Comments on GDPR Interim Compliance Models for WHOIS
& Associated Privacy Compliance Issues

Stephanie Perrin

I would like to take this opportunity to thank ICANN for its transparency in how it is handling GDPR compliance, and for giving us this opportunity to comment on the three proposed models. While I represent the Non-Commercial Stakeholders Group (NCSG) in many WHOIS Policy Development Processes and committees, I am submitting these comments in my own name as I have reservations about all three options as presented by ICANN, although I occasionally say "us" as a representative of NCSG. Of the three models presented, the NCSG appears to be in support of Option 3, as it expresses well our long held positions.

I will also take the liberty of commenting later on a rather fuller basket of data protection issues, because we understand that these are interim measures. We do not wish to lose this opportunity to suggest more complete responses to the problem of overcoming gaps in data protection at ICANN. Furthermore, I do hope that by adding to this document to make it more comprehensive in scope, we can help avoid the confusion that newcomers to our own stakeholder group face as they try to understand this rather complex state of affairs in which ICANN finds itself.

Executive Summary

The short answer to the Goldilocks challenge with which ICANN has presented us, is that of the three models, none are perfect. I prefer Model 2b. It is still not quite right however, and I would like to express my endorsement of the ECO model, which is much better. I would also like to note our appreciation of their workbook, which I find to be a very useful document, and a thorough and accurate legal analysis. I have explained my reasons for this choice, and the rationale for rejection of each of the ICANN proposed models in section I.

In section II, I have reviewed in detail some of the models received as of January 22, 2018. I have also reviewed the comments received to date.

In section III, which will be added in a separate submission, I propose to provide comments on the questions posed to Hamilton, and the legal advice received, including that which has been offered from stakeholders. In this section you will find some proposed questions that have not yet been posed to legal counsel, to the best of our knowledge. We understand that further analysis will continue after the interim measures have been adopted.

In that light, I will provide in the same document section IV, an exploration of some of the issues which we feel the focus on GDPR compliance, in the particular context of data disclosure and retention, has left relatively unaddressed, or which we wish to emphasize. Examples of these issues include:

- ICANN is the principal data controller here. Because the community has no input to the Registrar Accreditation Agreements (RAA) and are not a party to the contract, the responsibility for WHOIS policy rests clearly on the shoulders of ICANN and not the community. The prevailing rhetoric surrounding the "picket fence" that keeps the community out of these negotiations and supports claims that the contract is not a policy instrument is unsupportable. Absent an RDS policy, and we see no signs of one emerging soon, the contract is the policy instrument, and it appears that the US government set the policy.
- The determination of who gets access to personal information is a key policy issue, and failure to figure out how to accredit those who get access has held up the development of tiered access. I do not believe that self-accreditation is an acceptable option under any circumstances, and demand a more rigorous, standards-based process where independent audit is possible. I draw to your attention the fact that the right to have data protection overseen by an independent data protection authority is a right in Europe, guaranteed by section 8(3) of the European Charter of Fundamental Rights. Accepting self-accreditation from those who want access to the data is putting the foxes in charge of safety of the chicken house. I include proposals for interim measures in section I of this document. One of my principal objections to Model 3 is that it dumps the problem of figuring out who should get access to data on a disclosure basis on the contracted parties. This is not transparent, from an end-user point of view, and may result in either loose practices in disclosure, or a logjam in access for legitimate actors.
- We remind everyone regularly that there are now 120 data protection laws in place around the world. While few of them have fines of 4% of annual global turnover like the GDPR does, it would be cynical of ICANN to only move on compliance where there are aggressive enforcement measures in place. Furthermore, such an action exposes contracted parties to continued risk. The current WHOIS conflicts with law policy (or more accurately, procedure) is a failure across many factors, we simply need a privacy policy that harmonizes to the highest level now. This is the only sensible, cost effective way to deal with varying data protection laws in a global environment. Countries that insist on non-compliance with data protection best practice should be accommodated exceptionally, and be required to request access to personal data in compliance with fundamental human rights. In other words, the WHOIS conflicts with law policy needs to be stood on its head, and become the RDS conflicts with privacy policy instrument or procedure.

I hope that my comments are useful and will be taken as seriously as other comments in the community are. End-users deserve to have their rights upheld and their perspectives represented at ICANN.

Section I Comments on the ICANN Models

The three models clearly follow the Goldilocks principle; Model 1 is too much like the status quo and clearly does not accord with the Hamilton advice received, Model 2 is better (although still not fully compliant with the GDPR), and Model 3 is interesting from a data protection perspective but very difficult to put into place. I certainly support my colleagues who are endorsing this proposal as being at least in principal good from an end-user rights enforcement perspective.

The approach in this document to evaluating what to do at present, given the predicament that ICANN and its fellow data controllers find themselves to be in, is based on the principles one follows in performing a risk assessment. I also base my comments on the advice that we have given ICANN over the past 18 years, the visits we have arranged from data commissioners, and the lengthy correspondence and opinions that the data commissioners have provided to assist ICANN in meeting its obligations. Once again, my comments do not necessarily reflect an NCSG agreed perspective, but I do rely on well-known NCSG positions previously articulated.

Here then are some of the key risks I see in this project:

1. Lack of preparedness to meet data protection requirements

    a. There are 100 days left to reach compliance, at the time of writing.
    b. Registrars have complex systems to reconfigure. Last summer they said they needed models by September.
    c. The focus of ICANN has always been on the publication instrument and the needs of third-party users… not the registrants, and not the responsibilities of the co-controllers of the personal data.
    d. There are other instruments that handle data which have not received much focus at ICANN (e.g. zone files, the escrow data and the contracts that govern the agents etc.). These instruments or data collections also have to meet GDPR on May 25. Simply toggling the length of time that registrars are required to retain data after their needs have been served (as we see in the models) does not really address the data protection requirements beyond the WHOIS interface. I agree with the analysis in the ECO documents, but do not agree that these issues can be neglected for very long. This is a big risk, particularly if parties wishing to access data turn to the zone files or other mechanisms when the WHOIS interface goes dark.
    e. Unfortunately, there is a long and rather fractious history of ICANN not responding to requests for compliance from the DPAs.
    f. The only mechanisms that ICANN can point to as demonstrating compliance with law at the moment are the WHOIS Conflicts with Law Policy, (which is in reality a flawed procedure not a policy), and the Registrar Accreditation Agreements, which require a forced consent for collection, mandatory enabling of bulk access for value added

service providers, and mandatory publication of personal data. This does not demonstrate best efforts in our view.

g. ICANN now has a data protection officer, but it is not clear to us that there has been staff training in privacy, expansion in the Compliance Branch to include compliance activities required in matters of data protection, data access procedures and complaints mechanisms, etc.

2. Cost allocations

We recognize that some of the key original stimuli prompting the establishment of ICANN was a desire to open up the market, facilitate sharing of the business of domain name registration, enable competition etc. It is obvious that many of the trade-offs made over registration data were motivated by dominant players not wishing to pay for access to the data (thus an open WHOIS), registrars not wishing to pay to protect the data from disclosure (thus paid proxy services), bulk data access required to be provided at market rates (thus a requirement in the 2013 RAA that data be sold at reasonable rates, despite data protection law that might apply). Disruption of this information ecosystem is prompted by very real prospects of fines for data controllers, including value added service providers who have gained bulk access to date, so once again money is the driver, not policy considerations related to rights and responsibilities. There is no budget for data protection compliance in the current ICANN budget documents, and it is not clear at all who will pay for changes, notably tiered access models. In this category, then, we have questions about how change is going to take place over the following cost issues:

a. Closing the open system will mean higher costs for contracted parties, as they will have to deal with requests for data arriving in small numbers (not blanket access).
b. Can registrars continue to charge for proxy services when the GDPR gives rights to privacy?
c. Information aggregators have been getting bulk data at minimal or no cost; if they qualify for continued access to this data will they be able to access the data for free, and will they be able to resell the data at current rates to all current customers? The European Data Protection Supervisor (EDPS) has noted that this group will be subject to the GDPR as data controllers as well.
d. Various mandatory provisions for user rights will have cost implications: consent mechanisms including providing sufficient information to make the consent an informed consent, withdrawal of consent, right to be forgotten and erasure (throughout ecosystem), access to information, rectification rights, etc.
e. Current escrow provider and transborder data flow issues, to the best of my knowledge, have not yet been satisfactorily resolved between registrars and ICANN.

f. Tiered access models, which I support, have cost implications for accreditation and authentication, not to mention building the systems and automating second tier access to the extent possible. The question of who is going to absorb each of the new costs has not, to the best of our knowledge, been answered.
g. Given the possibility of Court challenges, there needs to be a contingency budget for ICANN's costs, including the possibility that if contracted parties cannot reach compliance and are fined, they sue ICANN as Controller.

Costs will be passed on to the end-user… what does this mean for ICANN's revenue stream, and for the viability of the DNS for the average individual? Will this result in further consolidation of the registrars' market?

3. Communications risks

Given that ICANN has survived with a non-compliant approach to data protection for so many years, it seems unlikely that community members will take this risk seriously. Nevertheless, there are communications risks, particularly given the state of unreadiness.

a. A finding of non-compliance, particularly if accompanied by severe criticism and fines, may be described as a failure in accountability on the part of ICANN. This needs to be effectively countered. Good luck. The Non-Commercial Users Constituency (NCUC) has been pointing out the state of non-compliance since its formation, and had a major effort in 2003 summarizing the views of the data protection commissioners, including the 2003 Article 29 Working Party Opinion which points out the non-compliance.
b. Data breaches need to be informed to the relevant data protection authority in 72 hours. Failure to do so could have serious implications. There needs to be explicit agreement among processors and controllers about shared and separate liability (see the ECO Playbook for a discussion of these requirements).
c. Failure to reach agreement among community members about measures, both interim and long term, may escalate and have serious implications for the viability of the multi-stakeholder model.

Legal and policy risks I will describe below in the detailed commentary on the models. As mentioned previously, I endorse the analysis in the ECO documents as being the most thorough which has been presented to date, and I am not going to repeat the arguments as I agree with almost all of their conclusions.

Approach

In the section on approach, item 2, it is stated that the goal is to maintain the existing WHOIS to the greatest extent possible. **We in the NCSG think the WHOIS has been broken for some years, and do not wish to maintain it.**

In item 3, while we recognize that ICANN's Bylaws have continued to consider compliance with privacy laws an exception to the policy of full disclosure, we now have data protection laws in most countries. It is time to harmonize in favour of compliance, not regard it as an exception.

Item 4 says ICANN acknowledges that contracted parties must comply with all applicable laws. What about ICANN? ICANN is a data controller, does it not also have to comply with all applicable laws? How dare it set policy in such a way as to obstruct its contracted parties in their efforts to comply with law? How can it continue to obstruct end-user rights? Bear in mind also that ICANN is a party to the escrow contracts, it has access to data therein, and all aspects of the escrow obligations must be in compliance with the GDPR (and other laws) including transborder dataflow. This is not the registrars' responsibility, it is ICANN's issue. In this respect the registrars are in my view acting as data processors for ICANN's purposes. I note the thorough discussion of this in the ECO paper.

In item 5, I note again that the approach to data protection compliance, and the pursuit of an overarching purpose of data processing, starts with a collection of use cases (user stories). ICANN creates policy and contractual compliance models for managing the DNS, it should start there to find its purpose for data collection, not with a canvassing of third parties as to who wants the data and for what myriad purposes. This is absolutely backwards. Data minimization is the key, not data exploitation, no matter how useful third parties find the information that is gathered for the purpose of domain name registration.

Commonalities across all models

Data elements
The current RDS PDP may decide that there is too much data collected. It seems unnecessary to try to determine data elements that cannot be justified at this point, given the urgency, but current thick data sets may be excessive.

Performance of a contract
I appreciate that performance of a contract is a legitimate reason to collect, use and disclose data. However that contract is supposed to be guided by a defensible policy, which ICANN lacks. Current contracts cannot be assumed to be at all compliant and will have to be revised. This provision also, as the Article 29 Working Party recently pointed out, relates to contracts where the data subject is a party. It would not help with the privacy infringing provisions of the current RAA, which are then carried through to the contracts between the registrars, resellers and their

customers. Provisions that originate with ICANN as data controller in a co-control relationship with registrars and registries through their contracts need to be reviewed.

Consent
Section 5 seems to be quite wrong. We do not agree that registrars **must** request that users consent to the full disclosure of thick WHOIS data. First of all, the ICANN community is at the moment trying to avoid the deletion of data elements because of time constraints, but we are confident that full disclosure of thick data does not comply with the GDPR. Secondly, consent is a very precarious basis for processing for a number of reasons (which are enumerated in the ECO document, I will not repeat them all here). It is almost impossible to ensure that the consent is informed, in such a complex global environment. Secondly, management of consent options (collect this, don't collect that, display this, don't display that, withdrawal of consent, etc.) is expensive, time consuming, and complex given the variety in relevant law. Assume a scenario where a registrar in a non-EU state, but which has a very different data protection law, is seeking consent from an EU customer. Both laws apply. This is very messy and is potentially expensive, which is why companies always try to harmonize their global policies in ways that ensure they achieve a high level of compliance. In this instance, that means the GDPR, but engines can surely be built that could factor in other relevant national law if required.

Transfers
Care must be taken to ensure that the rights (and the data) of the registrant are protected throughout the transfer process. This is particularly true for privacy/proxy customers. I like the concept of authorization codes which ECO proposes, but need to understand how it would work.

File Access and Notifications
Section 7 should note that the rather vestigial rights of correction of data (more like obligations with respect to accuracy) include rights of access and deletion.

Purpose
There has been an interminable discussion on purpose at ICANN, particularly in the current RDS PDP. I propose that you use the purpose that was agreed by the GNSO, by a supermajority vote, in 2006. It is basic and within ICANN's remit:

> 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.

The current RDS PDP has wrangled endlessly on the purpose of the registration data service, often conflating the purpose of the overall processing of data with the uses of the public disclosure instrument, the current WHOIS. It is evident that progress

towards a common understanding of what exactly the data protection community understands by the term is glacially slow, and demonstrates a failure in the multi-stakeholder process. "Purpose of processing" certainly does not mean that every possible use of every possible disclosure to third parties serves to justify the collection, use and disclosure of information that is superfluous to what is required to register a domain name and put it into secure and stable operation.

We understand that the law enforcement community has demanded easy access to personal data for many years, but this flies in the face of data protection law. The fact that WHOIS has been open, and has facilitated bulk access to this data for other purposes including tools used by law enforcement and private sector security practitioners does not mean the situation has to continue thus. While it is reasonable to take some measures in processing to support combatting fraud, guarding against security risks including phishing, pharming, and malware distribution, the purpose of the RDS cannot be retuned to read, "for the purposes of investigation of crime and Internet abuse". ICANN is not a law enforcement agency.

Subject to this caveat, I agree that the five explanatory points listed on page 6 would indeed be desirable. Considerable refinement and definitions are required to enable this.

The Models

We understand that the models are not presented as 3 options to be taken intact, but rather as models with various details that could be mixed and matched. I will therefore comment on aspects of each one.

Model 1

Model 1 has various territorial or jurisdictional considerations. I would suggest that harmonizing and having all registration data follow the same policy is the cheapest and easiest way to implement the GDPR. Forget trying to decide where someone resides, or whether the data is transiting Europe for processing. Simply protect it.

The minimum dataset in Model 1 is not minimal enough. We believe, and we would cite numerous communications from the data commissioners, including the Article 29 Working Party 2003 Opinion, that name and postal address are personal information, and it is not necessary to release either element. To access data not published, I believe strongly that third parties must be accredited and authorized. Requests must be limited and specific, and be recorded. I do not believe that self-certification is acceptable, and believe that professional standards must be developed under some kind of quality standards system. Such a standard would both define a professional code of conduct for the categories of the accredited requestors, but it would also set standards for the treatment and protection of personal information that has been released to them. One-off requests, e.g. a consumer complaining about a harassing email or website, would be processed in a

separate stream, as they would be assessed in a more labour-intensive way. Clearly the goal in an accreditation and authorization scheme is to automate access for routine, regular requestors. This does not mean wide open access for current users; it means accountability on all sides.

Model 2

Model 2 is an improvement on Model 1, but my jurisdictional comments remain… treat all registrants the same. We agree that not differentiating between whether a registrant is an individual or a legal person is important, for reasons which were well ventilated during the recent Privacy Proxy Services Accreditation Issues PDP. Legal persons are completely at liberty to release and publish their information, assuming they fulfilled their obligations under the GDPR, and if they wish to have additional fields that serve their security needs, that should be examined in the RDS PDP and accommodated if possible. However, the rules for registration data processing must not be set according to the wishes/needs of large corporations.

I would offer qualified support for Model 2b, although the ECO model is preferable. I repeat the caution on the use of consent for optional release of personal information: the costs of managing the consent of individuals is high, and it is impossible to ensure that individuals are truly aware of how far their data is going to travel, or how it will be combined and sold. As indicated in Model 1, I support a full standards development process to develop professional standards for parties who wish to have routine access to tiered data.

In terms of input on how to move forward on an accreditation scheme for tiered access, I offer the following ideas. A standards development process would require the gathering of volunteers who are willing to support it, and the collection of instruments which are currently in use in a voluntary way, among the various users of personal data (e.g. APWG, legal practitioners). I would propose a workshop on this topic at the annual general meeting in Barcelona to discuss how this could be achieved. In the meantime, a draft policy for those receiving data could be developed, including the requirement that they make an undertaking that they would abide by the GDPR and some off-the-shelf privacy standards (e.g. CAN/CSA-Q830, available ISO IT security standards, and others which the SSAC might help in suggesting. These parties would make specific undertakings to not release the information further unless the recipient is a signatory to the same undertakings.

The issue of the future of value added service providers whose business depends on data aggregation and analysis has arisen in some of the GDPR discussion at ICANN. Those businesses need to consider options for using personal data. Many kinds of analytics can be done on anonymized data, identifiers can be replaced, etc. The situation cannot continue as it is today.

Model 3

Model 3 appears very attractive at first glance. It responds to long held views in the NCSG, including the following:

- It is harmonized globally
- It appears to not make a distinction between individuals and legal persons, although I find it rather unclear
- It calls for third party access only with legal authority, and due process
- It decreases the data retention period to 60 days

I am concerned by the following statement: "This Model would appear to require a registration-by-registration, field-by-field assessment about whether personal data is included". This is a huge burden to place on contracted parties to sort out. A workable solution that is not going to drive up costs for contracted parties and thus end-users has to scale, in my view. Harmonizing to the highest standard would solve this problem and I find it odd that this option is not included here.

My second concern relates to access by law enforcement officials, private sector cyber-security professionals, and intellectual property abuse investigators. For greater clarity, here is the relevant section:

> To access registration data not published in the public WHOIS registries and registrars would only grant access to third-party request or when required by applicable law and subject to due process requirements, such as when the third-party requestor provides a subpoena or any other order from a court. or other judicial tribunal of competent jurisdiction for access to non-public WHOIS data.

Clearly, the NCUC and NCSG has been calling for this respect for the rule of law for many years. However, the reality is that cybersecurity enforcement is done mostly by private sector actors without delegated legal authority in many cases. Intellectual property investigators are similarly acting for themselves (or their clients) without formal law enforcement authority. This will therefore cause a major disruption in the ecosystem and put considerable pressure on contracted parties to comply with their requests. I am not suggesting for a moment that the status quo is acceptable, far from it. However, this is our opportunity to explore workable models, and I think Model 3 does not offer mechanisms to provide tiered access to accredited parties. Registrars and registries will have to analyze requests on a piecemeal, ad hoc basis. This in my experience usually results in bad outcomes, often non-transparent work arounds. I think we should seize this opportunity of the coming into force of the GDPR to address real issues about the accountability of third party recipients of personal data.

Because this model does not accommodate the needs of cybercrime and trademark abuse investigators sufficiently, it is my view that this would put too heavy a burden on registrars and registries, thus driving up the costs of domain names in an unacceptable manner. I note however that one of the NCSG's members, the Electronic Frontiers Foundation, has already submitted separate comments supporting this model, and their reasons for doing so we support.

The data retention for only 60 days is the best option for a data retention regime. Given that data is in escrow and thus available in an emergency, I do not support data retention beyond what is necessary for the registrar. 60 to 90 days seems reasonable.

Section II Comments on the Submitted Models

Strawman Proposal, Greg Aaron, IThreat Cyber Group

This proposal has many good aspects to recommend it. It asks the question, "Tell me how this proposal stands up to scrutiny? Is anything unworkable?, etc. Briefly:

- Consent issues cannot be left for later analysis; they are too central to the issues at hand
- Registrars and registries cannot continue to publish what they do now
- One cannot assume that companies have obtained the consent of employees to include their names in a public directory; one has to take steps to ensure they have.
- It is risky to assume that ccTLDs are compliant with the GDPR (e.g. Nominet).
- As discussed above, differentiating between citizens of the Europe Union, data that is passing through the EEC, etc. is just too complex for a workable system. The default has to be protection; corporations and organizations can opt out to publish data as they see fit.
- Under other necessary arrangements: Common language for data processing indeed could be developed… this would best be done in the privacy policy that NCSG has long recommended be developed.
- The question regarding "personally identifiable data" is, with respect, irrelevant for our purposes. There has been lengthy wrangling in the RDS PDP, due in the view of some of our active participants in that group to the tendency of US members to cling to this construction of personal information, rather than the broader definition of personal information used in EU (and many other) data protection laws. See the discussion of personal information in the ECO documents, they do a good job on this analysis. I agree that it is necessary to publish the IP address, but disagree that in the current environment, only the ISP can link it to the natural person. This is an interesting question for future research.

- While the last line "The GNSO's RDS WG closely examined the issue in 2017 and generally did not feel that any thin data fields constitute personally identifiable data" is generally accurate, representatives of the NCSG disagreed strenuously with both the use of the term "personally identifiable", as it is a red herring, and with the assertion that thin data is not personal information. Because it relates to the file of a natural person, the data is personal information. This does not of course mean it cannot be disclosed.

Coalition for Online Accountability

The Coalition for Online Accountability has submitted a proposal which in my view has many flaws. While recognizing the reality of some of the issues they raise, here are a few brief objections:

- As above, restriction to registrars located in or offering services in the EU is too narrow.
- Purpose statement is too broad, particularly with respect to the purposes of assisting law enforcement. This is outside of ICANN's remit and is disproportionate in terms of compliance with GDPR. Item 4, including combatting racism, child abuse, trafficking in human beings, is excessive.
- Other purposes as determined by ICANN (item 10) leaves this model open-ended.
- The data elements listed on page 3, A are excessive. We have already heard from data protection authorities on multiple occasions that name, address and phone number should not be published.
- Section 4 on determining the status of registrants as legal persons or individuals is simplistic. I agree with the detailed examination of this issue which is included in the ECO Playbook.
- An important paragraph appears on page 6:
  "If the Registrant does not give consent, or if the Registrant has withdrawn consent, his of her personal data will only be made available to third parties in accordance with the WHOIS Data Access Model described below." Note that this is a self-certification model, and in my view it does not meet the threshold to over-rule the consent of the individual (which has been withdrawn). Of course there are circumstances where the unlawful activity would provide a compelling reason to the registrar to divulge the requested data, but I would suggest that we need a more sophisticated model to govern disclosures.
- Item 6 (prohibited uses of WHOIS data) merely repeat restrictions in the 2013 RAA, which are not necessarily being followed at the moment. I suspect that there are many other current uses that are probably not in compliance with the GDPR, and rather than enumerate specific examples like this, it is perhaps more helpful to provide analysis of what the GDPR would prohibit.
- The data retention provision listed in 7 is also too broad. If an argument can be made for this for analytics purposes, data ought to be anonymized.

I have not commented on the details of the proposal, this discussion is limited to the Working Draft GDPR Compliant WHOIS Model labeled draft 12/21/17.

ECO Association of the Internet Industry: GDPR Domain Industry Playbook

I think that this model is so thorough and compatible with data protection law, as I understand it, that it deserves endorsement. It is far more comprehensive than ICANN's proposed models, and offers a way forward for implementation in a realistic manner. I have served at ICANN for five years now as a volunteer, first on the EWG on the new RDS (2013-2014), the PPSAI PDP, the WHOIS Conflicts with Law IAG, the new RDS PDP, and on the GNSO Council for over three years now, and this is the first time I have seen a document that thoroughly explores the application of data protection law to RDS issues and all the various dataflows. It is very welcome.

Because I am strongly in agreement with the approach, I will discuss quibbles and omissions and comments for further work more thoroughly than approvals, but here in a broad brush are the highlights of this proposal:

- Starting with data minimization is correct.
- The discussion on data risk levels (DRLs) may lose people. It perhaps needs a bit more explanation.
- I agree with characterization of consent as high risk. It is also high cost for the contracted parties to administer.
- Focus on what falls to ICANN to enforce (e.g. DRL1) and what belongs to other controllers and co-controllers to enforce is useful.
- Delineating who is a processor and who a controller is important, and has not been done prior to the ECO analysis.
- The document does not look in depth at data transfers. To the extent that ICANN either in its contracting or through consensus policy mandates data transfer, we do have to examine data transfers, in my view. For instance, data escrow is something ICANN is responsible for, and a party to. I believe that registrars are data processors with respect to these requirements. Acceptance of escrow providers in jurisdictions that would assure the data remains in compliance with GDPR is, in my view, well within scope of our deliberations and not something that registrars and registries should consider their responsibility… in this respect, the sooner that we solve the waiver process in the WHOIS Conflicts with Law Procedure, the sooner this issue will be resolved.
- The discussion of the thick registry model which appears in bold on page 19 I find rather confusing. The recommendation is not to abandon the model, yet the data elements identified for transfer tend to be thin. More explanation is needed here and in the later section on page 29.
- On page 24, ECO notes that the data retention of registrant data which is not required for domain registration and putting into active status (e.g. banking

data, customer data, billing data) cannot be demanded by ICANN. I agree. The point about liability for data breach is very important.

- I thoroughly applaud the recommendation to drop the admin, tech, and billing contact information. There are those who are endorsing an approach which starts with the EWG recommended data; obviously the additional elements recommended by that group (e.g. legal contact) go further and are worse.
- The discussion on page 26 on transfer issues is important, and underlines the rights of the end users. I would like to hear more about how authorization codes would be used here.
- Discussion of the domain name as personal data is important (p.30).
- On page 38, the group underlines that community involvement in policy development processes does not absolve ICANN of responsibility. This is important.
- On page 40. ECO notes that each controller must separately list its joint controllers in the record of processing activities. I would ask whether this covers the activities of resellers. From the perspective of end user rights, the relationships surrounding resellers, and the dataflows involving them and the accredited registrars are not at all transparent and this is not acceptable under the GDPR.
- I agree with and very much appreciate the discussion on data escrow (p.43-46).
- Part C on the discussion of the disclosure of data is very important and thoroughly analysed (53-75). Since the WHOIS has, as indicated earlier in my comments, largely been driven by third party demands for a registry that gives them access to registrant data, this is the problem that ICANN and its co-controllers must focus on. I believe this is the most thorough and accurate dissection of the legal issues and risks, and will not go through it in detail. There are two aspects of this section that I would like to discuss more thoroughly.

The first is the requirement in the GDPR for data controllers to ensure that access to personal data by public authorities, notably law enforcement authorities, must be authorized in law (p. 58-60). The criteria for developing procedures for law enforcement access are good, and will help to make this process speedy, efficient, and less expensive for contracted parties whilst safeguarding fundamental rights of the individual, and speedy access for law enforcement authorities. The Council of Europe should be encouraged to develop further any expedited processes under the Budapest Convention on Cybercrime, to the extent that this would speed up legitimate cross border requests for data. Pages 60-65 discuss the rationale for private sector requests, and reach conclusions that the cybercrime and security industry will be affected. I agree, and ICANN should in my view start an open discussion on the accreditation requirements for actors in this business. This is a known risk from the data protection perspective, and in my view all recipients of data must meet professional standards and be accredited to get access to data.

Furthermore, data analytics used by this community should be done using anonymized data to the maximum extent possible.

On page 73, ECO suggests the establishment of a Trusted Data Clearinghouse to provide a more efficient process for processing requests for data. This seems logical, even necessary, in my view. From a data protection perspective, audit is important, and a centralized approach to the issue makes this easier. High security standards are also important, and law enforcement requests may need to be securely anonymized. A central function could facilitate this, and it is one reason I supported centralized models in the 2014 Experts Working Group Report on RDS for gTLDS. This needs to be developed further, and necessary accountability mechanisms built in, and it needs to be done by the full multi-stakeholder community at ICANN.

I think the ECO report is thoughtful and tackles in a straightforward manner many of the very difficult situations ICANN and its stakeholders face with GDPR compliance. It should be supported and used as a basis for further investigation.

Conclusion

I look forward to a much richer discussion of WHOIS and privacy issues than has taken place previously, and would be happy to discuss these comments further. I will take the liberty of sending sections III and IV shortly, and apologize for missing the deadline.

Stephanie Perrin