Answers to Questions for ICANN58 Data Protection Experts
developed by members of the RDS PDP WG

Introduction

The following questions have been drafted by members of the ICANN GNSO Next Generation gTLD Registration Directory Services (RDS) Policy Development Process (PDP) working group (WG) for consideration by the Data Protection Experts who participated in the ICANN58 meeting in Copenhagen.

This working group's charter includes "analysing the purpose of collecting, maintaining and providing access to gTLD registration data (…) and safeguards to protect that data." On that basis, the working group is tasked to "determine if and why a next-generation Registration Directory Service is need to replace WHOIS (…)" – that is, the current system which provides public access to registration data collected when a domain name is registered. In addition, this working group is tasked with "creating policies and coexistence and implementation guidance to meet those needs."

The answers given to the questions were shared, discussed and consented by: the United Nations' Special Rapporteur on the right to privacy, the European Data Protection Supervisor, the Vice-Chairman of the Article 29 Working Party, the Chair of the Committee of Convention 108, the Data Protection Officer of Interpol and the Director of Information Society and Action against Crime of the Council of Europe. The answers had the aim to ensure a better understanding on the interpretation of ICANN policies and underlying privacy issues by senior privacy experts and to provide a base for further dialogue on that matters.

It is hoped that Data Commissioner insights into the following questions might enhance the working group's understanding of the European Union data protection framework and inform the working group's deliberations about the application of data protection laws to gTLD registration data and directory services policies. It is to be noted that the responses provided are not solely specific to EU laws but reflect the approach of global privacy legislation and thus may be more broadly useful to the WG.

Purpose

1. Our working group is now deliberating upon the purpose of domain name registration data and the registration directory system that provides public access to that data. Can you please help us understand what the data protection supervisors have meant over the years when they have told ICANN to specify the purpose of WHOIS?

Purpose has to be defined in advance of the data processing. Purposes have to have a legitimate aim and the processing has to be necessary and proportionate to the legitimate aim pursued. Translating this to ICANN means the WG would want to take a look into ICANN role and its mission statement and separate out the legitimate data processing purposes, and determine which data are necessary for which purpose. It is to be underlined that the compatibility of the processing to the original legitimate purpose should be also looked into at this point. You have also to bear in mind that according to all existing legal texts, the data controller has to be accountable for the data processing and that the purpose of the WHOIS

directories cannot be extended to other purposes just because they are considered desirable by some potential users of the directories.

To illustrate it with an example if ICANN determines that it has a role in cyber-security ,it will become accountable for these kinds of data processing (meaning accuracy of data, handling complaints, providing subject access etc…) but cannot give out data just because law enforcement authorities may find it useful.

How would you assess the purpose of collecting,
ICANN has to define the legitimate purposes for the data processing, and secondly, determine what data may legitimately be processed for what purpose. As data protection experts, we have repeatedly pointed out that ICANN should create layered access to the gTLD registration data.

processing, maintaining and providing access to gTLD registration data? For example, can you help us understand what a purpose applies to when it comes to registration data or directory services? Where will purpose be applied (and not be applied) in registration data and directory services policies? What criteria should be used to determine legitimate purpose(s)? What is the difference between "primary" and "secondary" purposes and how does that affect all of the above?

The question of access to gTLD registration data is a distinct one for which clear conditions are applicable. To be completed…

2. Article 6(1)(b) Directive provides that personal data may only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (Article 7). Processing of personal data is allowed to a limited number of legitimate grounds, specified in Article 7 Directive. Under what circumstances might the publication of registration data elements that are personal data be allowable?

The legal ground of 6(1)b can only be used if the data processing is necessary to perform a contract, in relation to each individual user. Clearly, this necessity depends on the purpose of the processing. If one of the purposes would be to allow people to get in touch with a domain name holder, ICANN needs to asses which data are strictly necessary for this purpose and which are the less intrusive ways to achieve this purpose. That is, ICANN has to assess the proportionality in relation to each user, and the subsidiarity, whether there are alternative ways of making these data available when necessary, such as the use of privacy proxies and layered access. ICANN needs to for example distinguish between registration data relating to individual users, and registration data relating to legal persons.
In summary publication is a processing operation, it needs to match a purpose and the proportionality is the key aspect to focus on: is the data published proportionate to the purpose of the processing? (which is to keep contact with domain name holder).

Registration Data Elements

3. Considering that gTLD registration data elements may refer to mere technical information, information that may relate to legal persons and information that may directly relate to an identified or identifiable natural person, only the last one of which has consequences from a data protection perspective, how do you think consistent policies for a Registration Directory Service could best be developed?

Policies should be developed using a Privacy Impact Assessment. One should take every segment of the data processing activities and assess whether on its own or in combination with other data processing personal data are processed in this segment of the activity. If yes, one should put in place data protection safeguards, if not only data security safeguards. It is for example necessary to distinguish between public contact data from companies (such as: admin@companyname.domain), and personal data from individual employees working for these companies.

For example, it is our understanding that "personal data" under the EU Data Protection Directive and the General Data Protection Regulation is specified if data relates to an identified or identifiable natural person. Currently, Registrars and Registries display the following info through a public directory service called WHOIS without any access restrictions: the domain name registrant's full name, street address, zip code, country code, telephone number and email address. Is this "personal data" as specified by the Directive and the General Data Protection Regulation, regardless of whether the registrant is a legal person or a natural person?

Yes, these certainly are personal data. It is important to distinguish between the different responsibilities. Since ICANN determines most purposes of the processing of the gTLD data, ICANN is a data controller. According to the European Data Protection Directive and the General Data Protection Regulation, parties may be joint-controllers. In this case, the registrars may be considered joint controllers, to the extent that they collect and process personal data for the purposes determined by ICANN and for their own purposes. Both ICANN and the registrars are violating European data protection law by determining, respectively facilitating an unlimited public access to these WHOIS-data. Such access is disproportionate and does not take into account the rights and freedoms of individual data subjects in the EU.

There are, in short, many different ways to achieve the management of domain names and provide a mechanism to contact registrants or their agents without releasing all this personal data in a public directory on the Internet.

As to the registrant being a legal person or a natural person, when ultimately the data published in WHOIS is personal data (of a natural person), data protection applies.

4. Article 5 of the EU commerce directive requires service providers to disclose their contact information. Does this directive apply to domain name registrants? Does that mean that registrants that are service providers in the EU could be required to have their contact data displayed in a registration directory service?

The obligation in Article 5 of the eCommerce Directive relates to parties providing an information society service, such as a webshop, usually for remuneration. There is no obligation on individuals when they use a domain name to publish their (private) contact details on their website. Commercial service providers must make available their name, a geographical address and an e-mail address, such as 'customerservice@webshop.domain'.
If they choose to publish WHOIS data this is mainly because of ICANN policies and contracts.

5. Below is an example of "thin data" elements made publicly accessible in today's WHOIS system for every registered gTLD domain name. Do you believe that any of the following data elements are considered personal information under the General Data Protection Directive, and why?

Domain Name: CNN.COM
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Whois Server: whois.corporatedomains.com
Referral URL: http://www.cscglobal.com/global/web/csc/digital-brand-services.html
Name Server: NS-1086.AWSDNS-07.ORG
Name Server: NS-1630.AWSDNS-11.CO.UK
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Updated Date: 15-feb-2017
Creation Date: 22-sep-1993
Expiration Date: 21-sep-2018

This information can be easily combined with other data sets freely or easily accessible, then yes, it is "personal data". Google itself is offering look up services, reverse look up services (for free). Besides there are websites which are harvesting data from whois.corporatedomains.com and making them accessible freely with personal data as on WHOIS Servers there is personal data. (see: www.who.is for instance). As long as the identification of a person behind this information and numbers is possible, it is considered as personal data.

Access to Registration Data for Criminal and Abuse Investigations

6. It is our understanding that the suppression of criminal offences is an exemption to the application of the General Data Protection Regulation. If or when could this exemption apply to private cybersecurity firms investigating crime, civil offenses, or abuses in general by using data obtained through a registration data directory service?

The use of the exemptions from the data protection legislation has to be provided for by law, and the exemption has to be necessary in a democratic society. Cyber security issues are dealt with by public organisations belonging to police, to national security agencies or other independent but public bodies bound by legislation and external oversight mechanisms. This basically means that the measures have to be foreseen by law, easily accessible and understandable, and they have to be necessary and proportionate to the legitimate aim pursued. If private sector firms are doing private law enforcement, civil offense, or abuse investigations, they are considered data controllers, and thus subject to the provisions of current and future data protection law.

7. If the application of General Data Protection Regulation provisions led to a completely private domain name registration database, where the vast majority of registrants refused to give access to their data, should the economic repercussions of closing the database be taken into account, to evaluate whether or not to apply the General Data Protection Regulation? For example, would economic repercussions be seen as threatening the 'monetary interests of the State' or the economic rights of private cybersecurity firms and the IP industry?

The question would imply that the application of data protection legislation will lead to a complete anonymity for domain name registrants. This is incorrect. ICANN should focus on legal conditions of lawful data processing and of lawful access by third parties for legitimate purposes to the data necessary for their tasks.

The monetary interests of a State are represented and enforced by the State. The economic interests of private parties do not prevail over the respect of human rights and fundamental freedoms. This exception on the applicability may only be invoked in specific circumstances, related to specific personal data.

Personal Privacy/Human Rights

8.Today, a public access WHOIS directory service enables anyone who may be the victim of defamation, threats, harassment, etc., to look up the name of a domain name registrant (which may or may not correspond to the owner of a website hosted at that domain name), as a deterrent to such attacks. Do you believe this deterrent effect can constitute a public service,

instead of protecting the privacy rights of the perpetrators? This effectively contributes to the fight against online violence against women, who are often the victims in such cases.

No, regardless of how useful access to registrants' personal data might be in specific cases, unlimited access is disproportionate. Moreover we should bear in mind that to achieve this purpose different procedures already exist. Victims of slander or defamation may use a notice and takedown procedure aimed at the hosting provider (and not turn to the registrar) of the website, to end the violation of their rights, and go to (civil) court to get an order for takedown of the information, or go to law enforcement to ask for a takedown, or start a criminal investigation to prosecute the offenders.

The determination of whether to publish the information of everyone in the world, who registers a domain name, in order to catch harassers and defamatory speakers, raises the question of the interest in disclosure versus the proportionality of the disclosure. There are big differences in the interpretation of this balance, and the question of who will decide is important. It is however a widely acknowledged principle that criminal investigation and law enforcement activity as such should be carried out in the respect of human rights and fundamental freedoms.

9. Under the General Data Protection Regulation, is consumer protection an objective pursued by the State which would fall into the category of protecting the rights and freedoms of others? If yes, do you consider anonymous public access to registration data an additional protection given to consumers, to help them avoid scams?

We don't understand the question. We have an issue with the unlimited access to WHOIS-data, and current practice of third party access. Such access, in our sense would have to be logged and audited to see if parties do not abuse the limited purpose for which they are requiring access.

10. With regards to General Data Protection Regulation compliance by entities within the EU, would it be enough legally if ICANN consensus policies define a new Registration Directory Service which allows for controlled access to registration data, without requesting the data subject's formal consent for each use, especially uses that do not benefit him/her, but are lawful (for example, the suppression of criminal offenses)?

Consent is only one legal basis for data processing, but it's not the only one. There are actually more bases for processing that relate to whether the processing is foreseen by law, or required by contract remembering that all must be fair and proportionate. The data processing for the legitimate interest of ICANN can be further assessed bearing in mind that for this use the so called "balance test" is required.

Furthermore it is to be stressed that even if the processing is founded on a correct legal basis, this does not exempt controllers from respecting the entire set of data protection principles (including fairness and proportionality of course).

11. Numerous stakeholders at ICANN have suggested that asking end users or beneficial registrants to consent to further uses of their registration data would solve the debate over the privacy of registration data made accessible through WHOIS. What are your views on the use of consent in this context?

Consent needs to be unambiguous, free, informed and specific.
Consent is not a waiver for disproportionate or unlawful processing. If the purpose cannot be achieved through consent, that legal ground simply cannot be valid. Moreover consent can be overly burdensome (you have to register and prove the consent for each of the purposes and data processing). It does not solve the problem of proportionality. Also, it should be underlined that you cannot consent to something which is unlawful.

Jurisdiction

12. Can you explain to us how the data commissioners factor in the European Charter of Rights (or, for that matter, local or supra-national fundamental rights instruments in the case of countries outside Europe) in the assessment of data protection issues? Is this matter within their jurisdiction?

There is UDHR + PSRC + Convention 108 + OECD guidelines + APEC privacy guidelines + 120 national data protection laws around the globe which are based on similar principles. ECR is not enforceable per se outside of Europe unless bilateral agreement foresees differently, ex: Privacy Shield

13. In view of the borderless nature of the internet and the fact that European Union citizens may freely acquire domain names from registries and registrars in third countries, how could potential conflicts of law based on the current and future European Union data protection framework best be avoided?

One of the solutions is to develop a proper privacy policy within ICANN as global organisation which takes into account all the global and regional legal requirements.

Being said that it is to be remembered that on data relating to all natural persons in the EU the EU legislation is applicable. Enforcement is on bilateral agreements which exist with some countries, with others it is on the way.

The General Data Protection Regulation is directly applicable law as well on all data controllers worldwide that systematically process personal data of Europeans. It is not relevant where (in what geography) the data are processed. The mandatory inclusion of

personal data of people in the EU in the WHOIS-register is processing of personal data that falls within the scope of the GDPR.

14. Can the EU enforce provisions of the General Data Protection Regulation on ICANN itself, or just the EU Registrars and EU Registries? Will there be such enforcement?

The reply to your question should be based on the assessment and identification of the controller. It is likely that ICANN has the decision-making power concerning the purposes and means of the processing for the top level domains. ICANN also has control over the processing methods, the choice of data to be processed and who is allowed to access the WHOIS for top level domains. With regard to ccTLD's, ICANN should assess whether the national registries are the data controllers, or joint controllers with ICANN, and possibly, joint controllers with the registrars for the ccTLD WHOIS.

Compliance with Applicable Laws

15. Article 6 of the General Data Protection Regulation provides that processing is lawful if, among other things, the processing is "necessary to protect the vital interests of . . . another natural person or for the legitimate interests pursued by . . . a third party." Under these principles, and given the longstanding and historical use of registration data made available through WHOIS as a de-facto public resource, do you agree this information should continue to be made readily available to those who investigate fraud, consumer deception, intellectual property violations, or other violations of law?

No. You mention two of the six legal grounds. The legal ground of 'vital interest' is reserved for critical life-saving circumstances, and can never be invoked for a general publication of personal data. *De facto* practice cannot be considered as the legal basis for data processing and the fact that the DPA's have not yet taken enforcement action to date does not mean the policy, and practice, should not change. In fact many DPA's have worked with national registries to limit availability of the ccTLD's.

16. Our working group deals with policies pertaining to generic top-level domains (gTLDs). However, each country establishes its own policies pertaining to country-code top-level domains (ccTLDs). Currently, all EU states have ccTLD registries which provide publicly available registration data through WHOIS, both for private individuals and commercial entities. Can you explain how these ccTLD registry policies are able to comply with EU data protection laws?

In the same manner as for gTLDs registration: by reviewing the current practice.

17. The gTLD ecosystem includes the Generic Names Supporting Organization which recommends policy, ICANN which implements that policy, registries which administer the

domain name space under a given gTLD, and registrars which register domain names for use by registrants. Within this ecosystem, who do you see as the data controller, in terms of the EU definitions of data controller and data processors?

ICANN.

_

Consumer Protection

18. Can you comment on your understanding of the need for owners of trademarks/brands and IP to avoid and combat infringement, and this need's connection to consumer protection, in the context of the EU ePrivacy Directive and the General Data Protection Regulation?

Consumer protection is only one of many public interest issues. It is our understanding that, generally speaking, brand owners take action to protect their brands and ensure maximum market access and minimal consumer confusion. It is not clear what this has to do with data protection. Protecting consumers from the actions of fraudulent actors depends on the specific nature of the fraudulent activity. Protecting a social media participant from having their personal information stolen from a fake social media site that has been registered to a criminal, is very different in terms of data protection proportionality assessment than, for instance, protecting the potential future purchaser of a fake GUCCI bag (that she knows is a fake) sold on a website that is not attempting to pretend it is anything but a site that sells fake GUCCI bags…..

19. Today, intellectual property and trademark rights holders depend on registration data obtained through the WHOIS directory service to police the misuse of their intellectual property on commercial websites, track down purveyors of counterfeit goods, and prevent fraudulent websites from engaging in illegal activity on the Internet. Is creating a repository of information for contactability to facilitate reaching those business registrants a valid purpose for this directory service and, if not, why not?

***De facto* practice cannot be considered as legal basis for data protection. It is not true that this is the only way such legitimate aims can be pursued, this is simply the way the actors mentioned in the question are accustomed to solve problems. There should be mechanisms put in place which disclose the least data possible, providing avenues of redress through which conflicts can be handled. ICANN has not updated the sophistication of its WHOIS database; meanwhile the Internet has developed many very sophisticated systems to do a host of different tasks useful to e-commerce. The fact that this may cost money is not a reason to remain in the past.**