[WORKING DRAFT]

Human Rights Implications of the WHOIS Policy[1]

Introduction

The WHOIS database contains personal information collected from individuals while registering a domain name. It is used for a variety of purposes, but the primary aim is to provide contact details of the registered name holder (registrant) of the domain in case of issues relating to the domain, including technical and law enforcement concerns.[2] The recently expired Affirmation of Commitments (AoC) required ICANN to maintain "timely, unrestricted and public access" to WHOIS information.[3] The consequence of this unrestricted public access is that all the information, including personal information, is easily accessible.[4]

The adverse impact of WHOIS on multiple human rights requires a closer study of the WHOIS Policy. However, this paper is not the first to raise these concerns. A Council of Europe report[5] analyzing ICANN policies from a human rights perspective identifies similar human right concerns. The report states that open access to the WHOIS database is extremely problematic because of the lack of safeguards over how third parties access and use personal data.[6]

Part I of this paper explains the WHOIS policy by examining the provisions of the AoC, as well as existing contractual obligations. Part II of the paper explores the human rights implications of this policy. It identifies the violation of privacy as the primary human rights concern and explores how this affects other human rights - including the right to security of person and the rights to freedom of expression and freedom of assembly and association. Part

---

[1] *By **Aarti Bhavana*** and ***Kritika Bhardwaj**, Programme Officers, Centre for Communication Governance at National Law University, Delhi, with research inputs from **Lily Xiao**, CCG Summer Intern and student at University of Melbourne.*

[2] 'WHOIS Primer | ICANN WHOIS' (*whois.icann.org*, 2016) <https://whois.icann.org/en/primer> accessed 9 September 2016.

[3] 'ICANN Affirmation of Commitments' (*ICANN*, September 30 2009) <https://www.icann.org/resources/pages/affirmation-of-commitments-2009-09-30-en> accessed 9 September 2016.

[4] Electronic Privacy Information 'ICANN and the WHOIS Database: Providing Access to Protect Consumers' (Testimony before the Subcommittee on Financial Institutions and Consumer Credit, United States House of Representatives, 18 July 2006) <https://epic.org/privacy/whois/phishing_test.pdf> accessed 9 September 2016.

[5] Dr Monika Zalnieriute and Thomas Schneider, 'ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values' (8 October 2014) Report of Council of Europe Report <https://tinyurl.com/zawwhyt> accessed 9 September 2016.

[6] ibid at p 42.

III argues that WHOIS must incorporate data protection principles in order to effectively safeguard the privacy of registrants. It looks at eight core principles associated with the protection of personal information internationally and analyses how the WHOIS policy can be modified to incorporate them. To conclude, this paper recognizes a lack of academic material available regarding this subject and recommends further research and discussion. Importantly, this paper contends that consideration for human rights should be an integral part of the foundations of WHOIS, rather than an afterthought[7].

I. The WHOIS Policy

In order to register a domain, the registrant is required to provide accurate personal information, which is entered in the WHOIS database.[8] This personal information includes the name and postal address of the registrant.[9] It also includes the name, postal address, email address, voice telephone number and facsimile number of the technical and administrative contact of the domain.[10]

This part of the paper briefly summarises the current WHOIS policy by looking at the (now expired) Affirmation of Commitments, its lingering impact and the existing contractual obligations. It briefly discusses the policies on privacy and proxy services and the current work being undertaken by the Next-Generation gTLD RDS PDP regarding this.

A. Location of the WHOIS Policy

The WHOIS policy originates from the Affirmation of Commitments (AoC), as well as a series of commitments under ICANN's agreements with its registries and registrars.

1) Affirmation of Commitments

The AoC[11] was a document signed by the United States Department of Commerce and ICANN in 2009. It required ICANN to 'implement measures to maintain timely, unrestricted

[7] Dia Kayyali, 'EFF to ICANN: Privacy Must be Purposeful—Not an Afterthought' (*EFF*, September 2015) <https://www.eff.org/deeplinks/2015/09/eff-icann-privacy-must-be-purposeful-not-afterthought> accessed 9 September 2016.
[8] Registrar Accreditation Agreement 2013 (RAA 2013), Section 3.2.1 <http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm> accessed 9 September 2016.
[9] ibid at Section 3.3.1.6.
[10] ibid at Sections 3.3.1.7-3.3.1.8.
[11] ICANN AoC (n 3).

and public access to accurate and complete WHOIS information…' In order to meet that obligation, the registrars and registries provide public access to WHOIS data on registered domain names. Anyone can use WHOIS to search and identify the registrant of a generic domain name.[12]

The AoC expired on 1st October 2016, with the completion of the IANA Stewardship Transition.[13] However, reviews provided under the AoC (AoC Reviews) have been incorporated into the amended ICANN Bylaws (as Specific Reviews).[14] This includes the Registration Directory Service (RDS) Review, which is to be conducted every five years.[15] By not mentioning any specific RDS (such as WHOIS), the bylaws leave open the possibility of a new RDS which may replace WHOIS. This is one of the issues being considered by the Working Group for the Policy Development Process on Next-Generation gTLD RDS (discussed under II. C. of this paper).

2) Contractual obligations

Registry[16] and Registrar Agreements[17] establish contractual obligations related to WHOIS. The WHOIS obligations for the current Registries are set out in their contracts with ICANN. Generally, the 'WHOIS Specification' can be found in the appendices of the Registry Agreements, all of which are available publicly on the ICANN website. ICANN's registrars have signed onto one of the three contracts: the 2001 Registrar Accreditation Agreement[18] (RAA), the 2009 RAA[19] or the 2013 RAA[20]. Each of these contracts contains numerous provisions regarding WHOIS service and data, and sets out requirements for the access and accuracy of WHOIS data.

The WHOIS provisions of the 2001 RAA and 2009 RAA are very similar in their language, intent and goals. The 2013 RAA, which is followed for registrars wishing to renew their

[12] 'WHOIS Online Accuracy Reporting System: Request for Proposal' (*ICANN,* 19 May 2014) <https://www.icann.org/news/announcement-2014-05-19-en> accessed 9 September 2016.
[13] 'Specific Reviews' (*ICANN*, 2016) <https://www.icann.org/resources/reviews/aoc> accessed 7 October 2016.
[14] ICANN Bylaws <https://www.icann.org/en/system/files/files/adopted-bylaws-27may16-en.pdf> accessed 6 October 2016.
[15] ibid at Section 4.6 (e).
[16] 'Registry Agreements | ICANN WHOIS Policies' (*WHOIS.ICANN*, 2013) < https://whois.icann.org/en/registry-agreements> accessed 9 September 2016.
[17] ibid.
[18] Registrar Accreditation Agreement 2001 <https://www.icann.org/resources/unthemed-pages/raa-2001-05-17-en> accessed 9 September 2016.
[19] Registrar Accreditation Agreement 2009 <https://www.icann.org/resources/pages/ra-agreement-2009-05-21-en> accessed 9 September 2016.
[20] RAA 2013 (n 8).

RAA or sell domain names in new gTLDs, represents an expansion of obligations related to WHOIS. The aim of the expansion is to improve the accuracy and overall effectiveness of the WHOIS system. The 2013 RAA introduces obligations relating to the validation and verification of certain WHOIS data elements, as well as obligations applicable to privacy and proxy services offered by the registrars and their affiliates.[21]

B. Privacy and Proxy Services

The current policy also provides for privacy and proxy services for individuals and entities who want to keep certain information from being made public via WHOIS.

These commercial services are of two types:[22]

- A *Privacy Service* keeps the domain name registered in the name of the registrant and instead of providing registrant's contact information lists alternative, reliable contact information, such as a mail-forwarding service address.
- A *Proxy Service* registers the domain name itself and licenses the use of the domain name to its customer. It provides the contact information of the service provider rather than of the customer.[23]

Further, the 2013 RAA stipulates that all publicly available personal data is to be retained,[24] including any personal data held by a proxy service.[25] The data is retained for the term of the agreement and subsequently for two years after the agreement is terminated.[26] ICANN is required to make this data available for inspection and copying upon reasonable notice.[27]

C. Ongoing policy work

There is currently a Policy Development Process (PDP) on Next-Generation gTLD Registration Directory Service (RDS) to Replace WHOIS. It is considering reforms to the

[21] ibid at Section 3.
[22] 'Privacy and Proxy Services | ICANN WHOIS Policies' (*WHOIS.ICANN*, 2013) <http://whois.icann.org/en/privacy-and-proxy-services> accessed 9 September 2016;
'Specification on Privacy and Proxy Registrations' (*ICANN*, 17 September 2013) <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#privacy-proxy> accessed 9 September 2016.
[23] ibid.
[24] RAA 2013 (n 8) at Section 3.4.1.2.
[25] ibid at Section 3.4.1.5.
[26] ibid at Section 3.4.2
[27] ibid at Section 3.4.3

WHOIS policy and whether it needs to be replaced with another RDS.[28] The PDP working group will deal with questions of who has access to the data and why (users/purpose), how data access can be controlled for different users (gated access), how data accuracy can be improved (data accuracy) and what steps can be taken to protect data and privacy .[29]
One option is to replace the WHOIS with the Registration Data Access Protocol (RDAP), a standardised successor of the WHOIS protocol.[30] RDAP allows access to registrant data, but with the option of authenticating access and providing differentiated responses based on who is accessing the data.[31] This addresses some of the privacy concerns by not displaying personal details to non-authenticated users.[32]

The next part of the paper highlights the human rights concerns with the current WHOIS policy. Since the PDP is in its early stages, this is a good time to consider these issues from a human rights perspective when developing recommendations for a next-generation gTLD RDS.

II. Human Rights Concerns

a. Privacy concerns

The right to privacy is guaranteed under Article 12 of the Universal Declaration of Human Rights (UDHR),[33] and Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[34] In recent years, the United Nations Organisation (UN) has recognised that the rights available to people offline should be protected online.[35] A report by the UN Special

[28] ibid.
[29] Next Generation gTLD RDS to Replace WHOIS PDP Working Group (WG) Charter (7 October, 2015) <https://community.icann.org/display/gTLDRDS/WG+Charter> accessed 8 October 2016.
[30] Registration Data Access Protocol (RDAP) <https://about.rdap.org/> accessed 8 October 2016.
[31] Registration Data Access Protocol gTLD Profile <https://www.icann.org/resources/pages/rdap-gtld-profile-2016-07-26-en> accessed 8 October 2016.
[32] Andrew Sullivan, 'Comments from the IAB on RDAP operational profile' (ICANN Public Comments) <https://forum.icann.org/lists/comments-rdap-profile-03dec15/msg00001.html> accessed 25 October 2016.
[33] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) <http://www.un.org/en/universal-declaration-human-rights/> accessed 9 September 2016.
[34] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).
<http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> accessed 9 September 2016.
[35] United Nations General Assembly Resolution 68/167 (adopted 19th December 2013)
<http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167> accessed 9 September 2016.

Rapporteur highlights that states should refrain from forcing the private sector to implement measures that compromise the privacy, security and anonymity of communications services.[36]

The UN Special Rapporteur has recognised that the right to privacy includes the ability of individuals to determine who holds information about them and how that information is used.[37] It cannot be said that once personal data is made publicly available it is no longer private.[38] The WHOIS policy prevents registrants from exercising their right to privacy by allowing their personal data to be publicly accessible.[39]

Privacy and anonymity on the Internet are crucial to protect other human rights[40] and loss of anonymity undermines these rights.[41] Specifically, public access to personal information through the WHOIS database poses a direct threat to the right to security, the freedom of expression and the freedom of association.

b. Right to Security of Person

The right to security of person is articulated in Article 3 of the UDHR[42] and Article 9 of the ICCPR.[43]

[36] Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (2013) <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> accessed 9 September 2016.
[37] ibid.
[38] 'Opinion 2/2003 on the application of the data protection principles to the Whois directories' (2003) Report of the European Council Art 29 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp76_en.pdf >accessed 9 September 2016.
[39] RAA 2013 (n 8) at Section 3.3.
[40] David Kaye, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (2015) p 5, 10 <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx> accessed 19 September 2016;
Human Rights Watch and American Civil Liberties Union, 'With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy' (July 2014) <https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf> accessed 9 September 2016.
[41] The freedom of expression and freedom of association have been recognised as potential rights at risk in relation to WHOIS in previous reports of this working party. See Cross-Community Working Party on ICANN's Corporate and Social Responsibility to Respect Human Rights, 'ICANN's Corporate Responsibility to Respect Human Rights: Recomendations for Developing Human Rights Review Process and Reporting' (2015) p 28 <https://www.article19.org/data/files/medialibrary/38148/ICANN_CS_to_respect_HR_report_ALL_FINAL-PDF.pdf > accessed 9 September 2016.
[42] UDHR (n 33).
[43] ICCPR (n 34).

Public information on the WHOIS database, such as phone numbers and addresses, can make domain registrants accessible in the physical world. This has in the past led to threats to their physical well-being and security.[44] The database facilitates 'doxing', which is the malicious practice of obtaining someone's personal information and making that information widely available to encourage crowd-sourced harassment and intimidation.[45] The harassment comes in many forms, ranging from expensive food delivery orders made under the victim's name,[46] to rape threats.[47] Previously, women entrepreneurs, small business owners working from home and activists in totalitarian regimes have found themselves targeted by these means.[48]

One of the most well-known cases of WHOIS doxing is that of anti-harassment activist Randi Harper.[49] In her case, the doxing led to 'swatting', which refers to the act of making hoax calls to law enforcement to dispatch armed police officers to the victim's address.[50] Her personal information was obtained from various sources, but her address was sourced from the WHOIS database.[51] Unfortunately, this is a fairly common practice, and several doxing 'tutorials' specifically refer to WHOIS as a source of information.[52]

To avoid such incidents, limited safeguards are already built into the WHOIS process. For example, Registrars are required to notify each new or renewed Registered Name Holder of

---

[44] 'Letter to ICANN' (*EFF,* July 2015) <https://www.eff.org/document/july-2015-letter-icann> accessed 9 September 2016.
[45] 'What doxxing is, and why it matters' (*The Economist*, 10 March 2014) <http://www.economist.com/blogs/economist-explains/2014/03/economist-explains-9> accessed 9 October 2016.
[46] Nathan Mattise, 'Anti-doxing strategy—or, how to avoid 50 Qurans and $287 of Chick-Fil-A' (*arsTECHNICA*, 15 March 2013) <http://arstechnica.com/security/2015/03/anti-doxing-strategy-or-how-to-avoid-50-qurans-and-287-of-chick-fil-a/> accessed 10 October 2016.
[47] Anna Merlan, 'The Cops Don't Care About Violent Online Threats. What Do We Do Now?' (*Jezebel*, 29 January 2015) <https://jezebel.com/the-cops-dont-care-about-violent-online-threats-what-d-1682577343> accessed 10 October 2016.
[48] Nadia Kayyali and Mitch Stoltz, 'Powerful Coalition Letter Highlights Danger of ICANN's New Domain Registration Proposal' (7 July 2015) <https://www.eff.org/deeplinks/2015/07/powerful-coalition-letter-highlights-danger-icanns-new-domain-registration> accessed 9 September 2016.
[49] Randi Harper, 'Tales from the Trenches: I was SWATed' (*Randi.io*, 3 April 2015) <https://blog.randi.io/2015/04/03/swated/> accessed 10 October 2016;
Alex Hern, 'Icann plan to end website anonymity 'could lead to swatting attacks'' (*The Guardian*, 7 July 2015) <https://www.theguardian.com/technology/2015/jul/07/icann-plan-to-end-website-anonymity-could-lead-to-swatting-attacks> accessed 10 October 2016.
[50] 'Swatting', Oxford Dictionary, <https://en.oxforddictionaries.com/definition/swatting> accessed 10 October 2016.
[51] Archived 8chan thread (*archive.is*, 10 January 2015) <https://archive.is/HTV2X> accessed 10 October 2016.
[52] For example, see 'How to dox anyone' (*CTRL|ALT|NARWAL,* 21 October 2012) <https://ctrlaltnarwhal.wordpress.com/2012/10/21/how-to-dox-anyone/> accessed 10 October 2016; Helge Liseth, 'How to Dox People Online' (*HelgeSverre*, 8 August, 2015) <https://helgesverre.com/blog/how-to-dox/> accessed 10 October 2016.

the purpose of the personal data collected[53]. Similarly, it is necessary that the registrant's consent for data processing is obtained[54]. However, since it is mandatory for registrants to disclose WHOIS data, anyone who needs to register a domain name within the current regulatory framework has to do so. The collection and storage of information itself makes the registrants vulnerable as the data storage may not be secure or it can be misused by anyone who has access to it.

Another collateral impact of WHOIS is its potential impact on political dissidents. For instance, law enforcement agencies of oppressive countries with records of human rights violations may use legitimate channels to acquire WHOIS data that helps them identify dissidents or owners of blogs.

c. Right to Freedom of Expression

The right to freedom of expression is guaranteed under international law. Article 19 of UDHR[55] and Article 19(2) of ICCPR[56] define this right as the 'freedom to hold opinions without interference and to seek, receive and impart information and ideas through *any media and regardless of frontiers*'. In recent years the UN has explicitly extended this right to online platforms.[57]

The right to privacy is often understood as being essential for the right to freedom of expression to be realised.[58] Without anonymity on the Internet, freedom of expression is directly and indirectly limited by the fear of being personally attacked or punished for controversial writing.

d. Freedom of assembly and association

[53] RAA 2013 (n 8) Section 3.7.7.4.1.
[54] ibid at Section 3.7.7.5.
[55] UDHR (n 33).
[56] ICCPR (n 34).
[57] 'The Right to Privacy in the Digital Age' (2014) Report of the Office of the UN High Commissioner for Human Rights p 5 <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf> accessed 9 September 2016.
[58] Frank La Rue (n 36).

The right to freedom of assembly and association is recognised in international law under Article 20 of UDHR[59] and Articles 21 and 22 respectively of the ICCPR[60].

Similar to WHOIS policy limiting freedom of expression, the freedom of assembly and association are also compromised by publicly available personal data.[61] If registrants can be identified by their personal information, it stifles the ability to use domains as platforms for assembly and association for fear that it may attract abuse from governments or other members of the public.

One of the aims of the WHOIS service is to provide accurate and up-to-date information.[62] However, the public accessibility of private information serves as an incentive for administrators to provide inaccurate details.[63] It is relatively easy for the ill-intentioned to provide fake information, which defeats the utility of the WHOIS database. However, those who provide accurate information find themselves in a vulnerable position, as this information can be misused in a manner that violates internationally recognised human rights, as highlighted above. As a result, the WHOIS database is inadequate to meet its stated aims. Having recognised this, this paper aims to outline the bare minimum privacy standards that should be used to review the rules to find an RDS model that serves a 'more holistic public interest'.[64] The following section examines how an RDS model ought to be modified to address these human rights concerns.

III . Incorporating Data Protection Best Practices into WHOIS

Over the years, ICANN has recognised the problems faced by registrars in fulfilling their WHOIS obligations while remaining compliant with their respective data protection laws.[65] Consequently, an internal procedure for handling conflicts between WHOIS and privacy laws

[59] UDHR (n 33).
[60] ICCPR (n 34).
[61] 'Submission to the Special Rapporteur on the rights to freedom of peaceful assembly and of association' (*Association for Progressive Communication*, 2012) p 4 <https://www.apc.org/en/system/files/APC%20-%20Freedom%20of%20peaceful%20assembly%20and%20association.pdf> accessed 9 September 2016.
[62] WHOIS Primer (n 2).
[63] Opinion 2/2003 on the application of the data protection principles to the Whois directories' (2003) Report of the Article 29- Data Protection Working Party <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp76_en.pdf > accessed 19 September 2016
[64] ibid.
[65] Privacy | ICANN WHOIS (*whois.icann.org*, 2016) < https://whois.icann.org/en/privacy> accessed 9 September 2016.

was developed.[66] This procedure allows Registrars to be exempt from their obligations if they are in breach of their local data protection law.

However, this procedure only kicks in once a data protection authority has initiated enforcement proceedings against the Registrar.[67] The procedure is inherently reactive and puts the onus on Registrars to prove that the WHOIS obligations are in conflict with their local laws.[68] Moreover, this procedure does little to protect the personal information of registrants located in jurisdictions without a robust data protection law, leaving them vulnerable to the threats identified above.[69] Instead of this patchwork approach to privacy, WHOIS policy must be suitably amended to incorporate privacy as a legitimate aim in itself.

This part of the paper identifies the core principles underlying data protection and examines the WHOIS policy against these principles. Further, it proposes *Privacy by Design* as an approach that can be used to incorporate these principles. The aim of this part is to guide the PDP Working Group in ensuring that threats arising from unrestricted access are prevented or mitigated.

In the international context, the formulation of principles for data protection can largely be credited to the Organisation for Economic Cooperation and Development ('OECD').[70] Developed in 1980, the OECD Guidelines governing the protection of Privacy and Transborder Flows of Personal Data ('Privacy Guidelines') outline eight core principles for the protection of personal information.[71] In 1995, the EU Data Protection Directive incorporated similar principles.[72] Influenced by the OECD Privacy Guidelines[73], the Asia

[66] ICANN Procedure For Handling WHOIS Conflicts with Privacy Law | ICANN WHOIS (*whois.icann.org*, 2016) <https://whois.icann.org/en/icann-procedure-handling-whois-conflicts-privacy-law> accessed 9 September 2016.
[67] ibid.
[68] Jeremy Malcolm '*Domain Registrars Have to Ask ICANN's Permission to Comply with Laws Protecting Your Privacy'* (19 October 2015) <https://www.eff.org/deeplinks/2015/10/domain-registrars-have-ask-icanns-permission-comply-laws-protecting-your-privacy> accessed 9 September 2016.
[69] ibid.
[70] Christopher Kuner (2011), 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future', OECD Digital Economy Papers, No. 187, OECD Publishing.
[71] Organisation for Economic Cooperation and Development, 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part Two ('OECD Privacy Guidelines'), available at <https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf> accessed 19 September 2016.
[72] 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, Article 6.
[73] OECD, 'Thirty Years After the OECD Privacy Guidelines' (2011) available at <http://www.oecd.org/sti/ieconomy/49710223.pdf> accessed 19 September 2016, p.11.

Pacific Economic Cooperation (APEC) forum also came up with a Privacy Framework incorporating almost identical principles.[74] These instruments provide the foundation for data protection and privacy statutes in several countries.[75]

a. OECD Guidelines

Given the public nature of ICANN's work and the multistakeholder approach followed by it, it is important to analyze the WHOIS policy in light of data protection norms. More importantly, the ICANN bylaws adopted in May 2016 require the RDS Review team to consider the OECD Privacy Guidelines while exploring structural changes to registration directory.[76]

This part examines informational privacy principles formulated under OECD Privacy Guidelines in the context of the WHOIS database.

1. Collection Limitation – This principle requires that the collection of personal data should be limited to information that is strictly necessary and that collection itself should be fair and lawful.[77] It also stipulates notice and consent as essential requirements before collecting any personal information.[78]

The 2013 RAA allows Registrars to collect and store several categories of data including contact information collected at the time of registration.[79] It also allows collection of all correspondence between the registrant and the registrar[80].

For the WHOIS policy to be fair and lawful, all personal information collected must serve a legitimate end. While the 2013 RAA stipulates that registrants must be given notice of how their information will be used[81], it is unclear how this obligation is given effect to, considering that the purpose of WHOIS is vaguely defined.[82]

---

[74] APEC Privacy Framework <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx> accessed 19 September 2016.
[75] Christopher Kuner (n 70).
[76] ICANN Bylaws (n 14).
[77] OECD Privacy Guidelines (n 71) at paragraph 7.
[78] ibid.
[79] RAA 2013 (n 8) at Section 3.3.1
[80] ibid at Section 3.4.2.2
[81] ibid at Section 3.7.7.4
[82] Purpose | ICANN WHOIS' (*whois.icann.org*, 2016) <https://whois.icann.org/en/purpose> accessed 9 September 2016.

Further, it is important to distinguish between the collection of information and its publication. A justification for collection of information under a contract cannot justify its publication in a public database.[83]

2. Data Quality – This principle stipulates that personal data should be relevant to the purposes for which it is collected and should be accurate, complete and up-to-date.[84] The accuracy of personal information is an important consideration for WHOIS. However, any solution aimed at addressing the problem of inaccurate data must also consider that unrestricted public access to the database acts as an incentive for individuals to provide inaccurate details.[85]

With respect to the relevance of information, it is advisable that the information collected must be strictly necessary to achieve the desired purpose(s). Correspondingly, the retention of this information should be according to its necessity. Data retention periods may differ for different categories of information and must be justified separately.

3. Purpose Specification – According to this principle, the purposes for which the information is collected must be specified at the time of data collection and its subsequent use must be limited to those specific purposes.[86]

Currently, WHOIS data can be used for '*any lawful purposes except to enable marketing or spam, or to enable high volume, automated processes to query a registrar or registry's systems, except to manage domain names'*.[87] This purpose is exceptionally broad. The purposes must be specific and narrowly defined. The mere fact that the collected data can be put to a beneficial use cannot justify its collection.[88] Again, a distinction needs to be made between collection and publication with respect

[83] Email from Jacob Kohnstamm (Chairman, Article 29 Data Protection Working Party) to Steve Crocker and Akram Atallah (26 September 2012) <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120926_letter_to_icann_en.pdf> accessed 19 September 2016.
[84] OECD Privacy Guidelines (n 71) at paragraph 8.
[85] Jacob Kohnstamm (n 83).
[86] OECD Privacy Guidelines (n 71) at paragraph 9
[87] Purpose | ICANN WHOIS' (*whois.icann.org*, 2016) <https://whois.icann.org/en/purpose> accessed 19 September 2016.
[88] Jacob Kohnstamm (n 83).

to purposes too. Collection alone may fulfil a purpose without any need to make the information publicly available. Alternatively, legitimate ends for law-enforcement may be met by providing authenticated access.

4. Use Limitation – According to this principle if the data is intended to be used for any purpose(s) other than those specified at the time of collection, individuals must be given adequate notice and an opportunity to object.[89]
Unrestricted public access to the WHOIS database automatically defeats this principle as it allows personal information to be used for *any* purpose. Consequently, to ensure that the use of personal information is limited to the specified purposes, restricting access to the WHOIS database is essential.

5. Security Safeguards – Personal data is required to be protected by reasonable security safeguards against risks such as unauthorised access, destruction, use or disclosure.[90]
The obligation to put reasonable security safeguards is of special importance in the WHOIS context. This obligation extends to preventing personal data from being accidentally or deliberately compromised.[91] The harms arising out of public access to the WHOIS database have been amply documented in this paper and elsewhere[92]. Safeguards could include a continuation of the policy that allows privacy and proxy services to be used by registrants. However, these services require registrants to take proactive steps to protect their information. A more robust safeguard would be to redesign the system such that public access is not the default setting. In this light, proposals such as RDAP, which allow for authenticated access are better alternatives to meet this obligation.

6. Openness – This principle requires that practices and policies be open and transparent.[93] It should be easy to identify the nature of personal data, their uses and

[89] OECD Privacy Guidelines (n 71) at paragraph 10.
[90] ibid at paragraph 11.
[91] Information Commissioner's Office, 'Guide to Data Protection' <https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-5.pdf> accessed 19 September 2016, p.75.
[92] Sarah Jeong and Kendra Albert, 'An Unassuming Web Proposal Would Make Harassment Easier (*Wired,* 07 February 2015) <https://www.wired.com/2015/07/unassuming-web-proposal-make-harassment-easier/> accessed 19 September 2016.
[93] OECD Privacy Guidelines (n 71) at paragraph 12.

the identity of the entity in-charge of implementing these principles.[94] The ambiguity associated with the purpose of the WHOIS database has an impact on the principle of openness. Openness demands that the purpose for collection of data and its subsequent use must be clearly communicated to the registrant at the time of collection.

7. Individual Participation – Individuals should be allowed to access the data held about them.[95] This principle has already been adequately incorporated under the current WHOIS framework.[96]

8. Accountability – Data controllers[97] should be accountable for complying with measures that have been put in place pursuant to the principles outlined above.[98] Consequently, registrants must have a remedy against registrars or ICANN in case of any negligence or wilful disregard for the protection of personal information collected by the latter. This right must exist irrespective of any actual harm stemming from the disclosure of data.

The obligation to prevent harm arising from misuse of personal information is inherent in these principles. However, the APEC Privacy Framework recognises it as a distinct principle for data protection.[99] It expressly acknowledges the risk from misuse of information and points towards the need for specific obligations to account for such risks.[100]

b. Privacy by Design

One method to incorporate these principles under the WHOIS framework is to adopt the '*Privacy by Design'* approach. Developed in the 90s, this approach rests on the premise that privacy cannot be guaranteed solely by regulatory or legislative methods and encourages

[94] ibid.
[95] OECD Privacy Guidelines (n 71) at paragraph 13.
[96] RAA 2013 (n 8) Section 3.7.7.4.4.
[97] The OECD Privacy Guidelines define a data controller as '*a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf*'.
[98] OECD Privacy Guidelines (n 71) at paragraph 14.
[99] APEC Information Privacy Principles, Principle I.
[100] ibid.

organizational methods to safeguard privacy.[101] It is a proactive approach aimed at preventing privacy invasive consequences rather than offering remedies.[102] *Privacy by Design* is a recommended approach since it seeks to reconcile competing interests rather than choosing one over the other.[103]

In 2012, the US Federal Trade Commission recognised *Privacy by Design* as one out of three recommended practices for online privacy.[104] Subsequently, it was incorporated into the European Data Protection Regulation as a distinct obligation for data controllers.[105]

One of the core principles of *Privacy by Design* is embedding privacy into the design and architecture of systems.[106] One of the ways to implement *Privacy by Design* is to conduct a Privacy Impact Assessment (PIA).[107] PIAs are an important tool for organisations to assess the risks arising out of processing personal data collected by them. The goal is to design systems in a way that minimize the privacy risks associated with them.[108] In the current context this can include incorporating systems or protocols such as the RDAP that allow layered or conditional access to the WHOIS database. RDAP includes features to identify, authenticate and authorize clients, thereby controlling access to information based on their identity.[109]

Conclusion

Multiple aspects of WHOIS policy have significant implications for the right to privacy on the Internet. This paper contends that the violation of the right to privacy has an effect on other human rights - the right to security of person, freedom of expression, and freedom of assembly and association.

---

[101] Ann Cavoukian, 'Privacy by Design' <https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-primer.pdf> accessed 19 September 2016.
[102] ibid.
[103] ibid.
[104] ibid.
[105] Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 25.
[106] Ann Cavoukian (n 101).
[107] Information Commissioner's Office, 'Conducting Privacy Impact Assessments Code of Practice' <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf> accessed 19 September 2016.
[108] ibid.
[109] Internet Engineering Task Force, 'Security Services for the Registration Data Access Protocol (RDAP)' <https://tools.ietf.org/html/rfc7481> accessed 19 September 2016.

There is limited research into the impact WHOIS has on privacy, and even less on the effect of the policy on other human rights. This paper highlights the core principles governing data protection globally and recommends that the WHOIS policy should be examined in light of these. Most importantly, this paper reiterates that ICANN should hold these human rights considerations as being fundamental to WHOIS policy, rather than an afterthought.