International Working Group
on Data Protection
in Telecommunications

675.55.6

Working Paper on Privacy and Data Protection Issues with Regard to Registrant data and the WHOIS Directory at ICANN[1]

62nd meeting, 27-28 November 2017, Paris (France)

The International Working Group on Data Protection in Telecommunications (IWGDPT, a.k.a. "Berlin Group") has for many years been interested in matters relating to the privacy and data protection of registrants of domain names. From the earliest days of the Internet, those early researchers who had a presence there were listed in a directory called the WHOIS. When the Internet was transferred from U.S. government control to the multi-stakeholder entity established to manage the Domain Name System (DNS), this WHOIS service was required to be maintained. It is not a single, centrally-operated database but run by entities who operate the domain name system as we know it today, the "registries" and "registrars".[2]

The Internet Corporation for Assigned Names and Numbers (ICANN) was created as a not for profit corporation in the state of California in 1998, in order to manage the assignment of names and numbers for the domain name system (DNS) of the Internet. The business of selling or licensing the use of domain names was opened up to more registrars at that time, as long as they were accredited. Obligations with respect to the collection, use, disclosure in WHOIS, and data retention are included

[1] The Privacy Protection Authority of Israel abstains from the adoption of this Working Paper.
[2] See ICANN description on WHOIS at https://whois.icann.org/en/about-whois#field-section-1.

Secretariat
Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

in the registrars' accreditation agreements,[3] and there have been four of these over the years.[4] Registrars and a wide variety of resellers have contact with the registrants or end-users, and certain data necessary to enable a domain name to function is shared with the registry, or the entity that controls the allocation of resources within its top level domain (e.g. .com, .paris, .fr). ICANN, with its multi-stakeholder community, controls the policy which governs the generic top level domains or gTLDs, while individual countries and regional government bodies govern the policy in their own two letter country codes or ccTLDs (e.g. .ca, .de, .eu).

The first common position of the Working Group with respect to the WHOIS was prompted by a report of the World Intellectual Property Organization (WIPO) on the needs to contact registrants, and was published in 2000.[5] Since that time, the IWGDPT has shared the concerns of the Article 29 Working Party on Data Protection, and followed their correspondence with ICANN over many years (see a short list in Appendix A).

The Council of Europe (CoE) released a report on ICANN procedures in relation to human rights in 2014.[6]The IWGDPT welcomes that the CoE since, in line with the Declaration of the Committee of Ministers on ICANN, human rights and the rule of law (adopted by the Committee of Ministers on 3 June 2015 at the 129th meeting of the Ministers' Deputies) is closely following the issues related to data protection and privacy within ICANN and more particularly the WHOIS. This is also reflected in its strategy report of April 2016,[7] and in the guide for compliance entitled Privacy and Data Protection Principles Guide for ICANN Related Data Processing[8] released in October 2017. Most recently, the Dutch Data Protection Authority, at the request of a Dutch registry published an analysis (October 30, 2017) about ICANN's required WHOIS practice. The Dutch DPA found that unlimited publication of WHOIS personal data of domain name registrants by this Dutch registry violated Dutch privacy law.[9]

---

[3] See the first Registrars Accreditation Agreement (1999), https://archive.icann.org/en/nsi/icann-raa-04nov99.htm.
[4] 2013 Registrar Accreditation Agreement, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa; 2009 Registrar Accreditation Agreement, https://www.icann.org/resources/pages/ra-agreement-2009-05-21-en; 2001 Registrar Accreditation Agreement, https://www.icann.org/resources/unthemed-pages/raa-2001-05-17-en; November 1999 Registrar Accreditation Agreement, https://www.icann.org/resources/unthemed-pages/raa-1999-11-10-en.
[5] Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet, adopted at the 27th meeting of the Working Group on 4/5 May 2000 in Rethymnon / Crete, https://www.datenschutz-berlin.de/working-paper.html
[6] https://rm.coe.int/168048f14f
[7] https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c1b60
[8] https://rm.coe.int/168076169f
[9] https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-unlimited-publication-whois-data-violates-privacy-law

While many years have passed, and numerous study groups, task forces, and expert groups have looked at the WHOIS issue, most of the issues raised in 2000 have yet to be resolved. The mechanism that ICANN has provided since 2008 for WHOIS conflicts with data protection law, requires that registrars must apply for a waiver from the precise requirements that are in conflict with local law. This process requires the registrar to provide proof of that conflict in the form of an enforceable order or opinion from a data protection authority. As of 2017, this waiver process to allow compliance with law is not being utilized extensively, and the registrars who are obliged to seek it, have reported significant dissatisfaction with the process.[10]

Although the privacy issues have been brought up and contested over the many years that WHOIS has been studied and discussed at ICANN, there has not been a de novo review that looks at the original purpose of the directory. Many "use cases" have sprung up because the data in the registrant directory is useful for marketing, research, rights protection, consumer protection, law enforcement, and other purposes. This has led to increasing demands for data from different stakeholders who are organized in the ICANN community, that have found their way to some extent into the 2013 RAA.[11] This was in the view of the Article 29 Working Party in contradiction of European data protection law in several respects. The Article 29 Working Party has shared extensive comments on this in the past.[12]

The 2014 Report of the ICANN Expert Working Group[13] proposed a new type of registry with tiered access, but also many more new data elements, and a consent clause that would in the view[14] of the privacy expert on the committee, result in eroding data subjects' rights. Given that a new group (the Generic Names Supporting Organization (GNSO)/Registration Directory Service (RDS) working group)[15] has been working at ICANN since late 2015 to study the policy issues of WHOIS and to determine its purpose, it is time to revisit the many issues and provide recommendations.

---

[10] Final Report on the Implementation Advisory Group Review of Existing ICANN Procedure for Handling Whois Conflicts with Privacy Laws https://gnso.icann.org/en/drafts/iag-review-whois-conflicts-procedure-23may16-en.pdf

[11] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

[12] See eg. Letter from the Art. 29 Working Party of 26.09.2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120926_letter_to_icann_en.pdf, and the follow up letter of 06.06.2013 from the Article 29 Working Party addressed to ICANN regarding the statement on the data protection impact of the revision of the ICANN RAA http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130606_letter_to_icann_en.pdf

[13] https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf

[14] https://www.icann.org/en/system/files/files/perrin-statement-24jun14-en.pdf

[15] https://community.icann.org/display/gTLDRDS/Next-Generation+gTLD+Registration+Directory+Services+to+Replace+Whois

This Working Paper examines those unresolved issues, and new ones which have arisen over recent years and provides recommendations on the respect for individual rights with regard to the registration of domain names. This paper and its recommendations are limited to issues concerning personal data.

Data Protection Issues

From early days, civil society participating at ICANN as a stakeholder group representing non-commercial users (the Noncommercial Users Constituency or NCUC) has demanded the right not to put personal data in the WHOIS. Registrars complied with this desire by providing privacy/proxy services, putting their own information into the WHOIS in place of the personal information of the end user. Where available to individuals, this service has taken some of the pressure off the privacy issue, but the existence of a proxy service for WHOIS does not solve all the problems.

With respect to domain or name registration data, there are several areas of concern:

- The requirements set out in the 2013 RAA concerning data collection from registrants of domain names appear to be excessive, disproportionate, and obtained without the free consent of the individual. The Article 29 Working Party has shared comments on this in the past.[16]
- The accountability for personal data processing does not appear to be clearly allocated between the various actors involved in the domain or name registration process. This makes it difficult for the data subject to define who is the controller or joint controller, and to enforce his/her rights with resellers, accredited registrars, registries, and ICANN itself.
- Personal data disclosure in the public directory, or WHOIS, is not proportionate to the original purpose of the WHOIS given the impact on privacy, and is contrary to data protection principles and to the data protection law in many jurisdictions. Layered or tiered access has been proposed as a privacy enhanced solution, but at the moment the directory continues as a fully and anonymously accessible, searchable database.

[16] See eg. the letter from the Art. 29 Working Party of 26.09.2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120926_letter_to_icann_en.pdf , and the follow up letter of 06.06.2013 from the Article 29 Working Party addressed to ICANN regarding the statement on the data protection impact of the revision of the ICANN RAA http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130606_letter_to_icann_en.pdf

- The data in WHOIS has been gathered by value added service providers, and it can be difficult for registrants, once they have provided name, address and phone number, to extricate themselves from these commercially available data collections (e.g. DomainIQ, Domain Tools[17]).
- The IWGDPT acknowledges the importance for law enforcement to have timely access to registrant data in order to investigate crime, when necessary and legitimate. The conditions for access have to be determined by law and not by ICANN. A system of layered access does not have to impose obstacles to such lawful access.
- Several data processing activities required by the 2013 RAA are outside of the original purpose of ICANN's gTLD policy organization, as adopted in 2006. The 2006 policy was approved by the Generic Names Supporting Organization (GNSO) Council and defines the following purpose for publishing registration data in the WHOIS directory:

  The purpose of the gTLD Whois service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a [Domain Name System] name server.[18]
- Other processings of registration data (e.g. collection and escrow) may have valid purposes, such as the fulfillment of a contract. ICANN needs to define these purposes as appropriate to its mission and mandate. To the extent that ICANN controls the collection of data through its contracts, and compels the registrars to collect, display, retain and escrow data, it is a data controller. ICANN has to create an exhaustive list of the legitimate purposes for the data processing, not just the publishing of any data in the WHOIS. It must therefore determine what data may legitimately be processed for what purpose. Different data protection laws are drafted in different ways, but they all share common principles. The purpose must be clearly defined in advance of collection (processing) and related to the mission of the organization. Data collection must be limited, specific, and proportionate. The fact that many different third parties now benefit from the ability to get data freely from the WHOIS, and use it for a multitude of their own purposes, does not necessarily mean that these are legitimate purposes for ICANN to collect data, nor that such practices may continue.
- Data retention may not be lawful or proportionate, particularly as some data elements seem to be processed solely for the possible future use by law enforcement. The entire issue of how law enforcement agencies, private sector security companies, and private sector trademark and copy-

[17] https://www.domainiq.com/ , https://www.domaintools.com/

[18] *Preliminary task force report on the purpose of Whois and of the Whois contacts* https://gnso.icann.org/en/issues/whois-privacy/prelim-tf-rpt-18jan06.pdf. At that time, the GNSO Council was responsible for developing ICANN gTLD policy.

right holders make use of registrant data is a question that needs to be examined in full acknowledgement of legally enforceable data protection rights of registrants, including Charter or Constitutional rights related to due process in criminal and civil procedures in each country.

Recommendations

In the light of the above, the IWGDPT makes the following recommendations:

Purpose

1. **The legitimate purposes of the processing of registrant data and of the disclosure in the public directory need to be defined. These legitimate purposes need to be limited to the narrow remit of ICANN, which is to manage the assignment of names and numbers in a manner that assures the security and stability of the Internet.**

   It is well understood that there could be legitimate purposes for various parties to collect certain personal information, but that does not necessarily mean that those purposes are legitimate purposes for ICANN to require processing of the personal data. Such requirements for the usage of personal data must be permitted by (national) law or international treaty or convention.

   As a general rule, any processing necessary for the fulfillment of the contract between registrar and registrant would be permitted by privacy legislation. Access to registrant data stored with the registrar would also be permitted under national law enforcement legislation as applicable. But such a lawful access, however, can neither justify the global publication of registrant data on the Internet, nor the retention of additional data not necessary for the original purpose. Access to data regarding the technical contact for a domain in order to swiftly resolve technical malfunctions may be in line with applicable privacy legislation. Any other uses by other stakeholders would have to be seen as secondary uses, for which the privacy legislation in many countries foresees certain restrictions, which may not allow for publication of registrant data on the Internet.

   The global distribution of stakeholders over different jurisdictions adds additional complexity, as – at least for registrars based in the European Union – the adequate level of protection in the jurisdiction of the party demanding access to registrant data has to be taken in account.

   The IWGDPT strongly recommends that ICANN address these issues in the current process for re-designing the WHOIS system, and clearly defines the various purposes accordingly.

Data Limitation

2. **The personal data collected from and about registrants must be limited to that which is necessary for the purposes as described in recommendation No. 1 of this Working Paper. This includes the processing of data necessary for the registration of the domain name. Also, the personal data disclosed in the public directory must be limited to that which is necessary for assuring contactability of registrants in the event that there are technical issues related to the name registered.**

It is important to make a distinction between these two purposes, focusing on data limitation. If the purpose of publication is to get in touch with the domain name holder for technical issues, it has to be assessed which data are strictly necessary for that purpose and what is the least intrusive way to achieve this purpose, for instance by using privacy proxies and layered access approaches. Furthermore, the data that the registrar is required to escrow, to secure the rights of the registrants and ensure continuity in the event of the sudden disappearance of the registrar, must also be limited to the purpose of the escrow.

Access to data by law enforcement

3. **Access to personal data must be as provided for by law. Such law needs to be transparent, foreseeable and proportionate to the legitimate aim pursued in a democratic society.**

Of course law enforcement agencies should be able, through a system of tiered access, to have timely access to the WHOIS data of registrants. Additionally, they should have the means to request additional data (for example financial data) from registrars to the extent necessary for their investigations. It does not necessarily follow that publishing personal data is the appropriate way to serve these legitimate purposes. The rise of cybercrime, phishing attacks, and the use of the Internet as a communications medium for a wide variety of crime is of concern to everybody. However, it is questionable whether it is the role of ICANN, as a private corporation, to require its contracted parties to assemble data and provide it, without regard to human rights concerning fair legal procedure, to the global law enforcement community, and to private sector security companies. While recognizing the important role that various private sector entities perform in combatting phishing and cyberattacks through the use of the DNS, this “clearinghouse” approach

to registrant data is not in compliance with data protection law. ICANN needs to promptly address solutions that ensure tiered access to accredited entities, who can show evidence of legitimate need for the data.

Data Retention Requirements

4. **There are two data retention requirements in the 2013 RAA[19] which are problematic in terms of data protection law. ICANN should reexamine them and ensure compliance with applicable law.**

   One ICANN requirement is to escrow data with an approved escrow agent (section 3.6), which is a legitimate processing activity as it relates to the rights of the registrant. The second is the requirement of the registrar to retain data for various purposes, notably access by law enforcement (section 3.4). As noted in previous correspondence cited in Appendix A, this should be re-examined, and must be reduced to what is necessary for business requirements.

   One of the fundamental principles of data protection law is to limit the time that data is held in identifiable form, and only keep it for the original purposes or other compatible purposes.

Searchability and other functions of a Reverse Directory

5. **Any new Registration Data Service should investigate means of restricting searches to those related to the purpose of the processing of the data.**

   Certain functions of reverse directories, such as the ability to check all entries registered to a person, are not consistent with the original purpose of the directory. A new RDS should explore and further require technical means to restrict bulk data capture.

Transborder Dataflow

6. **ICANN should explicitly address the issue of transborder dataflow in its policies, and ensure that data transfers ensure adequate data protection is maintained.**

[19] 2013 Registrar Accreditation Agreement, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

The issue of where the data is held has not been a subject of previous commentary from the IWGDPT. It is the understanding of the IWGDPT that under the recently completed new policy known as "Thick WHOIS",[20] registrars who formerly maintained the data of gTLD registrants themselves and provided WHOIS access through port 43, are now transferring the data to the registries, including the big registries such as .com, .net, and others. This represents 75% of the gTLD registrations, which means there will be significant transfers of personal data to the United States, where, for instance, the largest registry operator Verisign holds its data. It is important that data be protected in a manner that ensures continuous protection to the "adequacy" standard, and that registrants are aware of this transfer. If technology permits the data to remain in the jurisdiction of the registrant or registrar, we would recommend limiting dataflows to only those which are absolutely necessary.

Distinguishing Between Commercial and Personal Data

7. Commercial data which may be disclosed must not include personal data.

While recognizing that commercial entities have less or no protection under data protection law than individuals, we recommend that ICANN acknowledges that commercial data may also include personal data. In its WHOIS-policies, ICANN should take into account that contact data from small business, sole contractors, home businesses and start-ups may be personal data. Secondly, ICANN should develop a procedure to distinguish between public contact data from companies and personal data from individual employees working for companies. The IWGDPT notes that businesses engaged in electronic commerce are likely to be regulated by national or regional law, in which case it is often mandatory for them to publish contact data on their website. This is not a role for ICANN or the WHOIS.

Development of a comprehensive policy on the processing of data to provide uniform standards

8. The IWGDPT recommends that ICANN develop a data processing policy that is in line with the requirements of existing privacy legislation and internationally recognized data protection and privacy principles and standards.

[20] https://www.icann.org/resources/pages/thick-whois-transition-policy-2017-02-01-en

ICANN's current policy (the WHOIS conflicts with law policy) is not in line with the privacy laws in many jurisdictions. The policy requires registrars to apply for a waiver of the obligations regarding collection, use, retention and disclosure of personal information which are in their contracts. Given the high administrative hurdles of obtaining such a waiver, this policy puts the privacy of registrants of domain names at risk. It also puts many of the registrars in a difficult position. In practice, they have to face breaking national privacy law until the waiver is granted by ICANN, or be in breach of their contractual obligations vis-á-vis ICANN. On the other hand, less privacy aware registrars who are not paying attention to data protection law and therefore not respecting registrants' rights, will not face sanctions from ICANN. This does not seem to be a reasonable way to conduct business globally, when there are now 120 data protection laws in place. While in theory each registrar in each jurisdiction could apply for a waiver at ICANN that would allow him to act within the limits of its national privacy legislation, this process puts an unreasonable burden on the registrars and the relevant national authorities of having to act against unlawful contractual requirements. ICANN must therefore start with a WHOIS policy that is compliant with the highest data protection requirements.

The IWGDPT notes that lately ICANN has engaged in outreach with Data Protection Authorities,[21] and seeks feedback on compliance models,[22] released on January 12, 2018. This release has been after the editorial deadline of this Working Paper.

[21] The correspondence is available on the ICANN website: https://www.icann.org/resources/pages/correspondence

[22] See https://www.icann.org/news/blog/data-protection-and-privacy-update-seeking-community-feedback-on-proposed-compliance-models

Appendix A Correspondence of the IWGDPT and the Article 29 Working Party with ICANN

Since 2000, the IWGDPT and the Article 29 Working Party have made contact with ICANN to express their opinions on data protection issues with respect to how ICANN has managed and directed the collection, use, retention and disclosure of registrant data. A brief summary:

- 2000 the IWGDPT issued a common position on WHOIS data
- 2000 the IWGDPT issued a ten commandments for protecting privacy on the Internet
- 2003 IWGDPT wrote to ICANN with concerns about the Interim Report Of The Names Council's WHOIS Task Force Of October 14, 2002
- 2003 Article 29 WP issued opinion on WHOIS (2/2003)
- 2005 IWGDPT wrote to the International Working Group on Internet Governance (IWGIG) to let them know that the two groups exist and are interested in Internet privacy issues and further cooperation
- 2006 Article 29 WP wrote to Chairman (Vint Cerf) with concerns about ongoing WHOIS review and failure to identify purpose of data collection
- 2009 The International Conference of Data Protection and Privacy Commissioners resolved to explore observer status at ICANN
- 2012 the Article 29 WP wrote to Chairman (Crocker) and acting CEO (Atallah) expressing concerns about 2013 RAA with respect to legitimate purpose, data accuracy, and data retention.
- 2013 the Article 29 WP wrote to the Chairman (Crocker) and the CEO with its concerns about the 2013 RAA, indicating that all European registrars would require a “waiver” according to the ICANN Conflicts with Law procedure
- 2014 the Article 29 WP wrote to ICANN’s General Counsel (Jeffries) re-iterating its concerns about the 2013 Registrar’s Accreditation Agreement, and reaffirming its own authority to represent the 26 members of the group in a common position
- 2014 Peter Hustinx, then European Data Protection Supervisor wrote to the Chairman (Crocker) to inform him that the data retention directive had been declared unconstitutional by the European Court of Justice, and that ICANN’s data retention requirements were not lawful.
- The Article 29 Working Party has issued a letter on ICANN and its data practices on 11 December 2017.