ICANN Org Legal/Natural Persons Differentiation Study

Overview and Q&A

Karen Lentz, VP, Policy Research & Stakeholder Programs
Jared Erwin, Sr. Manager, Policy Research & Stakeholder Programs
Isabelle **Colas-Adeshina**, Policy Research Specialist, Policy Research & Stakeholder Programs

26 January 2021

Agenda

- Overview of study (15 min)

- Responses/Discussion on submitted questions (45 min)

- Q&A (30 min)

Overview of Study

EPDP Team Request & Consultation

◉ **Request**: The EPDP Team recommends that as soon as possible ICANN Org undertake a study, for which the terms of reference are developed in consultation with the community, that considers:

  ○ The feasibility and costs including both implementation and potential liability costs of differentiating between legal and natural persons;

  ○ Examples of industries or other organizations that have successfully differentiated between legal and natural persons;

  ○ Privacy risks to registered name holders of differentiating between legal and natural persons; and,

  ○ Other potential risks (if any) to registrars and registries of not differentiating.

◉ **Consultation**: At ICANN66, ICANN org and EPDP Team determined that study would examine effects of differentiation between legal and natural persons on various stakeholders: registries, registrars, registrants, and end-users

Research Questions

◉ Study looks at five key variables: cost, risk, cost-risk mitigation, benefits, and feasibility

◉ The following research questions guided the study:

○ What are the potential risks and costs of differentiation to Contracted Parties, registrants, and end-users?

○ What factors work to mitigate those risks and costs?

○ What are the benefits of differentiation?

○ How do mitigation factors and the benefits of differentiation impact the risks and costs of differentiation?

○ What factors explain the relative feasibility of differentiation for each party?

Report Scope & Content

◉ Report provides:
  ○ Introduction to differentiation from a legal and policy perspective.

  ○ Problems and prospects related to the stakeholders, framed in terms of cost, risk, cost-risk mitigation, and benefits.

  ○ Examples of differentiation in and outside the DNS ecosystem.

  ○ Analysis based on questionnaire sent to EPDP team and circulated amongst ICANN community.

  ○ A model/framework to help EPDP Team assess overall feasibility of implementing a differentiation method.

◉ Report **does not** provide recommendations or normative assessments of differentiation.

Questionnaire Overview

- ICANN circulated a questionnaire to: Contracted Parties, Natural Person Registrants, Legal Person Registrants, RDDS end-users, and ccTLD Community.

- Received 247 responses: 47% identified as Legal Person Registrants, 30% as RDDS end-user, 14% as Contracted Party; natural person registrants & ccTLD operators made up remaining responses.

- Comprised 6 questions:
  - Why does your organization differentiate?
  - What methods does your organization use?
  - Why does your organization not differentiate?
  - Has your organization's home jurisdiction impacted a decision to differentiate?
  - What are the perceived main benefits associated with differentiation?
  - What are the perceived risks and costs associated with differentiation?

- Responses are included throughout the report to help inform the model presented in the paper.

Examples of Questionnaire Responses

- ◉ Why does your organization differentiate?
  - ○ Because of data protection law requirements.
  - ○ Differentiation provides opportunities such as trademark enforcement, gaining access to data, and being able to contact owners for domain names.

- ◉ What methods does your organization use?
  - ○ Dependent on the organization field to identify if a person is registering a domain as a legal or natural person.
    - ■ If a registrant fills in the organization field it is assumed that they are a legal entity and
    - ■ If the field is left blank it is assumed that they are a natural person.

- ◉ Why does your organization not differentiate?
  - ○ The complexity behind the financial and technical feasibility in implementing such a business model was not worth the investments.
  - ○ A uniform approach was the safest to mitigate liabilities, legal risks, and opportunities for registrants to provide incorrect data.

Examples of Questionnaire Responses

◉ Has your organization's home jurisdiction impacted a decision to differentiate?
  ○ Those who do not differentiate noted that jurisdictional laws did not impact their decision.
  ○ Those who do differentiate noted that GDPR is viewed as the governing jurisdiction law which required them to differentiate between legal and natural persons.

◉ What are the perceived main benefits associated with differentiation?
  ○ Differentiation provides security, authenticity, and transparency of the domain owner or commercial entity, which creates consumer trust.
  ○ Differentiation provides access to an increased amount of information which is useful for third parties such as law enforcement agencies.

◉ What are the perceived risks and costs associated with differentiation?
  ○ The main perceived risks and costs associated with differentiation were the financial burdens associated with implementing a business model that would allow for differentiation and the risk of personal information accidentally being exposed.

Model - Feasibility Assessment Heat Map Template

◉ The table below is the "Feasibility Assessment Heat Map"; factors constituting each of the variables are derived from the research presented in the report

$$[\text{Risk } (-R) + \text{Cost } (-C)] + [\text{Mitigation } (M) + \text{Benefits } (B)] = \text{Feasibility Value } (FV)$$

	Risks	Costs	Mitigation	Benefits	FV
Contracted Parties	[Risk factors listed here]	[Cost factors listed here]	[Mitigation factors listed here]	[Benefit factors listed here.]	(-4 thru +4)
Natural Person Registrants	[Risk factors listed here]	[Cost factors listed here]	[Green shaded boxes assigned +1 feasibility point]	[Benefit factors listed here.]	(-4 thru +4)
Legal Person Registrants	[Risk factors listed here]	[Cost factors listed here]	[Mitigation factors listed here]	[Red shaded boxes assigned -1 feasibility point]	(-4 thru +4)
RDDS End-Users	[Risk factors listed here]	[Orange shaded boxes assigned 0 feasibility points]	[Mitigation factors listed here]	[Benefit factors listed here.]	-(-4 thru +4)

Model Example - Differentiation Through Registrant Self-Identification

- Example: differentiation costs/risks outweigh mitigation efforts/benefits, i.e., "infeasible"

Scenario 1 (Registrant Self-Identification): Feasibility Assessment Heat Map

$$[Risk\ (-R) + Cost\ (-C)] + [Mitigation\ (M) + Benefits\ (B)] = Feasibility\ Value\ (FV)$$

	Risks	Costs	Mitigation	Benefits	FV
Contracted Parties	Natural person registrant mis-identifies as a legal person; personal RDDS data flagged for availability in public RDDS (p. 20)	Liability depending on severity of violation (p. 12)	Verify registrant designation [neutral value assigned as verification is a cost as well as mitigation measure] (p. 31)	N/A compared to *Scenario 0*	-2
Natural Person Registrants	May mis-identify as legal persons; personal RDDS data flagged for availability in public RDDS (p. 20)	Privacy (p. 23)	N/A	N/A	-2
Legal Person Registrants	Identifies as a legal person and provides personal data of associates during registration without their consent (e.g in *Admin* and *Tech* fields) (p. 21)	Liability depending on severity of violation (p. 12)	Obtain consent from relevant associates to share personal data as part of registration OR provide generic contact information (e.g. *admin@company.example*) (p. 28)	Improves reachability [neutral value assigned as some legal person registrants do not want their data publicly available in RDDS] (p. 24)	-1
RDDS End-Users	May inadvertently process personal data as a result of incorrect self-identification (p. 20)	Liability depending on severity of violation (p. 12)	Apply technical methods to identify and remove personal data from any RDDS data obtained [neutral value assigned as these methods impose costs] (p. 45)	More RDDS data available as a result of RDDS data differentiation (p. 42)	-1

Key Points

- Differentiation would redistribute risks and costs associated with processing RDDS data.

- Differentiation between personal and non-personal data in RDDS could maximize the availability of registration data.

- However, given the imbalance of burden and benefit of differentiation as a practical matter, it is unlikely that a global policy to differentiate could ever reach a state that all viewed as "ideal". Some parties will bear risk and costs and others will enjoy benefits.

- Policy decision to determine balance of these factors and relative merits of differentiation.

Response to Submitted Questions

Question 3

◉ **Question**: The ICANN org study mentions that "contracted parties bear many of the costs and risks" or "face uncertain risks and costs". Are the authors of the study of the opinion that ICANN org does not face any risks associated with the differentiation? If so, what motivated that assumption? (ISPCP – p.5, 63)

◉ **ICANN org response**: As determined in consultation with the community/EPDP team, the study is intended to look at the effects of differentiation on various stakeholders, including contracted parties, registrants, and end-users. It is not a study of the risks/costs to ICANN org. In a scenario where differentiation is a policy requirement, the study finds that the contracted parties would likely bear the burden of risks/costs.

Question 4

- **Question**: Please have study authors explain/discuss Differentiation Scenario Model contained at end of study, especially how burden/benefit values calculated. (GAC – p. 58-79)

- **ICANN org response**: Values are assigned regardless of the type of risk/cost/benefit/mitigation effort, e.g., any factor having a positive effect on a stakeholder gets a score of +1.
  - Additionally, p.9 of the study states:
    - "As these variables are not amenable to quantitative measurement, the relationship between them cannot be rigorously tested without an expanded effort. To the extent they can be measured at all, they are presented in the model provided below as qualitative variables with relative weights. **These weights are derived from a review of legal analyses and academic research presented in the first sections of the report, as well as the results of a questionnaire on differentiation circulated amongst the EPDP Team and ICANN Community.**"

Question 5

◉ **Question**: EDPB in 7/5/2018 letter advises that Registrants shouldn't provide PI of others for admin/tech contacts and clarifying this in future Temp Spec updates (GAC – p. 28-29)

◉ **ICANN org response**: ICANN org requesting further clarification of this question.

Question 6

◉ **Question**: Data Processing Impact Statement: how could this mitigate risks? Consider scenario where engaged in clear messaging or verification along with explanation of consequences, confirmation and easy right to correct -- when assessed wouldn't that translate to low risk? (GAC – p. 29)

◉ **ICANN org response**: The Data Processing Impact Assessment (DPIA) is one example of a risk-mitigation tool mentioned in the report. It provides a way for contracted parties to record any precautionary measures they have taken to mitigate potential issues.

Question 7

◉ **Question**: Reference to how to design consent messages ("consent engineering"). Any research on how ccTLDs and others do this? No need to reinvent wheel. EU ccTLDs are used to GDPR compliance. Issue of consent analogous to Natural/Legal designation. (GAC – p.30)

◉ **ICANN org response**: While this study did not look at "consent engineering" of ccTLDs, ICANN org notes that Bird & Bird provided in their 13 March 2020 memo guidance on options for obtaining consent. Further study can be conducted regarding this topic upon EPDP Team request.

Question 8

- ◉ **Question**: Any more data gathered from respondents who differentiated about why they perceived differentiation as a low/medium (rather than high) effort? Interesting observations that those who d/n actually differentiate perceive the highest effort for doing so. (GAC – p.42)

- ◉ **ICANN org response**: ICANN org notes from responses to the questionnaire that:
  - ○ Reasons for perception of differentiation as a high effort:
    - ■ Participants shared a mutual concern that the concept of legal and natural person is likely foreign to most human beings. This increases the possibility of accidentally exposing personal information due to natural or legal entities being improperly inputted or identified.
    - ■ The above concern also led participants to feel the technical feasibility and the risk associated with differentiating between legal and natural persons provided little return of investment.
  - ○ Reasons for perception of differentiation as a low effort:
    - ■ No additional insight beyond what is provided in the report.

Question 9

- ◉ **Question**: RIPE NCC which serves EU publishes all contacts details regardless of natural/legal status b/c necessary for performance registry function and smooth operation of internet globally -- identifies this "defensible legal purpose"; why wouldn't publication of least legal registrant contact info fall under these defensible legal purposes too? Perhaps further legal advice? Also note reference to French ccTLD who publishes data of legal registrants and considers it consistent with GDPR (p.46). (GAC – p.50)

- ◉ **ICANN org response**: ICANN org requests further clarification of this question as it does not appear to be a question for ICANN org but rather is a request for additional legal advice.

Question 10

- ◉ **Question**: SSAC has previously noted important deficiencies in the ICANN study "Differentiation between Legal and Natural Persons in Domain Name Registration Data Directory Services (RDDS)". Those deficiencies need to be cured. As stated in SAC112: "The research report did not look at some of the most relevant and obvious examples, such as how and why natural and legal person data is collected and published in real estate registries, company registries, and trademark registries inside the EU; and how such registries outside the EU handle the data of subjects who reside in the EU. While the report stated that 'most EU ccTLD operators continue to publish some (and sometimes all) contact data fields for domains registered by legal persons,' the report did not provide the details, such as a list of which ccTLDs publish what data." (SSAC)

- ◉ **ICANN org response**:
  - ○ ICANN org chose the examples it saw as most relevant/pertinent. However, ICANN org can look into the suggested examples for insight into potential differentiation methods.
  - ○ The statement re: EU ccTLD operators is a reference to SAC101v2 and an article "How all 33 European ccTLDs are Handling GDPR" referenced/linked to in the study (footnote 77).

Question 11

Question: In the Feasibility Assessment Heat Map of Scenario 0 (No Differentiation), why is 'less legal risk' not considered as 'benefit' for Contracted Parties? (NCSG- p. 71-72)

ICANN org Response: In general, the risks, costs, and benefits specified were those identified in responses to the questionnaire. The model is intended as a tool for analysis of different scenarios, rather than a definitive calculation of benefits. Accordingly, this variable could be increased to account for reduced legal risk for the contracted parties as a benefit.

Q&A

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: email

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg