attention to ICANN's practices and principles. It will selectively assess what the organization actually does, the subject matters it works on, and the ways it goes about identifying problems, scoping solutions and implementing policies in the light of fundamental human rights requisites. This paper builds upon and goes beyond a previously written expertise commissioned by the Council of Europe: 'Comments relating to freedom of expression and freedom of association with regard to new generic top level domains'.⁹

7. This paper focuses on the meaning of ICANN's global public interest responsibilities from an international human rights perspective. The point of departure of this assessment is the Universal Declaration of Human Rights (UDHR). The rights to which all human being are inherently entitled as set out in the UDHR have been further elaborated in the International Covenant on Economic, Social and Cultural Rights (ICESCR) and the International Covenant on Civil and Political Rights (ICCPR) which are therefore equally important. These fundamental rights have also been set out in regional human rights treaties, such as the European Convention on Human Rights (ECHR).

8. This paper is written from a Council of Europe perspective. The Council of Europe is an international organization, promoting co-operation between 47 member states and beyond on legal and political standards on human rights, rule of law and democracy online and offline. The rights set out in the European Convention on Human Rights, as interpreted by the European Court of Human Rights, therefore play an important role in this analysis.

9. The reader should keep in mind that ICANN is a private organisation under US law. Private organisations are not duty-bearers under international human rights law, as is the case for states. Additionally, ICANN is not bound by the US Bill of Rights, which sets out fundamental human rights, since those norms apply exclusively to state actors. Nevertheless, business enterprises have a responsibility to respect human rights as set out in the UN Guiding Principles on Business and Human Rights, as unanimously adopted by the United Nations Human Rights Council in June 2011.¹⁰ These Guiding Principles present the global reference for corporate responsibilities to respect human rights and apply to all business enterprises, both transnational and others, regardless of their size, sector, location, ownership and structure. ICANN's set-up as a non-profit corporation seems to be captured by the broad notion of "other business enterprises" under these Principles, which includes any business entity, such as

⁸ See also: David E. Morrison & Michael Svennevig, 'The Public Interest, the Media and Privacy' (March 2002) <<http://www.ofcom.org.uk/static/archive/bsc/pdfs/research/pidoc.pdf> accessed 21 May 2014.

⁹ W. Benedek, Joy Liddicoat and Nico van Eijk, 'Comments relating to freedom of expression and freedom of association with regard to new generic top level domains', Council of Europe DG-I (2012) 4, 12 October 2012.

¹⁰ See the United Nations Human Rights Council, Guiding Principles on Business and Human Rights, HR/PUB/11/04, available at http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf/ (visited 23/09/2014).

corporate, or partnership, or any other legal form used to establish a business entity.¹¹ Thus, under the Principles, ICANN bears responsibility to respect human rights throughout its global operations regardless of where its users are located and of whether states meet their own human rights obligations under international law. Human rights are a fundamental parameter to manage Internet as a global resource in the public interest. The report aims at clarifying the role and responsibilities of states in securing human rights and the rule of law in ICANN mechanisms and procedures; and how states can support this multi-stakeholder model in a way that better guarantees to serve the global public interest.

10. In April 2014, a Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial), held in Sao Paulo, Brazil, identified a set of common principles and important values that contribute to an inclusive, multistakeholder, effective, legitimate and evolving Internet governance framework.¹² It noted that states have primary, legal and political accountability to protect human rights.¹³ The High Level Panel on Global Internet Cooperation and Governance Mechanisms recognized and fully supported and adopted these principles and emphasized in its report of May 2014 that the Internet governance ecosystem should respect human rights and shared values.¹⁴

11. The authors are grateful for the discussions that have taken place in several international fora since the publication of the first version of this report in June 2014 and for the valuable comments received from various communities, organizations and individuals.

¹¹ Sub-Commission on the Promotion and Protection of Human Rights, Commentary on the Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights, U.N. Doc. E/CN.4/Sub.2/2003/38/Rev.2 (2003), § 21.

¹² NETmundial Multistakeholder Statement, available at [/http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf/](http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf) (visited 18/05/2014).

¹³ Ibid.

¹⁴ Panel on Global Internet Cooperation and Governance Mechanisms, 'Towards a Collaborative, Decentralized Internet Governance Ecosystem', May 2014.

CHAPTER 1

HUMAN RIGHTS OBLIGATIONS BY GOVERNMENTS & INTERPRETATIVE DOCTRINES

12. In July 2012, the UN Human Rights Council (HRC) adopted by consensus a Resolution on the promotion, protection and enjoyment of human rights on the Internet,¹⁵ which affirmed that “the same rights that people have offline must also be protected online”. Before discussing human rights at stake in the ICANN mechanisms in more detail, it is important to stress from the outset that states have a certain amount of discretion in how they safeguard human rights.¹⁶ This discretion has become known as the margin of appreciation doctrine, which has an important influence on how human rights are interpreted at national level. The degree of discretion, which (at European level) is subject to supervision by the European Court of Human Rights (ECtHR), varies according to the particular facts in question and other factors. The margin of appreciation is not unlimited.¹⁷ For example, states have a narrow margin of appreciation in respect of political expression, yet they enjoy a wider margin of appreciation in respect of public morals, decency and religion.¹⁸ This is explained by a lack of a European consensus on these issues.

13. Three other interpretative principles of the European Court of Human Rights are of particular relevance in the context of ICANN procedures and mechanisms and may be utilised in order to enhance the ICANN policy-making process: (1), the practical and effective doctrine; (2) the living instrument doctrine, and (3) the positive obligations doctrine. According to the first, all rights guaranteed by the European Convention on Human Rights (ECHR) must be “practical and effective” and not merely “theoretical or illusory”.¹⁹ Under the second,²⁰ the ECHR is regarded as a “living instrument” which “must be interpreted in the light of present-day conditions”.²¹ Finally, the essence of the positive obligations doctrine is that, in order for states to ensure that everyone can exercise all of their rights enshrined in the ECHR in a practical and effective manner, the typical stance of non-interference (or negative obligation) by State authorities will often not suffice. As the Court affirmed in *Özgür Gündem v. Turkey*: “Genuine, effective exercise of [the right to freedom of expression] does not depend merely on the State’s duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals”.²²

14. These interpretative principles and doctrines suggest that the judiciary/international tribunals recognize that policy-making is changing. In this ever-evolving process, states must

¹⁵ UN, Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet* (5 July 2012) UN Doc. A/HRC/20/L.13, [/http://www.regeringen.se/content/1/c6/19/64/51/6999c512.pdf](http://www.regeringen.se/content/1/c6/19/64/51/6999c512.pdf) (visited 12/02/2014).

¹⁶ The first case where the Court has discussed the margin of appreciation is Judgment of 7 December 1976, *Handyside v. United Kingdom*, Series A, No. 24, § 48-49.

¹⁷ *Ibid*, § 49.

¹⁸ *Wingrove v. United Kingdom* (no. 17419/90), 25.11.1996, § 58.

¹⁹ *Airey v. Ireland*, Judgment of the European Court of Human Rights of 9 October 1979, § 24.

²⁰ For an overview of the historical development of the “living instrument” doctrine (including recent developments) by the European Court of Human Rights, see: Alastair Mowbray, “The Creativity of the European Court of Human Rights”, *Human Rights Law Review* 5: 1 (2005), 57-79.

²¹ *Tyrer v. the United Kingdom*, Judgment of the European Court of Human Rights of 25 April 1978, Series A, no. 26, § 31; *Matthews v. the United Kingdom*, Judgment of the European Court of Human Rights of 18 February 1999, § 39.

²² *Özgür Gündem v. Turkey*, Judgment of the European Court of Human Rights (Fourth Section) of 16 March 2000, § 43.

remain responsible for ensuring that the contemporary governance models/processes allow individuals to meaningfully exercise their rights. In the ICANN context, the practical and effective doctrine requires that appropriate appeal mechanisms respecting international and national laws are put in place to ensure that the due process and the rights enjoyed by domain names' registrants and concerned third parties are adequately respected. As ICANN expands and its mechanisms and procedures affect more and more individuals, the living instrument doctrine might suggest, for example, that vulnerable groups that did not merit special protection in the past may now deserve specific protection under, for example, the national regulation of hate speech online. This might be the case for homophobic hate speech which has recently been examined by the ECtHR. Finally, the positive obligations doctrine implies that states have a duty to take reasonable steps to ensure that the rights of, for example, Roma, homosexuals and other vulnerable groups are in fact protected. Indirectly, this implies a commitment of the governments to also defend this in the ICANN and GAC context. The ICANN expansion process means that more multi-stakeholder dialogue is necessary to ensure that it operates in the public interest. With this expansion comes increasing responsibility and accountability.

15. More emphasis by states on human rights in ICANN's policy mechanisms and procedures would bring it more in line with the expectations of the multi-stakeholder community. The following chapters will address the complex relationships between the interest and rights of different ICANN stakeholders.

16. In particular, the Applicant Guidebook and *2013 Registrar Accreditation Agreement (RAA)*²³ may bear on freedom of expression, association and religion, as well personal data protection and privacy. Chapter 2 focuses on the new gTLD and the freedom of expression and association as well as freedom of religion. Chapter 3 emphasizes the data protection and privacy issues related to the RAA. Together, these chapters highlight the complex relationship between ICANN's policies and procedures and international human rights.

²³ ICANN, 2013 Registrar Accreditation Agreement, <http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm#raa> (visited 14/04/2014).

CHAPTER 2

New generic top level domains and right to freedom of expression, freedom of association, freedom of religion, and principle of non-discrimination

2.1. Introduction

17. From a policy perspective, one of the most important functions of ICANN is to decide on the introduction of new gTLDs into the DNS.²⁴ ICANN's New gTLD Programme was established to add an unlimited number of new gTLDs to the root zone. The goal of this expansion was to enhance competition, innovation and consumer choice.²⁵ The first application round started on January 12th 2012 and ended in April 2012. In October 2012, the Council of Europe released an expert paper entitled 'Comments relating to freedom of expression and freedom of association with regard to new generic top level domains'.²⁶ This work has analysed the relationship between freedom of expression and the gTLDs, and authoritatively demonstrated that the domain names, including gTLDs, may entail expressive and communicative elements, and (national) courts have recognized the relationship between the so called 'expression function' of domain names and freedom of expression.²⁷ ICANN's remit does not generally extend to any examination of the content comprised in or to be hosted under TLDs.²⁸ Nonetheless, Internet content-related considerations do not fall completely outside ICANN authority and deliberations on new gTLDs delegations are not expected to be mechanical actions. The approval or rejection of applied-for new gTLD strings may involve an evaluation process where judgements related to content are made. Building on the earlier work of the Council of Europe, this chapter looks at applied-for sensitive and problematic strings from the perspective of protecting human rights, and the right to freedom of expression, freedom of association, freedom to religion and the principle of equality and non-discrimination.²⁹

²⁴ See Article 3 of ICANN's Articles of Incorporation.

²⁵ ICANN, 'About the Program' <<http://newgtlds.icann.org/en/about/program>>accessed 7 May 2014

²⁶ DG-I (2012)4, 12 October 2012, available at [http://www.coe.int/t/information/society/documents/DG-I%20\(2012\)%204%20FINAL%20pdf.pdf](http://www.coe.int/t/information/society/documents/DG-I%20(2012)%204%20FINAL%20pdf.pdf)

²⁷ See, e.g., French Constitutional Council Décision n° 2010-45 QPC du 6 Octobre 2010, official translation into English is available at <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/201045QPCen201045qpc.pdf>, see § 6. See also, Cour d'Appel de Paris, Arrêt du 20 Avril 2003 Société Groupe Danone ct. Association Le Réseau Voltaire pour la liberté d'expression, p.12, available at <http://www.foruminternet.org/telechargement/documents/ca-par20030430.pdf>. This case concerned the usage of domain names www.jeboycottedanone.com and www.jeboycottedanone.net; Dutch case of *Inholland vs. Kaasjager*, KG 05/447, 21 June 2005, available at www.domjur.nl; USA case of *Name.Space, Inc., v. Network Solutions, Inc. and National Science Foundation*, 202 F.3d 573, 577 (2d Cir. 2000), available at <http://www.yale.edu/lawweb/jbalkin/telecom/namespace.pdf>

²⁸ In order to resolve domain name disputes at the second level ICANN has developed a limited policy, on a narrow set of grounds with a small number of dispute resolution providers, i.e. the Universal Dispute Resolution Policy, available at <http://www.icann.org/en/help/dndr/udrp/policy>. Many other legal remedies and dispute mechanisms for TLD disputes exist in many countries via judicial and non-judicial mechanisms.

²⁹ See Section 3.1, p. 6 of the Comments relating to freedom of expression and freedom of association with regard to new generic top level domains – DG-I (2012)4, 12 October 2012, available at [http://www.coe.int/t/information/society/documents/DG-I%20\(2012\)%204%20FINAL%20pdf.pdf](http://www.coe.int/t/information/society/documents/DG-I%20(2012)%204%20FINAL%20pdf.pdf)

18. The Applicant Guidebook provides for 5 types of procedures that may affect an application for a new gTLD due to various ‘sensitivities’ or public objections involved. First, the Guidebook contains a list of words that are ineligible for delegation.³⁰ Second, the string review procedure is designed to determine whether an applied-for gTLD string might cause instability to the DNS which consequently might lead to non-approval of the new gTLD.³¹ Third, the procedure by which GAC may provide ‘GAC Advice’ on New gTLDs to the ICANN Board of Directors concerning a specific application. Fourth, the dispute resolution procedure triggered by a formal objection to an application by a third party (usually a trademark owner).³² Fifth and last, the so-called ‘string contention procedures’ for applied-for gTLDs that are identical or are similar enough to cause consumer confusion.³³

19. The potential direct impact on Internet content availability and ICANN’s possible role in content-related assessments was signaled in the San Francisco GAC Communiqué³⁴ and by the Council of Europe paper on freedom of expression and freedom of association with regard to new gTLDs,³⁵ thereby establishing a clear intersection with issues related to the exercise of the right to freedom of expression.³⁶ Content-related judgements and choices made by ICANN thus may result in decisions affecting the availability of information on the Internet. Such judgements are not dissimilar to editorial judgements made by mass communication publishers who routinely decide what content to publish in line with their editorial policies or business interest and which, in certain cases, have to consider what content is relevant for the purposes of serving the public’s interest in their right to know. The particular importance of the media in a democratic society has been stressed repeatedly by the international human

³⁰ See the new gTLDs Applicant Guidebook (the Guidebook), available at <http://newgtlds.icann.org/en/applicants/agb/> Module 2, section 2.2.1.2.3. This constitutes a content-related choice made a priori by ICANN which is expected to result in content-related judgement whenever questions involving usage of any of those ineligible words may arise. The use of the word ‘olympic’, ‘redcross’ and their variations are prohibited. This blanket prohibition is not discussed in more detail in this paper; however the analysis of the implication for freedom of expression of other issues related to sensitive and problematic strings apply to this issue as well. Blanket prohibitions usually fail proportionality test.

³¹ Module 2 section 2.2.1.3. The ICANN Board in explaining reasons for not following GAC advice regarding the potential risk/threat of TLD blocking to the universal resolvability and stability of the DNS stated that “[t]he issue of governments (or any other entity) blocking or filtering access to a specific TLD is not unique to the issue of the .XXX sTLD. Such blocking and filtering exists today. While we agree that blocking of TLDs is generally undesirable, if some blocking of the XXX sTLD does occur there’s no evidence the result will be different from the blocking that already occurs.” See 18 March 2011 ICANN Board Rationale for Approving Registry Agreement with ICM’s for XXX sTLD, Section V, 4, c, at page 16.

³² ICANN, APPLICANT GUIDEBOOK MODULE3 3-1 (2012) [Module 3; see *Objection and Dispute Resolution, ICANN*, <http://newgtlds.icann.org/en/program-status/objection-dispute-resolution> (visited 06/05/2014) (explicating the procedures for the four gTLD objections).

³³ See generally ICANN, GTLD APPUCANT GUIDEBOOK MODUL4E4-1, 4-20 (2012) [hereinafter ICANN, MoDULE 4] (detailing the auction procedure).

³⁴ See GAC Communiqué – San Francisco, March 16, 2011, stating that “with the revised proposed ICANN ICM Registry agreement, the Corporation could be moving towards assuming an ongoing management and oversight role regarding Internet content” available at

https://gacweb.icann.org/download/attachments/1540152/GAC_40_San_Francisco_Communique.pdf?version=1&modificationDate=1312225023000

³⁵ Comments relating to freedom of expression and freedom of association with regard to new generic top level domains – DG-I (2012)4, 12 October 2012, available at [http://www.coe.int/t/information/society/documents/DG-I%20\(2012\)%204%20FINAL%20pdf.pdf/](http://www.coe.int/t/information/society/documents/DG-I%20(2012)%204%20FINAL%20pdf.pdf/)

³⁶ This is also acknowledged in the Guidebook itself; see Module 3, section 3.5.3.

rights bodies and organizations, as well as by international and domestic courts and tribunals.³⁷

20. Furthermore, the concept of ‘pluralism’ plays a prominent part in the case-law of the European Court of Human Rights (ECtHR). That is to say that pluralism is an important factor determining the scope and impact of a number of fundamental rights, such as the right to freedom of expression, freedom of association and freedom of religion. The ECtHR decided that, in the context of granting broadcasting licenses, states may have to be guided by the importance of pluralism.³⁸ It also expressed the view that the exercise of power by mighty financial groupings may form a threat to media pluralism³⁹ as well as far-reaching monopolization in the press and media sector.⁴⁰ By using the concept of pluralism, the Court adds to the importance of individual and associational fundamental rights.⁴¹ Council of Europe states and the GAC thus should, in the same line of thinking, take care in ensuring that ICANN’s mechanisms includes and embrace a diversity of values, opinions, and social groups and avoids the predominance of particular deep-pocketed organizations that function as gatekeepers for online content.

2.2. ICANN Procedures and Human Rights Considerations

2.2.1. String Review – Security & Sensitive Expression

21. Under the string review procedures, an assessment is made whether an applied-for gTLD string might have an adverse impact on DNS stability and security.⁴² An evaluation of adverse impact is likely to include a “TLD-blocking or filtering impact assessment” due to “sensitive expression” included in the applied-for strings. This was the case in deliberations on the controversial ‘.xxx’ applied-for TLD, where the ICANN Board stated that the risk of blocking was not such as to justify non-approval of that string.⁴³ Such impact assessments in practice cannot be separated from considerations as to what is regarded as “useful or harmful” by different communities and Internet users around the world.

³⁷ See Comments relating to freedom of expression and freedom of association with regard to new generic top level domains – DG-I (2012)4, 12 October 2012, available at [http://www.coe.int/t/information/society/documents/DG-I%20\(2012\)4%20FINAL%20pdf.pdf](http://www.coe.int/t/information/society/documents/DG-I%20(2012)4%20FINAL%20pdf.pdf)

³⁸ *Demuth v. Switzerland*, Judgment of the European Court of Human Rights (Second Section) of 5 November 2002, App. no. 38743/97.

³⁹ *VgT Verein gegen Tierfabriken v. Switzerland*, Judgment of the European Court of Human Rights (Second Section) of 28 June 2001, App. no. 24699/94

⁴⁰ *De Geïllustreerde Pers N.V. v. The Netherlands*, Judgment of the European Commission of Human Rights of 6 July 1976, App. no. 5178/71

⁴¹ See: Aernout Nieuwenhuis, ‘The Concept of Pluralism in the Case-Law of the European Court of Human Rights’ *European Constitutional Law Review*, 3: 367–384, 2007

⁴² Module 1, section 2.2.1.3.1, see also See Also p. 7 of the Comments relating to freedom of expression and freedom of association with regard to new generic top level domains – DG-I (2012)4, 12 October 2012, available at [http://www.coe.int/t/information/society/documents/DG-I%20\(2012\)4%20FINAL%20pdf.pdf](http://www.coe.int/t/information/society/documents/DG-I%20(2012)4%20FINAL%20pdf.pdf)

⁴³ The ICANN Board in explaining reasons for not following GAC advice regarding the potential risk/threat of TLD blocking to the universal resolvability and stability of the DNS stated that “[t]he issue of governments (or any other entity) blocking or filtering access to a specific TLD is not unique to the issue of the .XXX sTLD. Such blocking and filtering exists today. While we agree that blocking of TLDs is generally undesirable, if some blocking of the .XXX sTLD does occur there’s no evidence the result will be different from the blocking that already occurs.” See ICANN Board Rationale of 18 March 2011 for Approving Registry Agreement with ICM’s for .XXX sTLD, Section V, 4, c, p. 16.

2.2.2. GAC ‘Early Warning’ & ‘Advice’ Procedure

22. The GAC can express its views on specific new TLDs based on the argument that the TLD is potentially sensitive or problematic concerning one or more governments via two distinct procedures: (1) ‘Early Warning’ and (2) ‘Advice’ to the ICANN Board. The ‘Early Warning’ is a notice from members of the GAC that an application is seen as potentially sensitive or problematic by one or more states. An Early Warning is “not a formal objection, nor does it directly lead to a process that can result in rejection of the application.”⁴⁴ The GAC could also provide an ‘Advice’ to the ICANN Board regarding an application identified as being problematic, such as one that potentially violates national law or raises sensitivities.

23. As is explained on the ICANN website: “If GAC Advice is based on a consensus of the GAC, it will create a strong presumption that the application should not be approved. If the ICANN Board does not act in accordance with this type of advice, it must provide rationale for doing so.”⁴⁵ Moreover, “if the GAC advises that there are concerns about a particular application, the ICANN Board is expected to enter into dialogue with the GAC to understand the scope of concerns and provide rationale for its decision. If the GAC advises that an application should not proceed unless remediated, this will create a strong presumption that the application should not proceed unless there is a remediation method available in the Applicant Guidebook (such as securing the approval of one or more governments) that is implemented by the applicant. If the issue identified by the GAC is not remediated, the ICANN Board is expected to provide a rationale for its decision if it does not follow GAC advice.”⁴⁶ As explained in the Council of Europe Comments of 2012, states have these obligations and commitments when they participate in entities with specialised technical mandates. This means that GAC advice must be given special consideration by the ICANN Board.⁴⁷ Numerous instances, such as the .XXX gTLD, demonstrate the complex and delicate nature of such procedures which also raise human rights issues related to exercise of freedom of expression, freedom of association, freedom of religion and so on.

2.2.3. Public Objection and Dispute Resolution Procedures

24. The public objection procedures include (1) The string confusion objection, (2) The legal rights objection, (3) Community objection and (4) Limited public interest objection.⁴⁸ A gTLD objected to under a string confusion objection must qualify as confusingly similar to an existing gTLD or a gTLD applied-for in the same application round.⁴⁹ A legal rights objection can occur when an applied-for gTLD infringes on the intellectual property rights of the objector, who must have a legal right over the disputed domain name to possess standing for this objection.⁵⁰ These two objections grounds for initiating Dispute Resolution Procedures are focused on the protection of traditional trademark rights. There is a delicate balance between freedom of expression and the property rights of trademark owners.

⁴⁴ See ‘My ICANN’ website for this definition, available at <https://www.mycann.org/news/topics/1528/page/5/articles/14906?language=fr>.

⁴⁵ See section ‘What Does GAC Advice Mean?’ in the ICANN’s website, available at <http://newgtlds.icann.org/en/applicants/gac-advice>.

⁴⁶ *Ibid*

⁴⁷ See Comments of 2012, p. 3.

⁴⁸ ICANN, Applicant Guidebook, Module 3, at 3-4.

⁴⁹ ICANN, Applicant Guidebook, Module 3, at 3-4. The International Centre for Dispute Resolution (ICDR) handles string confusion objections.

⁵⁰ *Ibid*.

25. To file a community objection, substantial opposition to the applied-for gTLD must exist from a significant portion of the explicitly or implicitly targeted community.⁵¹ ICANN determined that all “established institutions associated with a delineated community” have standing to object under a community objection.⁵² This ground for objections allows for an ample margin of discretion, as illustrated by the approval of the controversial ‘.xxx’ gTLD. Although, many objections were filed, they were not decisive for the final deliberation of the ICANN Board.⁵³

26. Finally, an objector under a limited public interest objection can claim that an applied-for gTLD is contrary to generally accepted norms of morality and public order that are recognized under international law.⁵⁴ The Guidebook specifies a list of morality and public order considerations which relate to incitement and promotion of violence and lawless action, discrimination, child pornography as well as a determination that an applied-for string would be contrary to specific principles of international law.⁵⁵ Similarly to the Sensitive String Review Procedure, the focus on morals, sensitive strings and public order means that evaluation involves judgement as to whether Internet users or communities are likely to find a particular applied-for gTLD against norms of morality and public order. Such evaluations may have a direct impact on the availability of Internet content and clearly intersect with issues related to the exercise of the right to freedom of expression, freedom of association, and freedom of religion.⁵⁶

2.2.4. String Contention Procedures

27. ICANN has also developed its own evaluation procedures for applied-for gTLDs that are identical or are similar enough to cause confusion for Internet users. The mechanisms are called ‘string contention procedures’. A string contention occurs either when (1) two or more applicants for an identical gTLD successfully complete previous evaluation and dispute resolution stages—most notably the objections period—or (2) when two or more applicants for a similar gTLD complete all previous stages and ICANN identifies the gTLDs as creating the probability of causing (consumer) confusion.⁵⁷

28. The first application round of the ICANN’s new gTLD Programme started on 12 January 2012 and ended in April 2012. On ‘Reveal Day’ on 13 June, it was announced that there were

⁵¹ *Ibid.*

⁵² *Ibid.*, at 3-8 (listing three factors that an arbitration panel will utilize when evaluating the first element and enumerating four for the second element).

⁵³ See ICANN Board Rationale of 18 March 2011 for Approving Registry Agreement with ICM’s for .XXX sTLD, Section V, A, p. 18: “The negative community impact will most likely be on those that do not support the idea of the introduction of the .XXX sTLD. However, refusing to approve registry agreements with strings that do not have unanimous community support, is not an acceptable option as ICANN continues to move toward the introduction of even more new gTLDs.”

⁵⁴ ICANN, Applicant Guidebook, Module 3,, at 3-4. Community objections and limited public interest objections are handled by the International Center of Expertise of the International Chamber of Commerce (ICC).

⁵⁵ ICANN, Applicant Guidebook, see Module 3, section 3.5.3.

⁵⁶ This is also acknowledged in the ICANN Applicant Guidebook itself, see Module 3, section 3.5.3.

⁵⁷ *Id.* §4.1. The Applicant Guidebook mentions that all applications for identical gTLDs will automatically be placed in string contention proceedings and all similar gTLD applications will be evaluated by a String Similarity Panel to determine whether the gTLDs would create a probability of consumer confusion. *Id.* at 4-3.

1,930 applications: 84 of these were community applications and 230 of them had more than one applicant.

2.2.4.1. Community Applicants

29. Under the ‘string contention procedures,’ communities are given precedence in case of TLD’s in contention. Precedence automatically takes place if the community applicant passes the so-called ‘community priority evaluation’ (CPE). This evaluation process is conducted by ‘The Economist Intelligence Unit’ and ‘InterConnect Communications’.⁵⁸ To pass the CPE, applicants for community-based gTLDs must demonstrate the following, scoring at least 14 of 16 possible points. Firstly, the community applicant must demonstrate an ongoing relationship with a clearly delineated community (4 points). Secondly, the applicant must have applied for a gTLD string strongly and specifically related to the community named in the application (4 points). Thirdly, the applicant must have proposed a dedicated registration and use policies for registrants in its proposed gTLD, including appropriate security verification procedures, commensurate with the community-based purpose it has named (4 points). Lastly, it must have its application endorsed in writing by one or more established institutions representing the community it has named (4 points).⁵⁹

2.2.4.2. Auctions

30. In most cases where multiple applicants apply for a single new gTLD it is expected that contention will be resolved by the community priority evaluation, or through voluntary agreement among the involved applicants. If that is not the case, auctions will take place to determine the winner of each contention set.⁶⁰ These auctions will be conducted in a way in which the auctioneer successively increases the prices associated with applications within the contention set, and the respective applicants indicate their willingness to pay these prices. As the prices rise, applicants will successively choose to exit from the auction. At the auction’s conclusion, the remaining applicant will pay the resulting prices and proceed toward delegation.⁶¹

31. The CPE Process and the Auctions, similarly to other string evaluation procedures, may have a direct impact on Internet content availability and clearly intersect with issues related to the exercise of the right to freedom of expression, freedoms of association and religion, as well as the principle of equality and non-discrimination.⁶²

2.3. Human Rights Framework Applicable to gTLD

32. The use of domain names, including gTLDs, concerns forms of expression that are protected by international human rights law which, in Europe, the 47 member states of the Council of Europe have undertaken to secure as part of the framework of civil and political rights and freedoms provided in the ECHR. This section builds on the previous work of the

⁵⁸ ICANN, ‘Preparing Evaluators for the New gTLD Application Process’ (22 November 2011) <<http://newgtlds.icann.org/en/blog/preparing-evaluators-22nov11-en>> accessed 7 May 2014.

⁵⁹ See ICANN, Applicant Guidebook, Module 4.2.3.

⁶⁰ An auction will not take place to resolve contention in the case where the contending applications are for geographic names. See: Applicant Guidebook.

⁶¹ ICANN, Applicant Guidebook, § 4.3.1

⁶² This is also acknowledged in the ICANN Applicant Guidebook itself, see Module 3, section 3.5.3.

Council of Europe and the section focuses on the ECtHR's jurisprudence on freedom of expression, freedom of association and religion as well as principle of non-discrimination. It places emphasis on 'sensitive expression,' that may involve issues related to hate speech, protection of morals, significance of religion and public order in the contemporary society. It also emphasizes a need for a delicate balance where freedom of expression needs to be weighed against other rights in the ICANN's evaluation of applied-for new gTLD strings.

2.3.1. Free Expression and Internet

33. Online communications and Internet-related issues have become a subject more and more scrutinized by the ECtHR.⁶³ The ECtHR finally recognised in a very forthright way the importance of the Internet in the contemporary communications landscape in its *Ahmet Yildirim v. Turkey* judgment of 18 December 2012:

34. "The Internet has become one of the principal means for individuals to exercise their right to freedom of expression today: it offers essential tools for participation in activities and debates relating to questions of politics or public interest."⁶⁴

35. This recognition clearly places great store on the participatory dimension of free expression. It also recognises the specific functionalities of the Internet – as a medium – that enables enhanced public debate in a democratic society. Internet-related policy developments are increasingly being addressed by the ECHR.⁶⁵ Moreover, there are other instruments prepared by the Committee of Ministers⁶⁶ and the Parliamentary Assembly,⁶⁷ which have political (not legal) persuasion and carry considerable moral force. A range of Council of Europe instruments have been adopted to protect freedom of expression, freedom of association and religion. For example, the Committee of Ministers in the 2011 Recommendation on a new notion of media affirmed that regulation affecting freedom of expression is in itself a form of interference and therefore, should be subject to the scrutiny under Article 10 of the ECHR.⁶⁸

2.3.2. Relevant Provisions

36. Freedom of expression is one of the classic fundamental rights laid down in the constitutions of many countries and in many international treaties, including Article 29 of the Universal Declaration of Human Rights and, Article 19 of the International Covenant on Civil and Political Rights. Similarly to these global instruments, Article 10 of the ECHR provides:

⁶³ See European Court of Human Rights (Research Division), Internet: case-law of the European Court of Human Rights (Strasbourg, Council of Europe, 2011); European Court of Human Rights (Press Unit), Fact sheet – New technologies (Strasbourg, Council of Europe, July 2013). Nina Vajic & Panayotis Voyatzis, "The internet and freedom of expression: a 'brave new world' and the ECtHR's evolving case-law" in Josep Casadevall, Egbert Myjer, Michael O'Boyle & Anna Austin (eds.), *Freedom of Expression: Essays in honour of Nicolas Bratza*, Human Rights Law Review, 16, 2014, pp. 391-407.

⁶⁴ Judgment of the European Court of Human Rights of 18 December 2012, § 54.

⁶⁵ See, e.g., *Editorial Board of Pravoye Delo & Shtekel v. Ukraine*, Judgment of the European Court of Human Rights of 5 May 2011 (on the challenges of sifting through the informational abundance offered by the Internet); *K.U. v. Finland*, Judgment of the European Court of Human Rights of 2 December 2008, (duty of care of ISPs).

⁶⁶ Susanne Nikoltchev & Tarlach McGonagle, Eds., *Freedom of Expression and the Media: Standard-setting by the Council of Europe, (I) Committee of Ministers* – IRIS Themes (Strasbourg, European Audiovisual Observatory, 2011).

⁶⁷ Susanne Nikoltchev & Tarlach McGonagle, Eds., *Freedom of Expression and the Media: Standard-setting by the Council of Europe, (II) Parliamentary Assembly* – IRIS Themes (Strasbourg, European Audiovisual Observatory, 2011).

⁶⁸ Recommendation CM/Rec (2011)7 of the Committee of Ministers to member states on a new notion of media, 21 September 2011.

“1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”

37. Similarly, freedom of association and assembly is also considered one of the classic fundamental rights laid down in many constitutions and international treaties, including Article 20 of the Universal Declaration of Human Rights and, Article 21 of the International Covenant on Civil and Political Rights. Article 11 of the ECHR provides:

“1. Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.

2. No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, 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. This Article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State.”

38. The European Court of Human Rights reiterates that the protection of personal opinions, secured by Article 10 of the ECHR, is one of the objectives of freedom of peaceful assembly as enshrined in Article 11 ECHR.⁶⁹ Freedom of thought and opinion and freedom of expression would be of very limited scope if they were not accompanied by a guarantee of being able to share one’s beliefs or ideas in community with others, particularly through associations of individuals having the same beliefs, ideas or interests.

39. In respect of freedom of thought, conscience and religion, Article 9 of the ECHR, similarly to the UDHR and ICPPR,⁷⁰ provides:

⁶⁹ See: *Schwabe and M.G. v Germany*, Judgment of the European Court of Human Rights (Fifth Section) of 1 December 2011, § 98; *Ezlin v. France*, Judgment of the European Court of Human Rights (Chamber) of 26 April 1991, App. No 11800/85, § 37; *Djavit An v. Turkey*, Judgment of the European Court of Human Rights (Third Section) of 20 February 2003, App. No 20652/92, § 39; *Barraco v. France*, , Judgment of the European Court of Human Rights (Fifth Section) of 5 March 2009, App. no. 31684/05, § 27; *Palomo Sánchez and Others v. Spain*, Judgment of the European Court of Human Rights (Grand Chamber) of 12 September 2011, App. nos. 28955/06, 28957/06, 28959/06 and 28964/06, § 52

⁷⁰ Article 18 of the Universal Declaration of Human Rights and Article 18 of the International Covenant on Civil and Political Rights.

1. *Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief, in worship, teaching, practice and observance.*

2. *Freedom to manifest one's religion or beliefs shall be subject only to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others.*

40. The ECtHR has developed a standard test to determine whether Articles 10, 11 and 9 of the ECHR, have been violated. Permissible restrictions under Articles 10(2), 11(2) and 9(2) to the exercise of these rights must (1) be prescribed by law, (2) be pursued for one of the legitimate aims listed in an exhaustive way in the ECHR and (3) be necessary in a democratic society (proportional to the aims pursued).⁷¹

41. Furthermore, the general principle of equality and non-discrimination is a fundamental element of international human rights law.⁷² Article 14 of the ECHR, similarly to the UDHR and ICCPR,⁷³ provides:

“The enjoyment of the rights and freedoms set forth in the Convention shall be secured without discrimination on any ground such as sex, race, color, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.”

42. The Convention itself does not include direct reference to sexual orientation. However, the ECtHR case-law clearly states that discrimination on the grounds of sexual orientation or gender identity is prohibited and must be prevented.⁷⁴ The Court has established in its case-law that discrimination means “treating differently, without an objective and reasonable justification, persons in analogous, or relevantly similar, situations.”⁷⁵ However, Article 14 ECHR does not prohibit a member State from treating groups differently in order to correct ‘factual inequalities’ between them. For example, special care, and thus discriminatory treatment might be needed for unaccompanied asylum-seeking children. In the same vein,

⁷¹ On Freedom of Expression: this test is laid down in a number of international human rights instruments, in addition to the Article 10 ECHR, see also the United Nations’ International Covenant on Civil and Political Rights (ICCPR), which prescribes that the exercise of the rights to freedom of expression and to seek, receive and impart information may be subject to certain restrictions, “but these shall only be such as are provided by law and are necessary: a) For respect of the rights or reputations of others; b) For the protection of national security or of public order (*ordre public*), or of public health or morals.” (ICCPR, Article 19, § 3). See also United Nations’ Universal Declaration of Human Rights (UDHR), which states that in the exercise of his rights and freedoms, everyone shall be subject only to such limitations as “are determined by law solely for purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society” (UDHR, Article 29, § 2).

⁷² The right to equality and non-discrimination is recognized in Article 14 ECHR, as well as in Article 2 UDHR and is a cross-cutting issue of concern in different UN human rights instruments, such as Articles 2 and 26 ICCPR, Article 2(2) ICESCR, Article 2 CRC, Article 7 CMW and Article 5 CRPD.

⁷³ See note above.

⁷⁴ See for example: *Vejdeland & Ors v Sweden*, Judgment of the European Court of Human Rights (Fifth Section) of 9 February 2012, App. no. 1813/07; *Alekseyev v. Russia*, Judgment of the European Court of Human Rights (First Section) of 21 October 2010, App. nos. 4916/07, 25924/08 and 14599/09

⁷⁵ See: *D.H. and Others v. the Czech Republic [GC]*, App no. 57325/00, § 175, ECHR 2007, and *Burden v. the United Kingdom*, App no. 13378/05 § 60, EHRR 2008.

certain categories of individuals might require special treatment under ICANN's procedural mechanisms. In certain circumstances a failure to attempt to correct inequality through different treatment may in itself give rise to a breach of Article 14 ECHR.⁷⁶ This principle and its relevance will be discussed with a case study on community applicants in paragraph 2.4.4.

2.3.3. Sensitive Expression: from Hate Speech to Protected Disturbing Speech

43. The spectrum of 'sensitive expression' from a legal perspective reaches from types of expression that are (1) not entitled to protection under international human rights law (e.g. incitement to various specified acts), through to types of expression that (2) presumptively would be entitled to protection, despite their morally objectionable character (e.g. negative stereotyping of minorities⁷⁷), to types that may or may not be entitled to protection, depending on the existence and weighting of a number of 'contextual variables' (e.g. extremely offensive expression).⁷⁸

44. Expressions which negate the fundamental values of the ECHR and other international human rights instruments are excluded from the protective realm of the ECHR (and ICCPR and UDHR) as an abuse of rights on the basis of Article 17 of the ECHR.⁷⁹ Although the ECtHR has not always applied the prohibition of abuse of rights consistently,⁸⁰ it generally tends to invoke it in order to ensure that Article 10 protection is not extended to racist,⁸¹ homophobic,⁸² xenophobic or anti-Semitic speech;⁸³ statements denying, disputing, minimizing or condoning

⁷⁶ See *Belgian Linguistics Case (No 2)* (1968) 1 EHRR 252, § 10; *Thlimmenos v Greece*, (2000) 31 EHRR 411, § 44). *Horváth and Kiss v. Hungary*, Judgment of the European Court of Human Rights (Second Section) of 29 January 2013, App. no. 11146/11, § 101.

⁷⁷ Michel Rosenfeld, "Hate Speech in Constitutional Jurisprudence: A Comparative Analysis", 24 *Cardozo Law Review* (2003), 1523-1567, at 1565.

⁷⁸ Michel Rosenfeld, "Hate Speech in Constitutional Jurisprudence: A Comparative Analysis", 24 *Cardozo Law Review* (2003), 1523-1567, at 1565.

⁷⁹ See *Garaudy v. France* (no. 65831/01), 24.06.2003, admissibility decision. Article 17 ECHR is a classical prohibition of abuse of rights clause and one of a several concurrent strategies that Council of Europe employs to counter hate speech. These strategies have been developed pursuant to the Council's various treaties and other standard-setting and monitoring initiatives. Article 17 reads: "Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention".

⁸⁰ For in-depth analysis, see: Hannes Cannie & Dirk Voorhoof, "The Abuse Clause and Freedom of Expression in the European Human Rights Convention: An Added Value for Democracy and Human Rights Protection?", 29 *Netherlands Quarterly of Human Rights* (No. 1, 2011), pp. 54-83; David Keane, "Attacking hate speech under Article 17 of the European Convention on Human Rights", 25 *Netherlands Quarterly of Human Rights* (No. 4, 2007), pp. 641-663.

⁸¹ Examples include: *Seurot v. France*, Inadmissibility decision of the European Court of Human Rights (Second Section) of 18 May 2004, Appn. No. 57383/00; *Norwood v. United Kingdom*, Inadmissibility decision of the European Court of Human Rights of 16 November 2004, Appn. No. 23131/03, Reports 2004-XI.

⁸² *Vejdeland & others v. Sweden*, Judgment of 9 February 2012. In 2010, the Committee of Ministers and Parliamentary Assembly both adopted texts setting out measures to combat discrimination on grounds of sexual orientation or gender identity, respectively: Recommendation CM/Rec(2010)5 of the Committee of Ministers to member states on measures to combat discrimination on grounds of sexual orientation or gender identity, 31 March 2010; Parliamentary Assembly of the Council of Europe, Resolution 1728 (2010), "Discrimination on the basis of sexual orientation and gender identity", 29 April 2010, and Parliamentary Assembly of the Council of Europe, Recommendation 1915 (2010), "Discrimination on the basis of sexual orientation and gender identity", 29 April 2010.

⁸³ *Garaudy v. France* (no. 65831/01), 24.06.2003, admissibility decision.

the Holocaust,⁸⁴ or (neo-) Nazi ideas.⁸⁵ As such, the Court has routinely held cases involving these types of expression to be manifestly incompatible with the Convention's fundamental values and therefore inadmissible.

45. The term hate speech is not enshrined in the ECHR, and the Court used the actual term for the first time in 1999,⁸⁶ but without explaining its introduction, intended purpose or relationship with existing case-law. Despite its frequent use, there is no clear or unique understanding of what is 'hate speech,' and the definitions and conceptions vary in different countries.⁸⁷ According to the Committee of Ministers of the Council of Europe, hate speech is understood as "covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin."⁸⁸ Further, the Additional Protocol to the Budapest Convention on Cybercrime (2003) has defined racist and xenophobic material as "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors."⁸⁹

46. The Court, on the other hand, has refrained from defining the term.⁹⁰ Instead, it prefers to "analyze each case submitted to it on its own merits and to ensure that its reasoning – and its case-law – is not confined within definitions that could limit its action in future cases".⁹¹ This flexible approach is of particular significance in the context of ICANN's procedures and policies related to gTLDs, as it suggests that a sustainable approach is needed with regular discussions and early engagement with the Council of Europe. These issues will be further explored in the following analysis.

⁸⁴ See, for example, *Pavel Ivanov v. Russia*, Inadmissibility decision of the European Court of Human Rights (First Section) of 20 February 2007, Appn. No. 35222/04.

⁸⁵ 1 Examples include: *Garaudy v. France*, Inadmissibility decision of the European Court of Human Rights (Fourth Section) of 24 June 2003, Appn. No. 65831/01, Reports 2003-IX. See further, Tarlach McGonagle, "Wresting (Racial) Equality from Tolerance of Hate Speech" (2001) 23 *Dublin University Law Journal* 21-54.

⁸⁶ The term was first used in four Judgments of the European Court of Human Rights, all of 8 July 1999: *Sürek v. Turkey* (No. 1), § 62; *Sürek & Özdemir v. Turkey*, § 63; *Sürek v. Turkey* (No. 4), § 60 and *Erdogdu & Ince v. Turkey*, § 54.

⁸⁷ See Malinowski, J., 'What is Hate Speech?' – Synergy Magazine, available at <http://issuu.com/vpmarketing/docs/synergy-53/28/> (visited 20/05/2014).

⁸⁸ See Appendix to Recommendation No. R (97) 20, available at [http://www.coe.int/t/dghl/standardsetting/hrpolicy/other_committees/dh-lgbt_docs/CM_Rec\(97\)20_en.pdf/](http://www.coe.int/t/dghl/standardsetting/hrpolicy/other_committees/dh-lgbt_docs/CM_Rec(97)20_en.pdf) visited 03/05/2014.

⁸⁹ See Article 2 of the Additional Protocol to the Budapest Convention on Cybercrime (2003), concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm/> (visited 21/05/2014).

⁹⁰ See further: Tarlach McGonagle, *Minority rights, freedom of expression and of the media: dynamics and dilemmas*, op. cit., Chapters 6.2.1 and 7.1.

⁹¹ Françoise Tulkens, "When to say is to do: Freedom of expression and hate speech in the case-law of the European Court of Human Rights", in Josep Casadevall, Egbert Myjer, Michael O'Boyle & Anna Austin, Eds., *Freedom of Expression: Essays in honour of Nicolas Bratza* (Oisterwijk, The Netherlands, Wolf Legal Publishers, 2012), pp. 279-295, at 281.

2.3.4. Protected Expressions: From Political Expression to Religious Expression

47. The right to freedom of expression necessarily covers expression that may “offend, shock or disturb” certain groups in society (which is not the same thing as a right to offend),⁹² as well as the content that is unsuitable for particular age groups (albeit may be subject to conditions as to its distribution).⁹³ The ECtHR has accorded the protection of the right to freedom of expression to various forms of expression which might not be regarded as acceptable by various communities and groups. Therefore, merely polemical texts without actually constituting hate speech⁹⁴ and fierce critique of secular and democratic principles are protected as part of a political discourse.⁹⁵ Political speech, especially when contributing to a wider debate on the issues raised, which is in consonance with the ECHR’s aims, is protected,⁹⁶ as is political speech that neither calls for nor condones violence.⁹⁷ The ECtHR has also found that general prohibitions of pejorative statements in comparative newspaper advertising may constitute a disproportionate intrusion into freedom of commercial speech of the media sector.⁹⁸

48. Council of Europe states are given a wider margin of appreciation in evaluating the permissible interferences with freedom of expression when they are necessary for the protection of morals and public order. The ECtHR has found that certain notions, such as morals and significance of religion, lack a uniform conception and interpretation and therefore benefit from a larger margin of appreciation.⁹⁹ The margin of appreciation of national authorities is wide but not unlimited and the ECtHR strictly examines whether the interference satisfies Article 10(2) requirements.¹⁰⁰ Combining the margin of appreciation with the other interpretative principles by the ECtHR introduced in Chapter 1 would suggest that many decisions by ICANN not to grant a particular applied-for gTLD string would need to pass a strict proportionality test in order to satisfy the ECHR requirements.

49. The following paragraphs will analyze how these international human rights obligations apply to the evaluation procedures of a new applied-for gTLD strings.

⁹² *Handyside v. the United Kingdom*, Judgment of the European Court of Human Rights of 7 December 1976, Series A, No. 24, § 49. See further, Onora O’Neill, “A Right to Offend?”, *The Guardian*, 13 February 2006; Francesca Klug, “Freedom of Expression Must Include a Licence to Offend”, 1(3) *Religion and Human Rights* (2006), 225-227.

⁹³ See the CoE, Recommendation CM/Rec(2012)4 of the Committee of Ministers to member states on the protection of human rights with regard to social networking services, adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers’ Deputies, available at <https://wcd.coe.int/ViewDoc.jsp?id=1929453/> visited 06/05/2014.

⁹⁴ *Lehideux et Isorni v. France* (no. 24662/94), 23.09.1998.

⁹⁵ *Gündüz v. Turkey* (no. 35071/97), 04.12.2003.

⁹⁶ *Otegi Mondragon v. Spain* (no. 2034/07), 15.03.2011.

⁹⁷ *Faruk Temel v. Turkey* (no. 16853/05), 01.02.2011.

⁹⁸ *Krone Verlag GmbH & Co KG v. Austria* (no. 3) (no. 39069/97), 11.12.2003.

⁹⁹ *Wingrove v. United Kingdom* (no. 17419/90), 25.11.1996, § 58.

¹⁰⁰ In *Open Door and Dublin Well Woman v. Ireland* (no. 14234/88) 29.10.1992, § 68. Involving allegations on restrictions on the right to receive and impart information on issues related to abortion the ECtHR found that the imposition by the concerned state of a permanent prohibition to provide advice in this context was too large and disproportionate.

2.4. Human Rights Analysis of the gTLD Application Procedures

50. ‘Sensitive expression’ in the Applicant Guidebook is understood by the GAC as all forms of expression to which “sensitivities regarding terms with national, cultural, geographic and religious significance” might apply. GAC denotes special significance to the issue of ‘sensitive expression’ and believes that the absence of culturally objectionable and/or sensitive strings contributes to the security and resilience of the DNS.¹⁰¹

51. ‘Sensitive speech’ can be covered or not covered by the right to freedom of expression, and the challenge for ICANN in the evaluation of applied-for gTLDs is to identify the tipping point at which a sensitive speech is not protected under international law so that its evaluation is consistent with human rights.

52. It must be noted that while it appears that the prohibition of abuse of rights as set out in Article 17, *prima facie* denies protection to a range of particularly abusive expression, a deeper analysis of the ECtHR case-law¹⁰² suggests that substantive examinations are favored by the ECtHR. The inconsistent application of Article 17 and far-reaching consequences of its application to freedom of expression suggest that blanket prohibitions of certain terms & words by ICANN should be done very carefully and only in moderation.¹⁰³ The *Handyside* judgment recognizes that in a democratic society, space has to be created and sustained for public discussion and debate. Democratic society is not without its rough edges and pluralistic public debate necessarily involves disagreement and confrontation between opposing viewpoints. The disagreement and confrontation raised by terms such as ‘sucks’ or ‘gay’ – even when expressed in strong terms – ordinarily comes within the scope of the protection offered by Article 10.

53. The next section will focus on examples in practice and the need for a delicate balancing exercise when freedom of expression and other rights are weighted.

2.4.1 Problematic and Sensitive Applied-For Strings

54. There have been several cases and disputes involving potentially ‘sensitive expressions’ in applied-for gTLDs which exemplify the delicate balance needed to protect the fundamental rights of applicants and other Internet users. A few applications have so far received outright

¹⁰¹ Governmental Advisory Committee “GAC Principles Regarding New gTLDs” 28 March 2007, Clause 2.1(a) and (b). in particular Clause 2.1 (b): New gTLDs should respect a) the provisions of the Universal Declaration of Human Rights which seeks to affirm “fundamental human rights, in the dignity and worth of all human beings and in the equal rights of men and women” b) the sensitivities regarding terms with national, cultural, geographic and religious significance.” See also GAC letter to ICANN Board, 4 August 2010 Re: Procedures for Addressing Culturally Objectionable and/or Sensitive Strings: The GAC firmly believes that the absence of any controversial strings in the current universe of top level domains (TLDs) to date contributes directly to the security and stability of the domain name addressing system (DNS) and the universal resolvability of the system”. Available at <http://www.icann.org/en/correspondence/gac-to-dengate-thrush-04aug10-en.pdf>. See § 67 of the Comments of 2012 for more details.

¹⁰² E.g., cases where what initially appeared as a ‘hate speech’ was found to be protected under Article 10 – *Jersild v. Denmark*, Judgment of the European Court of Human Rights of 23 September 1994, Series A, No. 298; *Lehideux & Isorni v. France*, 23 September 1998, Reports of Judgments and Decisions, 1998-VII; *Gündüz v. Turkey*, Judgment of the European Court of Human Rights (First Section) of 4 December 2003.

¹⁰³ In the same vein, leading commentators have called for refraining from using Article 17 in favor of the substantive test when hate speech is examined, see Hannes Cannie & Dirk Voorhoof, “The Abuse Clause and Freedom of Expression in the European Human Rights Convention: An Added Value for Democracy and Human Rights Protection?”, at 83.

objections such as '.gcc' (contested by some of the Gulf countries, claiming similarity between this string and the Gulf Cooperation Council) and '.africa', submitted by DotConnectAfrica (for lack of official support by governments from the region, given to another identical application). So far, GAC advice has come for the most part in the form of 'safeguards' rather than outright objections. The GAC noted that specific categories of TLDs require additional protections or restrictions to be implemented.

55. In addition to the 12,000 public comments received following the publication of the applied-for new top level domains, ICANN has also received over 240 comments from various governments around the world, issued as Early Warnings from the GAC, such as for the strings '.fail', '.gripe', '.sucks' and '.wtf' due to their "overtly negative or critical connotation". As a result, many individuals, businesses and organizations may seek to protect their brands or reputation which, according to GAC, calls for better mechanisms to address the potential for a high level of defensive registrations.

56. Concerns were also raised over strings that are linked to a regulated market sector, such as '.accountant', '.lawyer' and '.doctor', where misuse can potentially result in serious harm to consumers. National and religious concerns were also raised by various governments. For example, the government of UAE expressed its serious concern with regard to '.islam' on the grounds of lack of community involvement and support as well as private control over the name. The government of Samoa issued an Early Warning for '.website', urging that it not be granted as it could be confused with the country's ccTLD '.ws'. According to the submission, '.ws' has been "extensively marketed throughout the world as synonymous with 'WebSite' and is an important source of revenue for the small nation".

57. It is not only the GAC's 'Early Warning' channel, sparking controversy, which may involve human rights considerations. For example, the '.xxx' case demonstrates that the procedures and mechanisms that may lead to rejection of an applied-for gTLD could intersect. In the case of '.xxx', many objections were filed on the so-called 'Community Objections' ground for refusal, which relates to cases when "there is a substantial opposition to the gTLD application from a significant portion of the community to which the gTLD string may be explicitly or implicitly targeted."¹⁰⁴ Neither a substantial number of objections filed, nor GAC's Advice, were decisive for the final deliberation of the ICANN Board, which approved the string.¹⁰⁵ It explained its reasons with regard the potential threat of TLD blocking to the universal resolvability and stability of the DNS by stating that "[t]he issue of governments (or any other entity) blocking or filtering access to a specific TLD is not unique to the issue of the '.xxx' gTLD. Such blocking and filtering exists today. While we agree that blocking of TLDs is generally undesirable, if some blocking of the '.xxx' gTLD does occur there is no evidence that the result will be different from the blocking that already occurs."¹⁰⁶

¹⁰⁴ ICANN, Applicant Guidebook, Module 3, at 3-4.

¹⁰⁵ See 18 March 2011 ICANN Board Rationale for Approving Registry Agreement with ICM's for .XXX sTLD, Section V, A, p. 18 "The negative community impact will most likely be on those that do not support the idea of the introduction of the .XXX sTLD. However, refusing to approve registry agreements with strings that do not have unanimous community support, is not an acceptable option as ICANN continues to move toward the introduction of even more new gTLDs."

¹⁰⁶ See 18 March 2011 ICANN Board Rationale for Approving Registry Agreement with ICM's for .XXX sTLD, Section V, 4, c, p. 16.

2.4.2. Freedom of Expression and Trademarks

58. Two grounds for objection under the public objection procedures, – the string confusion objection and the legal rights objection – for initiating Dispute Resolution Procedures are obviously focused on the protection of traditional rights. A delicate balance is at stake where freedom of expression needs to be weighed against the property rights of trademark owners. A gTLD objected to under a string confusion objection must qualify as confusingly similar to an existing gTLD or a gTLD applied-for in the same application round.¹⁰⁷ A legal rights objection can occur when an applied-for gTLD infringes on the intellectual property rights of the objector, who must have a legal right over the disputed domain name to possess standing for this objection.¹⁰⁸ Invoking trademark protection should not be used as a means to limit the freedom of expression.¹⁰⁹

2.4.3. Sensitivities and Varying Levels of Acceptable Criticism

59. The examples of ‘.fail’, ‘.gripe’, ‘.sucks’ and ‘.wtf’ demonstrate that there is tension in answering the question whether people should have the right to say, for example, that a religion, a company or a politician ‘sucks’. The European Court of Human Rights suggests that the level of acceptable criticism of expression may vary according to the circumstances. In the *Lingens* case, the Court seminally found that the “limits of acceptable criticism” are wider for politicians than for private individuals because politicians “inevitably and knowingly” lay themselves “open to close scrutiny of [their] every word and deed by both journalists and the public at large, and [they] must consequently display a greater degree of tolerance”.¹¹⁰ In the same vein, one could think that the private corporate giants, operating transnationally, should also display a greater degree of tolerance and thereby accept criticism of their activities or policies. The limits of permissible criticism are even wider concerning the government because in a democratic system “the actions or omissions of the government must be subject to the close scrutiny not only of the legislative and judicial authorities but also of public opinion”.¹¹¹

60. As regards political speech, it must be noted that as politicians, political parties and governments increasingly rely on new information and communications technologies, the tensions between political expression and hate speech will accordingly play out more and more in an online environment. It is important for ICANN to be aware of the potential of the importance of specifying the notion of ‘hate speech.’ For instance, in 2012, the ECtHR recognized homophobic hate speech for the first time.¹¹² It is unclear whether the Court will in

¹⁰⁷ ICANN, Applicant Guidebook, Module 3, at 3-4. The International Centre for Dispute Resolution (ICDR) handles string confusion objections.

¹⁰⁸ *Ibid* §3.2.2.2.

¹⁰⁹ W. Sakulin, ‘Trademark Protection and Freedom of Expression: An Inquiry into the Conflict between Trademark Rights and Freedom of Expression under European, German, and Dutch Law,’ Amsterdam, 2010. Online: <http://dare.uva.nl/document/169804>, p. 210.

¹¹⁰ *Lingens v. Austria*, app. no 9815/82, judgment of 8 July 1986, § 42.

¹¹¹ *Incal v. Turkey*, Judgment of the European Court of Human Rights of 9 June 1998, Reports 1998-IV, § 54; *Arslan v. Turkey*, Judgment of the European Court of Human Rights (Grand Chamber) of 8 July 1999, § 46, *Öztürk v. Turkey*, Judgment of the European Court of Human Rights (Grand Chamber) of 28 September 1999, ECHR 1999-VI; § 66, *Sener v. Turkey*, Judgment of the European Court of Human Rights of 18 July 2000, § 40.

¹¹² *Vejdeland & others v. Sweden*, Judgment of 9 February 2012. In 2010, the Committee of Ministers and Parliamentary Assembly both adopted texts setting out measures to combat discrimination on grounds of sexual orientation or gender identity, respectively: Recommendation CM/Rec(2010)5 of the Committee of Ministers to member states on measures to combat discrimination on grounds of sexual orientation or gender identity, 31 March 2010; Parliamentary Assembly of the Council of Europe, Resolution 1728 (2010), “Discrimination on the basis

future recognize sexist or misogynist hate speech or hate speech targeting persons with disabilities – types of hate speech that present strong cases for inclusion within contemporary understandings of the term. Bearing this in mind, ICANN should adopt a very careful approach to balancing evaluations which should not lead to rejected applications such as ‘.wtf’ or ‘.sucks’, and on the other hand, one should ensure that ‘hate speech’ is not tolerated in the applied-for gTLDs.

61. To sum up, restricting offensive expression, such as ‘.sucks’ or ‘.fail’ in gTLDs would restrict the ability of all speakers, commercial and non-commercial; ICANN should consider legal models outside of trademark law to better address the balance of speech rights.¹¹³ GAC advice that an applied gTLD string should not proceed on grounds of other sensitivities would need to be considered on a case by case basis. As is clear from the case-law of the ECtHR, differences between sensitivities of a national, cultural or religious nature and those of a political nature may frequently be very difficult to determine. A more systematically applied human rights approach to GAC advice would provide the GAC with opportunities to explore a wider range of options for advice which can reflect more nuanced and complex considerations.

2.4.4. Case Study on String Contention Procedures: Community Applications

62. To what extent does ICANN serve the global public interest with its current Community Priority Evaluation (CPE) process, from a European human rights perspective? This question will be answered on the basis of a concrete example, that of the applications for the ‘.gay’ TLD. There are 4 applicants for the ‘.gay’ TLD, of which there are three standard applicants and one community applicant. Within the human rights framework presented above and in particular the right to freedom of assembly and association, ICANN’s procedures for community applications are assessed below with a case study on the ‘.gay’ TLD application. The focus of this analysis is in the scope of ‘community’ and the responsibility of states under international human rights law to take positive measures to protect certain vulnerable groups.

63. The preference for community-based TLDs in the contention process is based on policy advice from the GNSO and is intended to ensure that community-based applicants receive the TLD string to which their community is strongly related. “Perhaps the most important aspect of the suggested categories is that an applicant within these categories does, in fact, receive the string associated with its community, and that is what the existing process is designed to do.”¹¹⁴ Although further arguments for this preference cannot be found, the added value, mostly non-commercial, when a TLD is managed by and for the community, is perfectly understandable. Community-based TLD’s could take appropriate measures to ensure that the right to freedom of expression of their community can be effectively enjoyed without discrimination, including with respect to the freedom to receive and impart information on

of sexual orientation and gender identity”, 29 April 2010, and Parliamentary Assembly of the Council of Europe, Recommendation 1915 (2010), “Discrimination on the basis of sexual orientation and gender identity”, 29 April 2010.

¹¹³ Christine Haight Farley, ‘Convergence and Incongruence: Trademark Law and ICANN’s Introduction of New Generic Top-Level Domains’, John Marshall Journal of Computer & Informaton Law, 25, no. 4 (Summer 2009): 625-633, p. 631.

¹¹⁴ ICANN, ‘Letter from ICANN chair to GAC chair regarding GAC’s comments on DAGv3’ (published in October 2009), <<http://gnso.icann.org/mailling-lists/archives/council/msg09500.html>> accessed 13 May 2014; ICANN, ‘Draft ICANN Board – GAC Consultation: Providing Opportunities For All Stakeholders, Including Those From Developing Countries’, p. vii, <<http://archive.icann.org/en/topics/new-gtlds/gac-board-providing-opportunities-stakeholders-21feb11-en.pdf>> accessed 13 May 2014; ICANN, ‘New gTLD Draft Applicant Guidebook Version 3 – Public Comments Summary and Analysis, p 9, <<http://archive.icann.org/en/topics/new-gtlds/summary-analysis-agv3-15feb10-en.pdf>> accessed 13 May 2014

subjects dealing with their community. They could also take additional measures to ensure that the right to freedom of peaceful assembly can be effectively enjoyed, without discrimination.

2.4.4.1. The Scope of ‘community’

64. The scope of a ‘community’ determines to what extent specific groups deserve protected status. A broad interpretation will provide a higher amount of community applicants with protected status compared to the situation in which a more limited interpretation is being used. A narrow interpretation could restrict the ability of community organizations to associate i.e. to group them together to achieve goals. It could therefore impact on the right to freedom of assembly and association and the positive obligation resting upon states to protect vulnerable groups.

65. A community applicant must score 14 out of 16 points in the Community Priority Evaluation. A maximum of 4 points can be obtained on the criterion ‘Community Establishment’; 2 points will be awarded if the community is a clearly delineated, organized and pre-existing community. Insufficient delineation and pre-existence will lead to 0 points.¹¹⁵ In both its Beijing and Durban Communique, the GAC noted concerns about the high threshold for passing the CPE. It therefore advised to take better account of community views, and improve outcomes for communities, irrespective of whether those communities have utilized ICANN’s formal community processes to date.¹¹⁶

66. The GNSO recommendation from which the Applicant Guidebook definitions are derived, as well as the Applicant Guidebook itself and GAC Advice indicate that a ‘community’ should be interpreted broadly. According to the GNSO, this broad interpretation will include, “for example, an economic sector, a cultural community, or a linguistic community”.¹¹⁷ The Applicant Guidebook states that a community can consist of legal entities, individuals or of a logical alliance of communities.¹¹⁸ Additionally, the GAC advised the ICANN Board to clarify that “Community-based strings include those that purport to represent or that embody a particular group of people or interests based on historical components of identity, such as nationality, race or ethnicity, religion or religious affiliation, culture or particular social group, and/or a language or linguistic group”.¹¹⁹

67. This broad scope appears to have been changed when The Economist Intelligence Unit (EIU) published their Community Priority Evaluation Guidelines. It sets out that “delineation relates to the membership of a community, where a clear and straight-forward membership definition scores high, while an unclear, dispersed or unbound definition scores low. The following non-exhaustive list denotes elements of straight-forward member definitions: fees, skill and/or accreditation requirements, privileges or benefits entitled to members, etc”.¹²⁰ By doing so, it seems to renounce the previous mentioned broad interpretation of communities.

¹¹⁵ ICANN, Applicant Guidebook, Module 4.2.3

¹¹⁶ See: GAC, ‘GAC Communique – Durban, South Africa, 17 July 2013; GAC, ‘GAC Communique – Beijing, People’s Republic of China, 11 April 2013

¹¹⁷ ICANN Generic Names Supporting Organisation, ‘Final Report Introduction of New Generic Top-Level Domains’, 8 August 2007 <<http://gnso.icann.org/en/issues/new-gtlds/pdp-dec05-fr-parta-08aug07.htm>> accessed 13 May 2014

¹¹⁸ ICANN, Applicant Guidebook, Module 4.2.3

¹¹⁹ ICANN, ‘GAC Scorecard Sorted’, 14 March 2011 <<http://archive.icann.org/en/topics/new-gtlds/gac-scorecard-sorted-14mar11-en.pdf>> accessed 13 May 2014

¹²⁰ EIU, ‘Community Priority Evaluation (CPE) Guidelines’, 27 September 2013, <<http://newgtlds.icann.org/en/announcements-and-media/announcement-27sep13-en>> accessed 13 May 2014

This apparent narrow interpretation seems to be more specific and stringent than cultural usage of the word community.

68. UNESCO makes it clear that ‘community’ has a wide range of meanings and emphasizes that the concepts of community, identity and culture are used interchangeably in literature. UNESCO distinguishes three types of communities: geographical communities, communities of identities (such as those based on music, religion or sexuality) and communities of interests (such as social movements, like women’s rights).¹²¹

69. The notion of ‘community’ has not played an important role in the broader human rights context, neither specifically in the case-law of the European Court of Human Rights. The comparable notion of ‘associations’ can be highly relevant in this respect. As the UN Special Representative of the Secretary-General on human rights defenders stresses: “an association refers to any groups of individuals or any legal entities brought together in order to collectively act, express, promote, pursue or defend a field of common interests”.¹²² The European Court of Human Rights interprets the term association very broadly, and defines association as any form of voluntary grouping for a common goal.¹²³ The Court requires a certain degree of institutional organization, but this does not mean that an association must have legal entity status in order to enjoy protection afforded by Article 11 ECHR. The association has to be distinguishable from a mere gathering of individuals for the sake of socializing and therefore some degree of continuity and institutional elements must be in place.¹²⁴

70. The scope of ‘community’ could have an impact on human rights. A narrow interpretation could restrict the ability of community organizations to associate, for example, to group them together to achieve goals. The Community Priority Evaluation Guidelines as published by the Economist Intelligence Unit (EIU) use a stringent interpretation of communities, with the result that certain diverse and heterogeneous communities are not protected. The precedence given to community-based applicants would then not apply to communities, such as the LGBT community, while in the human rights context there is no doubt that the LGBT community can be seen as a community, that often is considered as a vulnerable group and/or a minority that requires special consideration.

2.4.4.2. Positive measures

71. The community applicant for ‘.gay’ (there are three other standard applicants) expressed an intention to operate in the interest of the community and for the benefit of the community. It developed policies that specifically apply to the gay community, such as protective measures against anti-gay hate speech. Additionally, the community applicant plans to pass on 67% of the revenue generated by the ‘.gay’ domain to non-profit LGBT organizations. The other applicants have not expressed the intention of specifically serving the

¹²¹ Pramila Aggarwal, ‘Understanding the Community’, <http://www.unesco.org/education/aladin/paldin/pdf/course01/unit_06.pdf> accessed 13 May 2014

¹²² UN GA, ‘Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai’, 21 May 2012, A/HRC/20/27, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-27_en.pdf accessed 13 May 2014; UN GA, ‘Report of the Special Representative of the Secretary-General on human rights defenders’ 1 October 2004, A/59/401, § 46, <<http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N04/533/18/PDF/N0453318.pdf?OpenElement>> accessed 13 May 2014

¹²³ *Young, James, Webster v. the United Kingdom*, Judgment of the European Court of Human Rights (Plenary) of 13 August 1981, App. nos. 7601/76; 7806/77.

¹²⁴ See: *McFeeley v. The United Kingdom*, Judgment of the European Commission of Human Rights (Plenary) of 15 May 1980, App. no. 8317/78

homosexual community. Moreover, the other applicants deny the existence of the gay community or claim that they do not target the string '.gay' to the gay community.¹²⁵ The International Centre for Expertise of The International Chamber of Commerce claimed that operating the '.gay' TLD by one of these applicants will not allow for more discrimination or more expression of abusive, hateful and harmful views than already exists.¹²⁶ Therefore it concluded that these standard applicants "do no harm" the community by their policies.

72. The International Centre for Expertise of The International Chamber of Commerce advanced that the loss of the chance to operate its own '.gay' TLD might be regarded as detrimental to the legitimate interests of the gay community.¹²⁷ Specific action might be required in order to ensure the full enjoyment of the human rights of the LGBT community. The starting point for such measures is the need to combat a high level of discrimination based on sexual orientation or gender identity. Lesbian, gay, bisexual and transgender individuals have been discriminated against for centuries and are still subjected to homophobia, transphobia and other forms of widespread and enduring intolerance. This leads to hostile acts ranging from social exclusion to discrimination – all over Europe and in all areas of life, on grounds of sexual orientation or gender identity. As a result, countless people have to conceal or suppress their identity and to live lives of fear and invisibility.¹²⁸

73. The ECHR allows states to treat a group unequally in certain circumstances in order to "correct factual inequalities" between them.¹²⁹ The ECHR has recognized that to avoid discrimination or secure equal rights, it may be necessary sometimes to treat an individual or group differently precisely because their situation is different from others.¹³⁰ In certain circumstances, a failure to attempt to correct inequality through different treatment may in itself give rise to a breach of the prohibition of discrimination. A difference of treatment is, however, discriminatory if it has no objective and reasonable justification; in other words, if it does not pursue a legitimate aim or if there is not a reasonable relationship of proportionality between the means employed and the aim sought to be realized. States enjoy a margin of appreciation in assessing whether and to what extent differences in otherwise similar situations justify a different treatment.¹³¹

¹²⁵ See: The International Centre for Expertise of The International Chamber of Commerce, Case No EXP/394/ICANN/11, The International Lesbian Gay Bisexual Trans and Intersex Association vs. United TLD Holdco LTD; The International Centre For Expertise of The International Chamber of Commerce, Case No EXP/392/ICANN/9, The International Lesbian Gay Bisexual Trans and Intersex Association vs. Top Level Design, LLC; The International Centre For Expertise of The International Chamber of Commerce, Case No EXP/393/ICANN/10, The International Lesbian Gay Bisexual Trans and Intersex Association vs. Top Level Domain Holdings Limited.

¹²⁶ Ibid

¹²⁷ See: The International Centre For Expertise of The International Chamber of Commerce, Case No EXP/394/ICANN/11, The International Lesbian Gay Bisexual Trans and Intersex Association vs. United TLD Holdco LTD, § 22.

¹²⁸ Council of Europe, Draft Recommendation CM/Rec(2010) of the Committee of Ministers to member states on measures to combat discrimination on grounds of sexual orientation or gender identity, Explanatory Memorandum, CM(2010)4 add3 rev 2, 29 March 2010 <http://www.coe.int/t/dg4/lgbt/Source/Motives_EN.pdf> accessed 13 May 2014.

¹²⁹ *Runkee and White v The United Kingdom*, Judgment of the European Court of Human Rights (Fourth Section) of 10 May 2007, App. nos. 42949/98 and 53134/99, § 35; See also: *Stec and Others v. the United Kingdom*, Judgment of the European Court of Human Rights (Grand Chamber) of 12 April 2006, App nos. 65731/01 and 65900/01, § 51.

¹³⁰ *Thlimmenos v. Greece*, Judgment of the European Court of Human Rights (Grand Chamber) of 6 April 2000, App. no 34369/97, § 44.

¹³¹ *Stec and Others v. the United Kingdom*, Judgment of the European Court of Human Rights (Grand Chamber) of 12 April 2006, App nos. 65731/01 and 65900/01, § 51.

74. Positive state measures to protect against discriminatory treatment, including by non-state actors, are fundamental components of the international system for protecting human rights and fundamental freedoms.¹³² The Committee of Ministers Recommendation R(97)21 on the Media and the Promotion of a Culture of Tolerance stresses the importance of the professional practices of the media and the responsibility they have to protect various groups and individuals from negative stereotyping or to publicize their positive contributions to society. Media organizations, including those operating on the Internet, are encouraged to promote in their own practices a culture of respect, tolerance and diversity in order to avoid negative and stereotyped representations of lesbian, gay, bisexual and transgender persons and the use of degrading material or sexist language.¹³³ The content related decisions made by ICANN may result in decisions made on the availability of information on the Internet, and can be regarded as similar to editorial judgements made by the media. Such editorial activities may entail special guarantees and responsibilities with regard to the protection of various groups and individuals.¹³⁴

75. Discrimination and hate motivated incidents are very upsetting for the victims and the community to which they belong. From the victim's point of view, having suffered such a treatment because of an immutable fundamental aspect of their identity is particularly difficult. Discrimination and hate crime also threaten the very basis of democratic societies and the rule of law, in that they constitute an attack on the fundamental principle of equality in dignity and rights of all human beings. Lesbian, gay, bisexual and transgender persons are the target of many such crimes or incidents.¹³⁵ The positive obligations of states under the ECtHR in this respect would require advocating that ICANN adopts and effectively enforces specific measures in order to combat discrimination on grounds of sexual orientation or gender identity, to ensure respect for human rights of lesbian, gay, bisexual and transgender persons and to promote tolerance towards them.

76. The concept of vulnerable groups could be a basis upon which ICANN can prioritize between different applicants for TLDs. Vulnerability reasoning enables ICANN to take positive measures to proactively serve the public interest. Safeguards comparable to the Category 1 safeguards for regulated markets could be adopted to make sure that whoever applies for a gTLD that relates to a vulnerable community needs to prove it has a solid plan.

2.4.5. Auction Procedures: Equality & Non-Discrimination

77. In most cases where multiple applicants apply for a single new gTLD it is expected that contention will be resolved by the community priority evaluation, or through voluntary agreement among the involved applicants. If that is not the case, auctions will take place to determine the winner of each contention set.¹³⁶ Especially relevant in respect of the String

¹³² Council of Europe, Recommendation CM/Rec(2010)5 of the Committee of Ministers to member states on measures to combat discrimination on grounds of sexual orientation or gender identity (31 March 2010) <http://www.coe.int/t/dg4/lgbt/Source/RecCM2010_5_EN.pdf> accessed 13 May 2014.

¹³³ http://www.coe.int/t/dg4/lgbt/Source/Motives_EN.pdf

¹³⁴ See: Wolfgang Benedek, Joy Liddicoat and Nico van Eijk, 'Comments Relating to Freedom of Expression and Freedom of Association with regard to New Generic Top Level Domains' Council of Europe DG-I(2012)4, 12 October 2012, p 9

¹³⁵ Council of Europe, Draft Recommendation CM/Rec(2010)... of the Committee of Ministers to member states on measures to combat discrimination on grounds of sexual orientation or gender identity, Explanatory Memorandum, CM(2010)4 add3 rev 2, 29 March 2010 <http://www.coe.int/t/dg4/lgbt/Source/Motives_EN.pdf> accessed 13 May

¹³⁶ An auction will not take place to resolve contention in the case where the contending applications are for geographic names. See: ICANN, 'Applicant Guidebook', Module 4.3

Contention Procedures, and Auctions, is the general principle of equality and non-discrimination, a fundamental element of international human rights law.¹³⁷ The prohibition of discrimination is closely linked to the principle of equality which holds that all people are born and remain free and equal in dignity and rights.

78. The auction procedure constitutes an inappropriate method to serve the public interest, since it has the potential to disproportionately award gTLDs to financially richer entities. The current procedure does not seem to provide any incentive for financially strong applicants to resolve contention through voluntary agreement among involved applicants. ICANN's public interest role seems to conflict with such discrimination and may be compared to those of the public service media in the information society.

79. The authors are concerned that pluralism and diversity can be threatened by auctions as a way to allocate a scarce resource, because this could lead to the concentration of TLDs in the hands of a small group of wealthy portfolio applicants. In addition to a risk of higher costs for acquiring the right to use a second level domain associated to these gTLDs, the risk associated with concentration also lies in the possibility of limited access to diverse information and content.¹³⁸ As a consequence of the responsibilities of states in this respect, would it be desirable for ICANN to strike a balance between economic interests and objectives of common interest? States have a role to play in ensuring that the fundamental values of pluralism and diversity are not compromised by ICANN's auction procedures.

2.5. Conclusion

80. In conclusion, gTLDs may include expression or be used as spaces for online association and therefore, entail a human rights and fundamental freedoms dimension which should be considered together with other technical matters. The evaluation of applied-for new gTLDs may involve content-related considerations that need to have the general interest in sight. While ICANN's judgement should not be interfered with unjustifiably, ICANN should exercise its role with due regard for fundamental rights and freedoms and in full compliance with international standards. In particular, any interference with the exercise of the right to freedom of expression and the right to freedom of association should be more systematically tested against the requirements of international human rights law and the global public interest.

81. Technical and policy choices involved in the digital environment should not be predominantly determined by economic factors. ICANN ought also to take account of social, cultural and political factors. A balance must be struck between economic interests and objectives of common interest. A balance might need to be struck between the development

¹³⁷ The right to equality and non-discrimination is recognized in Article 14 ECHR, as well as in Article 2 UDHR and is a cross-cutting issue of concern in different UN human rights instruments, such as Articles 2 and 26 ICCPR, Article 2(2) ICESCR, Article 2 CRC, Article 7 CMW and Article 5 CRPD

¹³⁸ See for a similar analysis in the context of the media: Council of Europe Conference of Ministers Responsible for Media and Information Society – Freedom of Expression and Democracy in the Digital Age, Belgrade 7-8 November 2013, Resolution No 2: Preserving the essential role of media in the digital age, <http://www.coe.int/t/dghl/standardsetting/media/Belgrade2013/Belgrade%20Ministerial%20Conference%20Texts%20Adopted_en.pdf> accessed 13 May 2014

of a purely market-based approach to new TLD allocation and the promotion of pluralism and cultural and linguistic diversity.¹³⁹

82. The Internet has a high public service value in that it serves to promote the exercise and enjoyment of human rights and fundamental freedoms for all who use it and their protection should be a priority with regard to the governance of the Internet and therefore to the governance of the DNS.¹⁴⁰ In our opinion, states should ensure that ICANN affords effective and equitable access to TLDs, with a view to preventing digital exclusion and the promotion of pluralism and diversity to ensure the adequate functioning of the Internet ecosystem.

¹³⁹ See: Council of Europe, 'Declaration on the allocation and management of the digital dividend and the public interest' (20 February 2008)

¹⁴⁰ Council of Europe, Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet (7 November 2007)

CHAPTER 3

WHOIS & RAA vs. data protection & privacy

3.1 Introduction

83. Companies wanting to be allowed to ‘sell’ domain names are currently obliged to sign up to the 2013 Registrar Accreditation Agreement (RAA)¹⁴¹ which governs the relationship between ICANN and domain name registrars (companies that sell domain names). The RAA requires registrars to make available a variety of information about domain names (referred to formally as Registered Names) and their owners (Registered Name Holders) and purports that such data will be retained by private companies for up to two years after the contract for the domain has been ended. This chapter aims at highlighting the human rights issues related the 2013 RAA, since its provisions relating to personal data retention and disclosure, as well as the ability to subcontract given to registrars may put the fundamental rights of privacy and personal data protection in danger.

84. As states participate and develop ICANN’s procedures and policies in the multi-stakeholder process, they retain their obligation to ensure that human rights are protected within their jurisdictions. As elaborated in Chapter 1, the essence of the positive obligations doctrine is that, in order for states to ensure that everyone can exercise all of the rights enshrined in the ECHR in a practical and effective manner, the typical stance of non-interference (or negative obligation) by state authorities will often not suffice. As the Court affirmed in *Özgür Gündem v. Turkey*: ‘Genuine, effective exercise of certain freedoms does not depend merely on the State’s duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals’.¹⁴² It is important that governments recognise their extraterritorial obligations to respect, protect and promote the human rights of people outside their national borders, as this is a critical accountability mechanism in the digital age. States bear responsibility to take reasonable steps to ensure that the RAA complies with human rights, and that the right to privacy and personal data protection are effectively protected.

3.2 ICANN Policy on Personal Data Retention & Public Access

3.2.1 Data Retention Specification

85. The final ‘Data Retention Specification’ distinguishes between name and contact details for the domain name owners as well as all other types of data a registrar might collect, such as log files and billing records containing the “means and source of payment”, log files about the communication with the registrar including source IP address, telephone number, e-mail address, Skype handle or instant messaging identifier, as well as the date, time and time zones

¹⁴¹ICANN, 2013 Registrar Accreditation Agreement, <http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm#raa> (visited 14/04/2014).

¹⁴² *Özgür Gündem v. Turkey*, Judgment of the European Court of Human Rights (Fourth Section) of 16 March 2000, § 43.

of communications.¹⁴³ Registrars are required to keep the first category of personal data for a period of two years after the contract for the domain has expired. The second category of personal data must be retained for 180 days following any “relevant interaction” with a Registered Name Holder.

86. Following specific requests from certain European registrars, pursuant to Section 3 of the 2013 RAA, ICANN has granted waivers for several registrars from certain data retention provisions in the 2013 RAA in September 2014. ‘Registrar's Waiver Request’ is granted on the basis that registrar’s compliance with the data collection and retention requirements of the Data Retention Specification in the 2013 RAA violates applicable law in the particular country in question. As of September 23rd, there have been 6 requests granted to Registrars.¹⁴⁴

3.2.2. Public Access to Data on Registered Names

87. In addition, section 3.3 of the RAA requires registrars to “provide an interactive web page and a port 43 WHOIS service providing free public query-based access to up-to-date data concerning all active Registered Names sponsored by Registrar in any gTLD.” The data accessible includes many different types of personal information, such as the name as well as primary and secondary name server(s) and the contact details of the Registered Name, the identity of Registrar, the creation and expiry dates of the registration, and the name and postal address of the Registered Name Holder (3.3.1). Moreover, it provides that the “Registrar may subcontract its obligation to provide the public access provided that Registrar shall remain fully responsible for the proper provision of the access and updating.”¹⁴⁵

88. Both obligations in data retention specification and the policy of public access to data on registered names under RAA raise questions relating to the respect for private life and personal data under international human rights standards which will be discussed in the following section.

3.3. Human Rights Framework Applicable to RAA

89. The right to privacy is laid down in many national constitutions and proclaimed in international law instruments, including the UDHR and ICCPR. Article 8 of the ECHR provides:¹⁴⁶

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right 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

¹⁴³ Data Retention Specification of the ICANN, 2013 Registrar Accreditation Agreement, <http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm#data-retention> (visited 14/04/2014); 1st type of data specified in 1.1.1 to 1.1.7; 2nd type – 1.2.1 to 1.2.3.

¹⁴⁴ For related announcements, posted individually per registrar, see ICANN’s website:

<https://www.icann.org/news/announcement-6-2014-09-10-en> and the following posts (visited 23/09/2014).

¹⁴⁵ Section 3.3.3 of ICANN, 2013 Registrar Accreditation Agreement.

¹⁴⁶ Similar to Article 7 of the European Charter of Fundamental Rights.

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.”

90. The jurisprudence of international human rights tribunals, including the ECtHR and the ECJ, provides that the infringements of fundamental rights might only be permissible if they possess certain characteristics, as already discussed in Chapter 2. Briefly, all the permissible restrictions under Article 8(2) have to (1) be prescribed by law, (2) be pursued for one of the legitimate aims listed in an exhaustive way in the ECHR and (3) be necessary in a democratic society (proportional to the aims pursued).¹⁴⁷ Furthermore, Council of Europe states carry a positive obligation to seek to ensure that the ICANN’s 2013 RAA rules satisfy all of these conditions and respect the right to private life in the digital age.

91. The explicit statements regarding the importance of privacy on international level were been recalled in May 2011, when Frank La Rue, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression “urged states to adopt effective privacy and data protection laws in accordance with human rights standards, and to adopt all appropriate measures to ensure that individuals can express themselves anonymously online.”¹⁴⁸

92. In July 2012, the UN Human Rights Council (HRC) adopted by consensus a Resolution on the promotion, protection and enjoyment of human rights on the Internet,¹⁴⁹ which affirmed that “the same rights that people have offline must also be protected online.” While this principle is now widely supported by governments around the world, many nations have a long way to go to actually implement it.

93. In April 2013, Frank La Rue delivered a landmark Report on state surveillance and freedom of expression.¹⁵⁰ This report broke the long-standing silence of the UN on the implications of state surveillance on individual privacy rights. Importantly, the Rapporteur did not hesitate to highlight how the extra-legal government surveillance techniques intrude and threaten both the right to privacy and freedom of expression; he also stated that each are regarded as an essential prerequisite for the enjoyment and exercise of the other.¹⁵¹ La Rue also called on states to “refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services”.¹⁵² The GAC and governments, especially those that lobbied for prolonged periods of data retention, should take this into account.

¹⁴⁷ As regards the ECFR, see *Digital Rights Ireland*, § 38.

¹⁴⁸ See the Report by UN *Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Frank La Rue (17th session of the Human Rights Council (2011), Document A/HRC/17/27, p.22. /http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf/ (visited 16/04/2014).

¹⁴⁹ UN, Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet* (5 July 2012) UN Doc. A/HRC/20/L.13, /<http://www.regeringen.se/content/1/c6/19/64/51/6999c512.pdf>/(visited 12/02/2014). Presented by Sweden, HRC Resolution received broad international backing from more than 70 HRC member countries, including China, Brazil, Nigeria, Ukraine, Tunisia, Turkey, the US and the UK.

¹⁵⁰ See the Report by UN *Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Frank La Rue (23rd session of the Human Rights Council (2013), Document A/HRC/23/40, /http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf/(visited 07/02/2014).

¹⁵¹ UN Report, 2013, p. 21.

¹⁵² UN Report, 2013, p. 22, § 96.

94. Disclosures by Edward Snowden and others during 2013 about sweeping mass-surveillance programmes in the USA, UK, France and other countries shocked the international community to an extent never seen before. These revelations, initially concerning the US National Security Agency's (NSA) access to electronic communications data held by private companies (most notably the so-called PRISM programme), clearly demonstrates the prevalence of government demands on private-sector data.¹⁵³

95. And indeed, in response to Edward Snowden's revelations about some states' extraterritorial electronic surveillance activities,¹⁵⁴ the UN rapidly raised its voice on the protection of privacy in the digital sphere. On 18 December 2013, the UN General Assembly unanimously adopted a resolution, sponsored by Germany and Brazil, calling on all countries to guarantee privacy rights of Internet users by ensuring the full and effective implementation of all relevant obligations under international human rights law.¹⁵⁵ Through the adoption of the resolution on *The Right to Privacy in the Digital Age*, the General Assembly requested the UN High Commissioner for Human Rights to present recommendations to the Human Rights Council and the General Assembly on the 'protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data, including on a mass scale.'¹⁵⁶

96. In its Report, released in June 2014, the UN High Commissioner for Human Rights echoed the deep concerns expressed earlier over mass surveillance and interception and very convincingly questioned and analysed the legitimacy of mass data retention, the role and responsibility of private sector actors, and the potential impact on privacy and human rights that interception might have.¹⁵⁷

97. The Report was subsequently endorsed by the states as well as other stakeholders in the UN Human Rights Council's panel discussion on the right to privacy in the digital age, featuring several experts, on the 12th September, 2014. The Commissioner will prepare a summary report of the panel discussions, which will be submitted to the Human Rights Council at its 28th session. The panelists and NGOs also called for the establishment of a new special rapporteur on the right to privacy.¹⁵⁸

98. The right to privacy in the digital age and the High Commissioner's Report will next be considered by the UN General Assembly at its forthcoming session in October 2014. All these recent events, including the General Assembly's resolution, the High Commissioner's Report, as well as Human Rights Council's panel discussion, present part of a larger effort of the UN

¹⁵³ See Kuner, C., *et al.*, Editorial: 'Systematic Government Access to Private-Sector Data Redux,' *International Data Privacy Law*, 2014, Vol. 4(1), p. 1.

¹⁵⁴ See BBC News, 'The UN General Assembly adopts anti-spy resolution,' 18 December 2013, available at <http://www.bbc.co.uk/news/world-latin-america-25441408/> (visited 06/02/2014).

¹⁵⁵ See UN, Third Committee Approves Text Titled 'The Right to Privacy in the Digital Age', as It Takes Action on 18 Draft Resolutions (26 November 2013) GA/SHC/4094, available at <https://www.un.org/News/Press/docs/2013/gashc4094.doc.htm/> (visited 06/02/2014). Text: http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1/ (visited 12/02/2014).

¹⁵⁶ See Paragraph 5 of the Resolution. The General Assembly will take up these issues in its 69th session, scheduled for September 2014, when a special session to examine the report and recommendations will be held.

¹⁵⁷ See the report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/27/37, available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf/ (visited 15/09/2014).

¹⁵⁸ See the Video of the HRC panel, available at UN Web TV, <http://webtv.un.org/meetings-events/watch/panel-discussion-on-the-right-to-privacy-10th-meeting-27th-regular-session-of-human-rights-council/3781559740001/> (visited 23/09/2014).

bodies, to address the increasingly urgent issues of privacy and surveillance. They also signal that privacy in the digital age is considered an important issue for the United Nations' agenda.

3.4. Human Rights Analysis of WHOIS and RAA

99. The ECtHR has a considerable body of jurisprudence establishing that a mere collection and storage of personal data constitutes interference – permissible or not – with the right to privacy enshrined in Article 8 of the European Convention on Human Rights (ECHR). The subsequent use of the stored information has no bearing on that finding.¹⁵⁹ Thus, the RAA also constitutes an interference with privacy rights. Equally, the Court has found that it does not matter whether the information gathered on an individual was sensitive or whether the applicant had been inconvenienced in any way.¹⁶⁰ This is also echoed in the jurisprudence of the ECJ.¹⁶¹

100. In a very recent and important decision in *Digital Rights Ireland and Marine and Natural Resources* case (hereinafter ‘Digital Rights Ireland case’),¹⁶² the ECJ made it clear that the retention of personal data for the purpose of possible access to them by the competent national authorities directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 and 8 of the European Union’s Charter of Fundamental Rights. The access of the competent national authorities to the data constitutes a further interference with that fundamental right.¹⁶³

101. Accordingly, the provisions specifying data retention as well as the disclosure obligation under 3.3. RAA constitute an interference with the individual rights guaranteed by Article 8 of the ECHR and Articles 7 and 8 of the European Union’s Charter of Fundamental Rights. In order to be permissible under the ECHR, they have to (1) be in accordance with the law, (2) pursue one of the legitimate aims listed in an exhaustive way in the ECHR, and (3) be necessary in a democratic society (proportional to the aims pursued).¹⁶⁴

3.4.1. Prescribed by Law/In Accordance with Law

102. The ECtHR has held that the mechanisms interfering with the private lives of individuals must be in accordance with the law and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the

¹⁵⁹ See judgments in *Leander v. Sweden*, 26.03.1987; *Kopp v. Switzerland*, 25.03.1998; *Amann v. Switzerland*, 16.02.2000).

¹⁶⁰ *Amann v Switzerland* (2000) Application 27798/95; § 70.

¹⁶¹ See, to that effect, Cases C-293/12 *Digital Rights Ireland and Seitlinger and Others* and C-594/12 *Marine and Natural Resources and Others* and *Kärntner Landesregierung* § 33; Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* EU: C:2003:294, § 75.

¹⁶² *Digital Rights Ireland*, § 29, also quoting Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* EU:C:2010:662, § 47.

¹⁶³ See, *Digital Rights Ireland*, § 35 as regards Articles 7 and 8 ECHR; and as regards Article 8 of the ECHR, ECtHR, *Rotaru v. Romania* [GC], no. 28341/95, § 46, ECHR 2000-V; and *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 79, ECHR 2006-XI).

¹⁶⁴ As regards the ECHR, see *Digital Rights Ireland*, § 38.

persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.¹⁶⁵

103. Whereas data processing on the basis of a contract is fully acceptable, provided that other data protection principles are respected, the RAA rules go beyond that and require keeping the data *after* the termination of the contract. Any additional processing and storage thus would have to be based on legal rules.¹⁶⁶ In this regard, states must be aware that the *Data Retention Directive*¹⁶⁷ which imposed data retention obligations on providers of public electronic communication networks and services did not cover ICANN registrars. In any event, on 8 April 2014, the Directive was declared invalid under European law because of its disproportionate interference with the individuals' right to private life and protection of personal data.¹⁶⁸

104. The Article 29 Working Party, which is made up of a representative from the data protection authority of each EU member state, has already expressed its doubts as to whether a private organization like ICANN should introduce data retention by means of a contract in order to facilitate (public) law enforcement: "If there is a pressing social need for specific collections of personal data to be available for law enforcement, and the proposed data retention is proportionate to the legitimate aim pursued, it is up to national governments to introduce legislation that meets the demands of article 8 of the European Convention on Human Rights (and article 17 of the International Covenant on Civil and Political rights)."¹⁶⁹

105. An open access by third parties to the WHOIS database may be even more problematic, as it does not contain effective safeguards regarding the way that personal data will be collected and processed by third parties, whether public sector actors or businesses (for instance for marketing purposes). In fact, with these provisions, any third party will be able to collect personal data about the domains' 'owners' and contacts without restraint, creating problems regarding the core principles of data protection and giving anyone the opportunity to collect and process personal data without the person's consent.

3.4.2. Legitimate Aim

106. Even if Council of Europe member states enact legislation permitting/instructing a private body like ICANN to collect personal data, such a collection would have to pursue a legitimate aim. The Courts have generally recognized that in certain specific clearly laid out conditions, interference might be justified if it pursues a legitimate aim.¹⁷⁰ *Digital Rights Ireland the ECJ* held that the retention of data by private bodies (i.e. ICANN) for their possible transmission to the competent national authorities genuinely satisfies an objective of general

¹⁶⁵ As regards Article 8 of the ECHR, *M.M. v United Kingdom* [2012] ECHR 1906; *Liberty and Others v. the United Kingdom*, 1 July 2008, no. 58243/00, § 62 and 63; *Rotaru v. Romania*, § 57 to 59, and *S. and Marper v. the United Kingdom*, § 99).

¹⁶⁶ *Malone v. The United Kingdom*, judgment of 02.08.1984; *Silver v. The United Kingdom*, judgment of 23.03.1983.

¹⁶⁷ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

¹⁶⁸ Given that the Court has not limited the temporal effect of its judgment, the declaration of invalidity takes effect from the date on which the Directive entered into force.

¹⁶⁹ Article 29 Data Protection Working Party, letter to ICANN, 06 June 2013, Statement on the Data Protection Impact of the Revision of the ICANN RAA, Ref. Ares(2013)1791630 – 06/06/2013; <http://www.icann.org/en/news/correspondence/kohnstamm-to-crocker-chehade-06jun13-en.pdf> (visited 26/09/2014), at p. 2.

¹⁷⁰ *Digital Rights Ireland*, § 41 – 44.

interest, namely the fight against serious crime and, ultimately, public security.¹⁷¹ This echoes a rich and well developed jurisprudence of the ECtHR; however, in order to comply with human rights exigencies, such interference must still be necessary in a democratic society and be proportionate to the aim pursued.

3.4.3. Necessary & Proportionate in a Democratic Society

107. Even if the data retention and disclosure would be seen as pursuing a legitimate interest in preventing crime, the RAA must still be tested for ‘necessity.’ The ECtHR has generally held that the notion of necessity implies two things:

(1) that an interference corresponds to a pressing social need,¹⁷²

(2) that it is proportionate to the legitimate aim pursued¹⁷³

108. Such prolonged data retention and public disclosure policy thus could only be justified if is not disproportionate to the aim pursued. The ECJ has stated that an interference with fundamental rights must be “appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives.”¹⁷⁴ Highlighting the role of personal data protection as a fundamental right, the ECJ has generally accepted that “derogations and limitations in relation to personal data must apply only in so far as strictly necessary.”¹⁷⁵

109. As the Article 29 Data Protection Working Party noted: “Taking into account the diversity of these registrars in terms of size and technical and organizational security measures, and the chance of data breaches causing adverse effects to individuals holding a domain name, the benefits of this proposal seems disproportionate to the risk for individuals and their rights to the protection of their personal data”.¹⁷⁶

110. In this regard, the RAA rules seem to be disproportionate principles passed into a binding private contractual agreement. To serve the global public interest it is therefore important to review these rules to find a balance that better serves a more holistic public interest.

3.4.4. Purpose Limitation

111. Indeed, the data retention requirement in the 2013 RAA does not seem to be compatible with the purpose limitation principle – which could be understood as an expression of a broader proportionality principle – as spelled out in all the main international data privacy

¹⁷¹ *Digital Rights Ireland*, § 43-44; Case C-145/09 *Tsakouridis* EU:C:2010:708, § 46 and 47.

¹⁷² *The Sunday Times v United Kingdom* (1979) 2 EHRR 245).

¹⁷³ *MS v Sweden* (1997) 3 BHRC 248.

¹⁷⁴ *Digital Rights Ireland*, § 46 and Case C-343/09 *Afton Chemical* EU:C:2010:419, § 45; *Volker und Markus Schecke and Eifert* EU:C:2010:662, § 74; Cases C-581/10 and C-629/10 *Nelson and Others* EU:C:2012:657, § 71; Case C-283/11 *Sky Österreich* EU:C:2013:28, § 50; and Case C-101/12 *Schaible* EU:C:2013:661, § 29).

¹⁷⁵ Case C-473/12 *IPI* EU:C:2013:715, § 39 and the case law cited.

¹⁷⁶ Article 29 Data Protection Working Party, letter to ICANN, 06 June 2013, Statement on the Data Protection Impact of the Revision of the ICANN RAA, Ref. Ares(2013)1791630 – 06/06/2013; <http://www.icann.org/en/news/correspondence/kohnstamm-to-crocker-chehade-06jun13-en.pdf> (visited 26/09/2014), at p. 2.

instruments, both of a legally binding nature such as the Council of Europe Convention 108¹⁷⁷ and the EU Data protection Directive¹⁷⁸ or of a non-binding nature such as the UN Guidelines,¹⁷⁹ the OECD Guidelines,¹⁸⁰ APEC Privacy Framework,¹⁸¹ and the Madrid Resolution.¹⁸²

112. Article 5(e) of the Council of Europe Convention 108 and Article 6(e) of the EU Data Protection Directive state that the data must be preserved:

*“in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which data were collected/stored”.*¹⁸³

113. The 2013 RAA fails to specify the legitimate purpose for which it was collected. In this regard, the RAA is similar to other data retention and sharing mechanisms, such as the PNR¹⁸⁴ and SWIFT agreements¹⁸⁵ all of which aimed to make authorities' personal data obtained and stored by private companies available to law enforcement. Contrary to these mechanisms, the RAA data retention requirement does not have any legal basis under international law or

¹⁷⁷ CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 1981.

¹⁷⁸ European Union Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data 95/46/EC; OJ L 281, 23.11.1995, 31.

¹⁷⁹ UN Guidelines for the regulation of computerized personal data files, A/RES/45/95, 14 December 1990. Article 3(b) reads: 'None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified.'

¹⁸⁰ The newly revised OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data, 2013, available at <http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines/> (visited 12/06/2014). Article 9 of the OECD purports: 'The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.'

¹⁸¹ Asia-Pacific Economic Cooperation Privacy Framework of 2004. Principle III purports: 'The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.'

¹⁸² International Standard on the Protection of Personal Data and Privacy, adopted at the 31st International Conference of Data Protection and Privacy Commissioners, 6th November, Madrid, 2009, available at http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf. Article 7(2) reads: 'The responsible person should not carry out any processing that is non-compatible with the purposes for which personal data were collected, unless he has the unambiguous consent of the data subject.'

¹⁸³ Article 5(e) of the Council of Europe Convention 108 and Article 6(e) of the EU Data Protection Directive.

¹⁸⁴ The PNR agreements require air carriers to permit the state authorities to access the PNR data stored in their databases for further processing. The PNR storyline has three US-EU Agreements concluded in 2004, 2007 and 2012. The 2004 *Agreement between the European Community and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security* (O.J. 2004, L 183/84) and 2007 *PNR Agreement* (O.J. 2007, L 204/18) and the 2012 *PNR Agreement* (O.J. 2012, L 0215). See the ECJ, Judgment of May 30, 2006 (PNR) – Cases 317/04 and 318/04 – E.C.R. 2006, P. I-4721.

¹⁸⁵ The SWIFT saga has two agreements concluded in 2009 and 2010; see *Agreement between the European Union and The United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program* (O.J. 2010, L 8/11) and 2010 *SWIFT Agreement* (O.J. 2010, L 195/5).

European law.¹⁸⁶ Whereas all these mechanisms did have an initial legal bases specified, they were nonetheless declared invalid by the ECJ.

114. As noted by the Article 29 Data Protection Working Party in its June 2013 letter to ICANN, “the fact that these data may be useful for law enforcement (including copyright enforcement by private parties) does not equal a necessity to retain these data after termination of the contract.”¹⁸⁷ This echoes a broader point made by the European Data Protection Supervisor that “the general trend to give law enforcement authorities access to the data of individuals, who in principle are not suspected of committing any crime, is a dangerous one.”¹⁸⁸ Indeed, recently, the European Data Protection Supervisor also sent a letter to ICANN, stating that: “It would not be acceptable for the data to be retained for longer periods or for other, incompatible purposes, such as law enforcement purposes or to enforce copyright.”¹⁸⁹

115. The Article 29 Working Party has made a request to ICANN in its letter of 8th January 2014, to accept the Working Party’s position - that the 2013 RAA fails to specify a legitimate purpose which is compatible with the purpose for which the data was collected – ‘as appropriate written guidance which can accompany a Registrar’s Data Retention Waiver Request.’¹⁹⁰ As mentioned earlier, several such waiver requests now have been granted on the 11th September 2014 – however, this fact doubtfully would satisfy the requirements of the purpose limitation principle.

116. Within the UN, the UN High Commissioner for Human Rights in its above mentioned Report *The Right to Privacy in the Digital Age*, confirmed the approach articulated earlier by the data protection authorities by highlighting: “Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of Governments on private sector actors to retain data “just in case” it is needed for government purposes. Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers’ communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.”¹⁹¹

¹⁸⁶ The *Data Retention Directive* imposed data retention obligations on providers of public electronic communication networks and services, and registrars are not covered under this legislation. In any event, the Directive is declared invalid under the EU law.

¹⁸⁷ Article 29 Data Protection Working Party, letter to ICANN, 06 June 2013, Statement on the Data Protection Impact of the Revision of the ICANN RAA, Ref. Ares(2013)1791630 – 06/06/2013; <http://www.icann.org/en/news/correspondence/kohnstamm-to-crocker-chehade-06jun13-en.pdf> (visited 26/09/2014).

¹⁸⁸ European Data Protection Supervisor, Press Release ‘Smart Borders: Key Proposal is Costly, Unproven and Intrusive’, 19 July 2013, http://europa.eu/rapid/press-release_EDPS-13-08_en.htm (visited 14/04/2014).

¹⁸⁹ European Data Protection Supervisor, letter to ICANN, 17 April 2014, Statement on ICANN's public consultation on 2013 RAA Data Retention Specification Data Elements and Legitimate Purposes for Collection and Retention, Brussels, PH/ZB/mk D(2014)0958 C2014-0449, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2014/14-04-17_EDPS_letter_to_ICANN_EN.pdf (visited 12/06/2014).

¹⁹⁰ Article 29 Working Party, letter to ICANN of 8th January 2014, Ref. Ares(2014)22160 - 08/01/2014, available at [/http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140108_letter_icann.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140108_letter_icann.pdf) (visited 26/09/2014).

¹⁹¹ See the report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/27/37, para. 26, available at

117. Therefore, States should reconsider whether they fulfill their human rights obligation by permitting ICANN to retain personal data for such prolonged periods in order to make it available for law enforcement purposes, and whether such practices are strictly necessary in a democratic society.

3.5. Conclusion

118. The new data retention provisions in the 2013 RAA were included following strong demands made by numerous law enforcement agencies and the governments of a crossnational intelligence alliance, among others.¹⁹² The provisions were adopted despite data protection concerns raised by the Article 29 Working Party and by the Chair of the Council of Europe Consultative Committee of the Data Protection Convention, as well as many civil society organizations.¹⁹³ The EU Commission also expressed “concerns as regards (...) data protection and in particular as regards the purpose of the processing and the retention of the data.”¹⁹⁴ Taking these disquiets into account, states should seek to ensure that a human rights perspective is included in the ICANN procedures.

119. As regards the ‘Registrar’s Waiver Request’ procedure, under which a registrar might be granted a waiver in order to *be able* to comply with national law, it should be noted that this mechanism still falls short of an adequate process to satisfy the minimum data privacy requirements. One might even question the very rationale and legitimacy of such a procedure from a legal perspective, where registrars are required to ask for a permission from ICANN – via the Waiver procedure - to *be able* to comply with national law in a jurisdiction in which it is operating.

120. The States should also be aware that ICANN is not obliged to exercise a public function and store personal data *after* the termination of the contract for the law enforcement purposes. ICANN may update RAA rules at any time so that personal data is retained for no longer than is necessary for the performance of the contract; and should governments wish to collect personal data for law enforcement purposes, they are free to establish such frameworks with a legal basis under international law (or EU law).¹⁹⁵ As regards public access to personal information, the WHOIS database system should not have unlimited public access to personal data, such as names, addresses, and e-mails. Over a decade ago back in 2003, the Article 29 Party expressed the view that ‘It should in any case be possible for individuals to register domain names without their personal details appearing on a publicly available

http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf/ (visited 15/09/2014).

¹⁹² ‘Five Eyes’ intelligence alliance countries are Australia, Canada, New Zealand, the United Kingdom and the United States.

¹⁹³ E.g. Derechos Digitales and the Statewatch expressed their opinion on the issue; see Derechos Digitales, letter to ICANN of July 19, 2012, <http://www.derechosdigitales.org/wp-content/uploads/letter-of-concern-ICANN-Derechos-Digitales.pdf/> and Statewatch, ‘Want to set up a website? The ‘Five Eyes’ want your personal data,’ <http://www.statewatch.org/analyses/no-234-websites-five-eyes.pdf>.

¹⁹⁴ At a meeting of the ICANN GAC in July 2013 in Durban the Commission’s representative has also expressed “concerns as regards... data protection and in particular as regards the purpose of the processing and the retention of the data’, see ICANN, ‘Transcript: GAC Plenary – Staff Update on New gTLDs’, 13 July 2013, <http://durban47.icann.org/node/40877> (visited 14/04/2014).

¹⁹⁵ The *Data Retention Directive* imposed data retention obligations on providers of public electronic communication networks and services, and registrars are not covered under this legislation. In any event, the Directive is declared invalid under the EU law.

register.¹⁹⁶ Indeed, national and international data protection instruments establish high standards for accessing and processing personal information by third parties that are not compatible with public disclosure of personal data by Domain Name registrars. The governments should ensure that ICANN includes provisions governing the disclosure and third-party use of data, and ideally, personal information should be accessible only to public officers through a court order or according to national law.

121. More emphasis on data privacy is particularly desirable in order for ICANN to fulfill its global public interest role and guarantee human rights protection. Due diligence principle as defined by the UN Guiding Principles requires meaningful consultation with affected stakeholders and in the context of ICANN, this includes ensuring that domain name owners have meaningful information and transparency about how their personal data is collected and potentially shared with others, so that they are able to raise concerns and make informed decisions. As recently pointed by the UN High Commissioner for Human Rights, individuals should be provided with a remedy that includes 'information about which data have been shared with State authorities, and how.'¹⁹⁷

122. The UN Resolution on *Privacy in the Digital Age*, and other recent documents and events organized and published by the UN bodies on the surveillance and privacy suggest that the views of the international community on the role of privacy in the 21st Century are crystallizing and might include sufficient agreement on a rule of customary international law. The UN General Assembly Resolution on *Privacy in the Digital Age* not only carries much more moral and political significance and manifests the global criticism of mass-spying practices, it also demonstrates consensus on the importance of safeguarding the right to privacy. The importance of individual privacy rights has also been recently emphasized in the judgment made on 8 April 2014 by the European Court of Justice in *Digital Rights Ireland* where it declared the EU Data Retention Directive¹⁹⁸ invalid because of its disproportionate interference with the European citizens' right to private life and protection of personal data.¹⁹⁹ These developments suggest that states should seek to ensure that the ICANN's RAA does not interfere with the fundamental rights to respect for private life and to the protection of personal data, in a manner which would be contrary to conditions allowing interference with such rights, such as set out in article 8, paragraph 2 of the ECHR.

¹⁹⁶ The Article 29 Party, *Opinion 2/2003 on the application of the data protection principles to the Whois directories*, adopted 13/06/2003, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp76_en.pdf/ (visited 26/09/2014).

¹⁹⁷ See the report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/27/37, para. 46, available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf/ (visited 15/09/2014).

¹⁹⁸ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

¹⁹⁹ Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland and Seitlinger and Others*. Given that the Court has not limited the temporal effect of its judgment, the declaration of invalidity takes effect from the date on which the Directive entered into force.

Conclusion and Recommendations

123. The Internet is a global resource which should be managed in the global public interest. This is not only ICANN's ethos, but also one of the main conclusions of the NETmundial Conference in April 2014. ICANN's mission to serve the public interest is a very welcome starting point for the development of its policies and principles. Nevertheless, the concept of 'public interest' is vague, providing neither guidance nor constraint on ICANN's actions. It is therefore important to flesh out the concept of serving the global public interest in order to strengthen accountability and transparency in ICANN's multi-stakeholder model.

124. ICANN has tried to strike a balance between competing rights and interests. It is remarkably difficult to determine what the interests of the 'global public' are. The development of policy based on such a vague notion generates the risk of it being misused by resourceful and powerful stakeholders. As ICANN is expanding its tasks and activities, partly resulting from the new gTLD programme, better guidance to balance interests is required.

125. First, ICANN's current standards on 'sensitive applied-for new gTLD's' do not fully comply with the right to freedom of expression – particularly for Europe, but most likely also for other regions. The disagreement and confrontation raised by terms such as '.sucks' – even when expressed in strong terms – ordinarily come within the scope of the protection offered by the right to freedom of expression. ICANN should therefore exercise its role with due regard for fundamental rights and freedoms and in full compliance with international standards. Restricting potentially offensive expressions, resulting from a juxtaposition the likes of '.sucks' or '.fail' in gTLDs would restrict the ability of all speakers, commercial and non-commercial, to express themselves. It is therefore desirable for ICANN to consider applying another legal model, outside of trademark law, to better address speech rights. Additionally, human rights norms provide a tool for the GAC when deliberating cases of GAC Early Warning and GAC Advice on sensitive strings.

126. Second, in the light of the positive obligations of states to reach out to specific types of groups who for various reasons are vulnerable or merit differentiated treatment, it is desirable that the people-centeredness of ICANN's policy development is improved. Technical and policy choices involved in the digital environment should not be predominantly determined by economic factors. ICANN could improve its policies and procedures by having a more sensitive approach towards social, cultural and political factors. A balance must be struck between economic interests and other objectives of common interest, such as pluralism, cultural and linguistic diversity.

127. Third, law enforcement considerations seem to be over-represented in the new data retention provisions in the 2013 RAA at the expense of privacy considerations. The legitimate purpose of the processing and the retention of the data are questionable, which indicates that there could be a disproportionate interference with the right to private life. Increased emphasis on data privacy is therefore highly desirable, inter alia, in the light of the UN Resolution on *Privacy in the Digital Age* that suggests that there might be a sufficient level of consensus for there to be a rule of customary international law on the right to privacy in a digital age.

128. Last, as has been put forward by many experts in the field, public access to personal information in the WHOIS database is not fully consistent with human rights law. National and international data protection instrument establish high standards for accessing and processing personal information by third parties. GAC members have the responsibility to protect the human rights of their citizens and should therefore make sure that ICANN includes provisions governing the disclosure and third party use of data.

Roles & Responsibilities – ICANN & GAC

ICANN

129. ICANN's policies and procedures can have an impact on a broad range of internationally recognized human rights. Therefore it has the responsibility to respect human rights. ICANN is not state bound by international human rights laws and, therefore, does not have positive obligations to protect human rights comparable to that of the states. Nonetheless, it has a responsibility to respect human rights as set out in the UN Guiding Principles on Business and Human Rights,²⁰⁰ which present the global standard for corporate responsibilities which applies to all business enterprises, both transnational and others, regardless of their size, sector, location, ownership and structure. Under the UN Guiding Principles, companies operating in the ICT sector, are expected to adopt an explicit policy statement outlining their commitment to respect human rights throughout the company's activities and have appropriate due diligence mechanisms to identify, assess, prevent any adverse impact on human rights. Therefore, due diligence principle requires ICANN to assess whether and how its procedures and mechanisms, such as the new gTLDs, 2013 RAA, and WHOIS database may result in an adverse impact on the human rights.

130. The protection of human rights is also closely linked to advancing long-term, sustainable development. Rights are both part of the goal of development and instrumental to attaining other goals such as economic growth or democracy. Additionally, the need for ICANN to include a human right perspective is highly desirable with regard to its own legitimacy, accountability and transparency. The inclusion of a human rights perspective enhances ICANN's ability to guarantee the sustainability of the internet as a single unfragmented source.

131. A core aspect of human rights due diligence principle as defined by the UN Guiding Principles is meaningful consultation with affected stakeholders, transparency and accountability. Accountability means ensuring that ICANN is answerable for its actions. ICANN has the duty to explain, clarify and justify its actions. Transparency is also a necessary precondition for the exercise of accountability since without access to clear, accurate and up-to-date information, it is impossible to judge whether the desirable standard has been met. Human rights provide indicators or criteria to measure to what extent the standard of 'serving the public interest' has been met. Human rights provide a framework which allows stakeholders to measure whether ICANN's decisions are taken in the global public interest. Human rights are objective and internationally agreed upon with solid reasoning to clarify and justify behaviour. They provide a workable framework for checks and balances for the accountability system of ICANN.

132. With great power comes great responsibility. ICANN's success brings with it responsibilities for being the voice and direction of the global multi-stakeholder Internet community. It is responsible for providing value in return for the loyalty of the Internet community. It therefore needs to work hard to create the right policy approaches to ensure that ICANN and the Internet as a single unfragmented source can continue to fulfil its full potential. As the role of ICANN in the field of internet governance increases, its responsibility and accountability will grow. A more attentive approach towards human rights could help to create an accountable and transparent way of doing business.

²⁰⁰ United Nations Human Rights Council, Guiding Principles on Business and Human Rights, HR/PUB/11/04, available at [/http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf/](http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf) (visited 23/09/2014).

GAC

133. Governments have primary, legal and political accountability to protect human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties. In the member states of the Council of Europe any interference with these rights and freedoms should meet the conditions laid down in the European Convention on Human Rights as interpreted by the European Court of Human rights. These obligations continue to exist when states participate in activities of entities specializing in technical mandates. If states fail to protect or promote the respect of these rights, they could be held accountable for violations of domestic human rights provisions or international human rights standards. They could also be held accountable, as a last resort, before supranational courts, such as the European Court of Human Rights.

134. The inclusion of a human rights perspective in ICANN's mission to serve the global public interest is highly desirable from the GAC's perspective. The GAC is not a decision-making body. The GAC's key role is to provide advice to ICANN on issues of public policy, and especially where there may be an interaction between ICANN's activities or policies and national laws or international agreements, such as human rights treaties. Although it is the GAC's responsibility to protect its citizens, it is questionable whether it can be relied on to be the sole voice of human rights. The inclusion of a human rights perspective in ICANN's policy making therefore makes it easier for GAC members to live up to the expectation of their citizens to protect their human rights.

135. In the light of the responsibility of GAC members to protect the human rights of their citizens, it is remarkable that its role is solely advisory in the late stage of the decision making process. ICANN's policy development processes would benefit from a human rights perspective at an earlier stage of policy development. This should be taken into account in the currently ongoing reflections on how to improve an earlier engagement of the GAC in ICANN's policy development processes. States in the GAC need to be more aware of their duties under international human rights law to protect their citizens, and to make sure they provide the whole ICANN community with their expertise.

Recommendations

136. There are multiple public interest challenges to be faced now and in the future. We offer some recommendations with a view to supporting the multi-stakeholder model which more efficiently serves the public interest.

Reference to human rights in ICANN's Bylaws

137. ICANN should be under an obligation to ensure respect for human rights. Therefore, human rights should be referred to in ICANN's Bylaws. Reference to human rights would fit in under 'Core Values', as set out in Article 1. Although ICANN has not dealt with content regulation to a large extent so far, its policy-making powers could in principle allow it to engage in these kinds of activities to a greater degree. The inclusion of human rights in the internal rules for ICANN by the Board is a step in the right direction in the light of internal accountability. Human rights will provide a means to measure whether ICANN is serving the public interest.

138. Specific reference in ICANN's Bylaws to human rights that are particularly relevant in the field of internet governance is desirable. This will provide guidance and make it clear to the internet community as to what it means for ICANN to serve the public interest. A provision could be introduced prohibiting policies and procedures that would violate the rights to freedom of expression or freedom of association. Additionally, specific reference to the need to respect the right to freedom of expression and the right to freedom of association in case of resolution of trademark and other IP disputes is of added value. In this respect, ICANN policies could have a salutary rebalancing effect.

139. Second, ensuring the right balance between security and fundamental rights would be best served by the introduction of a provision that declares personal data can only be gathered legally under strict conditions and for a legitimate purpose; this could be a valuable addition in the light of accountability and transparency. Furthermore, ICANN's Bylaws could emphasize the right of individuals to complain and obtain redress if data is misused.

Define public interest objectives

140. To establish clear and unambiguous terms of service in line with international human rights norms and principles, public interest objectives need to be identified. One could think of 'the respect for human rights, fundamental freedoms and democratic values'. Further elaboration on the scope of such rights is desirable to provide clarity and certainty with respect to accountability and transparency. One could additionally think of 'the respect for linguistic and cultural diversity and care for vulnerable persons and groups'.

Improve human rights expertise and early engagement in the GAC

141. States need to make sure that when participating in GAC, there are members that have human rights expertise based on formal academic qualifications and actual human rights experience. Seeing that governments have primary, legal and political accountability for the protection of human rights, states need to make sure that GAC members are sensitive to human rights. When ICANN's policy development includes interaction between ICANN's activities or policies and national laws or international agreements, the GAC should intervene at an early stage to provide the ICANN community with the necessary input from a legal perspective.

Early engagement mechanism for the safeguarding of human rights

142. The GAC cannot be relied on to be the sole voice for human rights. Earlier engagement between human rights, international law and technology is needed to provide the community with means to better understand the human rights impacts of the introduction of new policies within the ICANN environment. This should be taken into account in the currently ongoing reflections on how to improve an earlier engagement of the GAC in ICANN's policy development processes.

143. ICANN should consider establishing a Panel designed to provide advice on human rights and international law with regard to ICANN's actions and decisions. Such an advisory Panel could consist of a limited number of experts from relevant international organizations, such as the United Nations, the Organization of American States (OAS), the OECD and the Council of Europe. Such a Panel could deliver early engagement expertise in the field of human rights and international law. It is desirable that such a panel is limited in size, to be able to provide straight forward guidance at an early stage.

144. Setting up such an Advisory Panel would further ICANN's principles of accountability and transparency. The expert panel would provide clear and accurate information on international

law and human rights in the light of ICANN's operations. Subjecting ICANN's policy development to independent expert scrutiny prior to implementation will preemptively identify and address possible human rights concerns. This will allow the ICANN community to judge whether the necessary standards will be met in ICANN's policy making.

Review ICANN's legal basis

145. To efficiently guarantee serving the public interest, ICANN should be free from risk of dominance by states, other stakeholders, or even its own staff. Dominance is often coupled with increasing risks of human rights interference, such as mass surveillance or censorship. ICANN would benefit from an international or quasi-international status guaranteeing it minimum rights and necessary independence of action vis-à-vis the various national or international authorities with which they deal.

146. Particularly in view of the fact that the United States Commerce Department's National Telecommunications and Information Administration (NTIA) announced its intent to transition Internet domain name functions to a global multi-stakeholder community, it is highly relevant to review ICANN's legal status. The legal basis and related internet governance model is of significant value for the protection of human rights. Protection of human rights should therefore be an important consideration in the deliberations on ICANN's legal status. The legal status of the International Federation of the Red Cross and Red Crescent Societies could be one source of inspiration for new and innovative solutions in this regard.

147. It would be possible to imagine ICANN's corporate roots remaining in the US, while its operations are being hosted in other countries. A solid legal basis is needed to provide broad legitimacy and stability. A technical instrument, such as a convention, in which the sustainability of the internet as a single unfragmented resource is guaranteed, could be envisaged. It goes beyond the scope of this study to provide an in-depth analysis of the legal and political possibilities in this respect.