Dissenting Report from Stephanie Perrin (24 June 2014)

It has been an honor and a privilege to serve on the EWG for the past 16 months, and I am truly impressed at the work we have done, and the spirit of consensus that has enlivened our discussions on the complex matters we were tasked to address. This has been a tremendous amount of hard work, and my colleagues have worked selflessly, with weekly calls, research and reading, and many face to face meetings. Finding the correct balance between transparency, accountability, and privacy is never easy, especially in a global context with different cultures, legal regimes, and economic power. I am very proud of what we have achieved, so it is with great reluctance that I raise issues where I cannot agree with the consensus on some aspects of this report. I feel it is my responsibility, as one who was brought on the committee to provide data protection expertise, to point out some weakness in some of the provisions that we are recommending.

The EWG report is complex, and must be read in its entirety; sometimes it is quite hard to follow how things would actually be implemented, particularly if you are a reader who is not immersed in the arcane details of domain name registrations on a daily basis. There is nothing devious in that, the matters are very detailed and deciding which order to put them in, what topics ought to be addressed in which section, is not easy. The end result, however, is that one must follow a thread through the report to determine ultimate impact. The purpose of this appendix is to follow the thread of protection of the sensitive information of the average simple domain name registrant. Whether they be an individual, small company, or small organization, we need to see what happens, and how rights, whether legislated or simply claimed on the principle of fundamental fairness in the administration of a public good, are enforced. I regret to say that I am not happy with what I find when I follow that trail. I have tried to explain how these rights ought to be implemented and enforced, to those who are more familiar with their own areas of expertise both within the EWG and in the broader community, and this appendix is added in an attempt to help further clarify these issues. I am concerned that the rights and important interests of these individuals may not be effectively protected by the inter-related provisions which we have set out.

There are three basic outcomes where I cannot agree with the consensus.

1) The requirement to have a legal contact, where address and phone number are mandatory to provide, and published outside the gate,[1] in the publically available data.
2) The default, if one is a simple registrant who does not want to hire a lawyer or other actor to assume the role of legal contact and publish their details in the RDS, to publishing registrant information, notably address and phone number in the RDS outside the gate.
3) The inclusion of a principle of consent (28), whereby a registrant may consent to the use or processing of her gated information for the permissible purposes enumerated for accredited actors behind the gate.

Let me provide some context around each of these points.

Firstly, these details appear in the section on purpose-based contacts (PBCs), which proposes a new ecosystem of validated contacts.[2] I support this, and the associated accountability mechanisms, whole-heartedly. I agree with the consensus view, that domain name registrants must be accountable for the use of the resource. Being a privacy advocate, I do not equate accountability with transparency of detailed personal or business information, I equate it with responsiveness. If a registrant fails to respond to serious issues, it is appropriate to expedite the action, depending on the issue, and contact the registrar to take action.

However, I understand the objective of our proposal of gated access to be the sheltering of customer data: the purpose of the gate is to screen out bad actors from harassing innocent registrants, deter identity theft, and ensure that only legitimate complaints arrive directly at the door of the registrants. It is also to protect the ability of registrants to express themselves. anonymously[3]. Placing all contact data outside the gate defeats certain aspects of having a gate in the first place.[4] Obviously large companies are eager to publish their contact data, as it makes it easier for them to streamline requests and manage the actions over thousands of domain names.[5] A simple registrant with a couple of domain names has entirely different needs and resources, and is unlikely to want to spend money hiring an ISP or Registrar to provide these contacts for them.[6]

I whole-heartedly applaud the emphasis we have achieved in this report on the necessity of having privacy/proxy services in the RDS ecosystem, for both individuals and organizations. I do not believe that should be the only way an individual or small organization can avoid having their private information published[7]. We have a principle that recommends providing resources[8] for registrants who are economically disadvantaged, but it is not clear how we could implement that globally, particularly in developing economies where the need is likely greatest.

An additional context, is that we propose a rules engine that enforces jurisdiction, with respect to the privacy rights of individuals who are protected by personal data protection law. This is an ambitious and potentially very useful proposal, but it only protects individuals, and occasionally legal persons in some jurisdictions, and only where data protection is in place, and would find the presence of name, address and phone number in a public directory to be in conflict with data protection law[9]. These are very important caveats. Not all data protection regimes would find, or have found, that directory information must be protected. Secondly, it is not clear enough for me how that rules engine would encode rights. Would it be based on precedents? My interpretation of the law? Your interpretation of the law? This is a difficult question and provides no certainty as to the outcome in the instances where I have cited my disagreement. A third problem with the rules engine, is that it proposes to address regimes with data

protection law only….what happens to organizations that have a constitutional right to privacy for the purposes of free speech and freedom of association, such as in the United States? Finally, is it fair to individuals in jurisdictions where their countries have not enacted data protection law? Does ICANN, in the monopoly administration of a public resource, not have a responsibility to set standards on an ethical basis, based on sound best practice?

The two remedies then, I find inadequate for the reasons cited above:

1) Hire a privacy proxy/service provider, or proxy contact, if you do not want your contact data published in the public portion of the RDS
2) The rules engine will enforce data protection rights, and place this data behind the gate.[10]

I am not confident that these will be effective as a means of allowing independent registrants to gate their name and contact information. We have indeed proposed another mitigation for this and other privacy-related problems in the privacy section. The EWG recommends that ICANN develop a privacy policy to govern the RDS. I am extremely pleased with this recommendation. It is my view, however, that it will not be a proper policy unless it governs the collection instrument, which can be found in the requirements set out in the 2013 RAA, and the escrow requirements, to be found in the same place. However, this is a magnificent step forward as far as I am concerned, and I believe once the PDP is struck to work on the policy, my arguments will be persuasive on the need to include the collection and retention instruments, as presented in the contract requirements. Once again, though, until this instrument is developed, and the actual enforcement mechanisms determined, it would be unwise to rely on its potential to reverse the clauses to which I am objecting.

I would like now to address the consent principle. It is my view that we cannot elevate one principle of data protection above the others, because they are inter-related. Consent must be read in the context of legitimacy of purpose, proportionality, rights to refuse, rights to withdraw consent, specificity of purpose and use, and so on. To offer individuals and organizations the opportunity to consent to the use of their sensitive, gated data, for all the permissible purposes, in my view can be read as providing blanket consent to accredited users behind the gate.[11] It can be read as voluntarily giving up any privacy protection one might have expected under local law, and any right to select some purposes as opposed to others. It greatly simplifies one of the biggest problems we faced as a group in grappling with the concept of accrediting users only for certain specific purposes, but from a privacy perspective it greatly reduces the effectiveness of the gate as a privacy mechanism. Once again, if you understand the risks, you will hire a proxy service. From the perspective of an elite North American, this looks like a no-brainer, just hire a proxy.

However, we have a responsibility to examine this from the perspective of a global eco-system. We have now set up a system where accredited actors have

access to inside data, others do not. We have labored long and hard in the group to ensure that the parameters of the RDS are flexible and allow individuals to apply for access beyond the gate to resolve specific problems and issues they encounter, but in fact the vast majority of end-users will be unlikely to make effective use of this right. I totally agree with my colleagues that the market will rush to provide this kind of service at low cost, but I flag it as an element to watch in this discussion.

I hope that this clarification serves to flag some issues that are important with respect to data protection. I would like to reiterate my strong support for this report. I believe this report, and the work that lies behind it, is an important contribution to the Whois evolution. I would stress however, that we are setting up the ecosystem to manage personal information globally. Different cultures have different norms with respect to the transparency of their citizens, and it is appropriate to err on the side of protection of information. I would therefore conclude with the following recommendations:

1. Gate the legal contact information for individuals and organizations who wish to protect their private data
2. Consent needs to be meaningful, specific, explicit and for legitimate purposes. A blanket consent as envisioned here does not meet these requirements

Privacy policy at a mature level needs to be developed to inform the other policies referred to here. It cannot come in as the caboose at the end of the train.

I appreciate the opportunity to make these comments.

Respectfully,
Stephanie Perrin

Endnotes:

[1] As noted above, there is some confusion between the text of the report, the graphs and charts, and the appendices that describe how "gated" and "public" data would be protected. It is my contention that this report must be clear; we therefore need to come up with another expression for "public" and "published" that does not convey the impression that all data marked P in the charts is available to everyone.

[2] The EWG Report defines a number of "Purpose Based Contacts" ("PBC") which include a Registrant's contact point for legal purposes, technical purposes, and other specified purposes. These are mandatory, as established in Recommendation 11 ("A domain name must not be activated…until a valid PBC ID is provided for every applicable purpose."). In effect, this means Registrants must provide a point of contact for 6 purposes at minimum, including one for technical support, to report abuse and as a legal contact (see Table on p. 39).

[3] It is probably more accurate to say that the gate exists to protect privacy, not anonymity, although for the average casual user of the publicly accessible data in the new RDS, many registrants should appear anonymously. I have left this report intact but note this clarification.

[4] The EWG Report requires that all Purpose-Based Contacts (PBCs), including legal contact, be public: "Public access to an identified minimum data set must be made available, including PBC data published expressly to facilitate communication for this purpose." (Recommendation 21). Public, or 'ungated', data elements are available to "Any Requestor" for "any purpose" (see p. 11). While most larger companies will certainly have designated contact points for legal and other PBC purposes, the majority of individual registrants will not and this will, in effect, mean that all of their contact information will be designated PBC information and will be 'ungated' or publicly available (see footnotes 3 and 4 below). There is quite a bit of inconsistency in the language here, which I find confusing. If I find it confusing, after 15 months of intense immersion on this working group, I believe others will as well. Please note principle 8: "At least one Purpose-based Contact (PBC) must be provided for every registered domain name which makes public the union of all mandatory data elements for all mandatory PBCs. This PBC must be syntactically accurate and operationally reachable to meet the needs of every codified permissible purpose." My reading of that is that if you do not provide separate contacts for each purpose (eg. Legal, admin, technical, etc.) then your sole contact must contain all the mandatory elements required for each of the PBC's defined. Now, it is the stated intention of the EWG that this information is gated, except for the contact ID, which is a number. It is my contention that this is at best unclear, at worst, we have language which contradicts itself, and we lack definitions that would help the average reader understand our intentions. I believe we need to edit this and provide a non-sophisticated user with a document which is more clear. The EWG has provided some excellent materials which focus on these issues and provide more clarity:
https://community.icann.org/display/WG/EWG+FAQs
http://london50.icann.org/en/schedule/mon-ewg-final-overview/presentation-ewg-final-overview-23jun14-en.

[5] As noted above, every Registrant must provide a "Purpose-Based Contact" (PBC). However, most large companies are likely to have, for example, external legal representation which these entities can provide to fulfill the PBC requirement. This may, in effect, shield these larger companies from disclosing their Registrant information, as Registrant information remains 'gated'. However, as the EWG Report openly acknowledges, the PBC system is designed to help large complex entities with "more extensive contact needs", not the average registrant who will only have one point of contact: "This PBC approach preserves simplicity for Registrants with basic contact needs and offers additional granularity for Registrants with more extensive contact needs. To illustrate this concept, three different fictional but typical examples are given below" (EWG Report, p. 37)

[6] The result of this potential inability of smaller Registrants to hire special shields or pay an attorney, ISP or Registrar for special contact services is that for most Registrants, who do not have extensive contact needs

or extensive contacts to offer, their own contact information automatically will become their "Purpose Based Contact" (PBC) information. The EWG Report explains: "During domain name registration, the Registrant's Contact ID must be used as the default PBC ID for each purpose. The Registrant must be informed of all permissible purposes and given an opportunity to publish other PBC IDs for each purpose, including replacing the Registrant's Contact ID for any or all purposes." (Recommendation 9). The EWG Report elaborates on this:

> *"…the Registrant's own ID be used if more specific PBCs are not provided for a given domain name. For example, if a Legal Contact has not been specified for a given domain name, the Registrant should be informed that parties may need to contact them for this permissible purpose and be given an opportunity to designate a PBC to receive such requests for this domain name. If the Registrant opts not to designate a PBC… [and] prefers to not make public those data elements, the domain name may be registered using an accredited Privacy/Proxy service. (EWG Report, p. 36).*

Again, I would point out that use of the term "make public" would logically be interpreted by the casual reader as made publically available…i.e. not gated. Finally, footnote 36 on p. 137 makes it abundantly clear that this choice is presented to Registrants on a 'take it or leave it' basis: "If Registrant does not supply any Contact IDs during DN registration, Registrant should be informed that the Registrant's own addresses will be published as the primary PBC and given a chance to consent, to provide another primary PBC ID (for example, a Privacy Provider's Contact ID), or cancel registration."

The ultimate effect of this is that most Registrants will have their contact information published under the PBC categories unless they use legal representation or a proxy. Whether this data is outside the gate, or inside, is important, but even if it is inside the gate, it is potentially available to a whole host of users, as yet uncounted, who can use it for all permissible purposes. This in most part replicates the current state of affairs for WHOIS, meaning the move to an RDS system will offer no additional anonymity or privacy to the majority of Registrants. Some jurisdictions, including some with many gTLD Registrants, have constitutional and privacy law protections to safeguard their speech rights and the privacy of directory information (see for example a recent Supreme Court of Canada decision assuring this right: http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do, and a comparable decision from the US Supreme Court: http://www.law.cornell.edu/supct/html/93-986.ZO.html).

It is unclear how the contact publication requirements protect these rights, and will not force Registrants to expose themselves in a way that violates their law's protection.

[7] Please note that for the purposes of the use of privacy/proxy services, the issue of whether the data is inside the gate or outside is less relevant. Having my personal data in the RDS is the key issue. It has been pointed out that some PBC services will be provided by registrars at no cost, but in my view the most reliable, comprehensive way to protect your personal data within the ecosystem is to hire an accredited privacy/proxy service to represent you.

[8] See principle 93. It seems I misunderstood the scope of this recommendation, which I had understood to be elastic enough to help subsidize costs for privacy/proxy services. Apparently this recommendation is restricted to helping economically disadvantaged registrants achieve identity validation. My apologies for the error.

[9] Note that even if all personal data of registrants is gated, the RDS is still a "public directory". Access is more limited than the current WHOIS, but it is still potentially very significant in scope.

[10] Note that in some cases, the personal data will not be collected and put into the RDS. The terms of service requiring data to be collection and put in the RDS could be considered to be in violation of data protection law in some regimes, in which case it might have to remain with the Registrar. This is a hypothetical issue, but a real one until we have an opinion on the system from the relevant data protection authorities.

[11] Recommendation 28 of the EWG Report specifies that all Registrants will be offered an opportunity to consent, at the time of registration, "to the use of their data for pre-disclosed permissible purposes."

In support of the overarching legal principles given in Section VI, Registrars and Validators should afford domain name Registrants and Purpose-Based Contacts

> the opportunity, at the time of data collection, to consent to the use of their data for pre-disclosed permissible purposes, in accordance with the data protection laws of their jurisdiction. In formulating the policy, this principle must be addressed in the broader context of these overarching legal principles.[7]

Once this consent is obtained, even 'gated' or 'non-public' data may be accessed and used for a long list of broadly phrased permissible purposes. The nature of this consent principle is key, and needs further detailed explanation. As currently drafted, it excludes recognition of the right of Registrants to refuse this access/use and excludes the obligation for this consent to be informed, in the absence of jurisdictional data protection law requirements to the contrary. Nor does it, as drafted, require specificity of consent, meaning that individuals will not be given the option of consenting to one permissible purpose (academic research) while refusing another (law enforcement). The EWG Report further recognizes that even the existing long list of expansive permissible purposes is not final, and envisions a mechanism for its periodic expansion (See Recommendation 25).

If I had sufficient faith that additions and precisions on such issues could easily be added in the working group processes that will flow from the report, I would not raise these issues. Sadly, my current analysis of ICANN's respect for privacy protection, throughout the ecosystem, does not give me such confidence, nor does the robust nature of discussion in working groups. I remain committed to helping draft better language, and working on restoring the balance in this very important piece of work.