DRAFT DRAFT DRAFT

We are the "no comments left behind" subteam – the ones analyzing these comments who what ideas, concepts, direction and guidance we might have missed. With so many comments submitted to the WG (over 21,000 including petition signatories), there may have been gems left unexplored by the specific analysis done by the other subteams.

Accordingly, we worked with materials from staff and our own review of comments to create a template that analyzed the comments for 7 categories of input:

- Category A – Issues involving Law Enforcement (e.g., procedures for access to customer data by LE)
- Category B – Methodology (e.g. periodic review/suggested processes after accreditation process is introduced)
- Category C - Other new or additional features that PPSAI WG should be consider adopting
- Category D – Unintended consequences of disclosure of data for (1) registrants, (2) requestors, (3) providers (and hopefully ways WG might address them)
- Category E – Additional reasons for/against the creation of the accreditation program
- Category F – Additional due process concerns not already covered by other Sub Teams, and
- Category G - Other specific topics within WG scope not captured by the above categories.

We are sure it will not surprise you that our template runs over 40 pages. We found many good ideas that don't fit into existing subteams, but merit the WG's consideration; we found many important issues, unintended consequences and proposed features (particularly for review) that merit consideration and review.

We received some appreciative remarks from commenters thanking us (the WG) for the opportunity to comment; we, in turn, are appreciative that so many individuals and organizations, often with little or no past association with ICANN, took the time to review our work, respond and share their ideas, concerns and insights.

What follows is a summary of the Comments, however, given the detail involved in the recommendations that we received.

I. Category A – Issues involving Law Enforcement (e.g., procedures for access to customer data by LE)

We received a number of comments that respond to issues of Law Enforcement access to p/p Customer information. These responses address issues that we, the WG, have discussed, but not yet embodied into a formal document. They include issues of jurisdiction and what jurisdictions Providers should be required to respond to (and not),

scope of what is considered "law enforcement" for purposes of Reveal, and over 11,000 comments of comments, including from Google and Respect Our Privacy, calling for the requirement of a court order or existing due process mechanisms prior to revealing data, including for law enforcement.

Currently Annex E, original and as revised, addresses third party access, and specifically, intellectual property access to Customer data, and is titled "Revised Illustrative Draft Disclosure Framework for Intellectual Property Rights-holders."

If and when the WG moves on to Reveal of Data by a) law enforcement and b) other types of third parties, we have a set of comments, concerns and guidance from commenters in the comments categorized as Category A.

- Category B – Methodology (e.g. periodic review/suggested processes after accreditation process is introduced)

Category B represents a range of commenters who ask the WG for post-implementation processes and reviews that check for success in implementation and confirm that additional problems have not bee create:

- Ongoing Periodic reviews – P/P provide a refuge against "spam, harassment, and other third-party attacks" – a review would check whether p/p services after accreditation continue to do so and whether Reveal has created any problem in this area and whether it has "create[d] a chilling effect on online speech."
- Accountability measures – are accountability measures and financial penalties, as adopted, being implemented and enforced? (See also, Category __, New Features, below).
- Has the Accreditation scheme, as ultimately adopted, been "built on a strong and robust contractual compliance enforcement system?"
- Is any accreditation model "integrated to the greatest extent feasible with the existing RAA so as to minimize accreditation and compliance costs."
- Does the accreditation process, as adopted, take national laws into consideration and work within them them?
- Early Review – within a short period after adoption and implementation of the final rules, ICANN should implement a mandatory review process to survey customers to understand the impact of disclosures made pursuant to the requirements ICANN has imposed.

- Category C - Other new or additional features that PPSAI WG should be consider adopting

Category C represents other new and additional features the WG must consider building into the structures and frameworks it is developing today.

- Notification of ICANN Compliance about a Reveal or Publication breach by P/P Provider.

- Clarification of the accreditation and accountability processes, e.g. "Would like to see privacy/proxy services obligated to comply with the specifications applicable to registrars/resellers/affiliates under the 2013 RAA" and the accreditation scheme "must be built on a strong and robust contractual compliance enforcement system."

- Penalties for any array of violations:
    - For Requestors who would Reveal the data inappropriately
    - For Providers who would Publish the data inappropriately
    - For Providers who would do not respond to demands for Reveal appropriately.

  e.g., "The success of the recommendations depends on strong implementation of accountability measures such as revocation of accreditation and financial penalties."

- Making the language of our WG recommendations and procedures *much easier and more understandable for everyone who will be directly impacted*: "State legislation is crystal clear by comparison. Please reduce the amount of incorporation by reference,

- Category D – Unintended consequences of disclosure of data for (1) registrants, (2) requestors, (3) providers (and hopefully ways WG might address them)

We heard an earful and more about unintended consequences from those we had most hoped to hear from. A letter signed by 105 individuals, all leaders in women's communities and Internet communities, as well as 65 organizations, including: The Tor Project, the Unslut Project, ACCESS, Internet Democracy Project, India, National Center on Domestic and Sexual Violence, National Coalition Against Domestic Violence, National Council of Women's Organizations, Women's Media Center, Women, Action and Media, Stop Street Harassments and Coalitions Against Domestic Violence in Arizona, Illinois, Iowa, Nebraska, New York, North Caroline, Virginia, Wyoming, and many more.

What these comments spoke to where the unintended consequences of disclosure, and particularly the unintended consequences of barring access privacy/proxy services to for those websites "handling online financial transactions for commercial purpose…" The comments of this group merit close review and cannot be properly abstracted due to the detailed explanation of swatting and doxing:

We are writing to you about the Initial Report on the Privacy & Proxy Services published on May 5th, which proposes requiring "commercial website" owners to display their address under their WHOIS data. Broadly defined, this prevents millions of site owners from safeguarding their private information. We strongly oppose the Working Group's proposal,which will physically endanger many domain owners and disproportionately impact those who come from marginalized communities. People perceived to be women, nonwhite, or LGBTQ are often targeted for harassment, and such harassment inflicts significant harm.The endemic nature of inequity online is a matter of deep concern for all of us, as

we are working to make the Internet a safe and accessible place for all voices.

The proposal in front of ICANN would radically undermine progress in that direction, in part by making it far easier to dox domain owners. "Doxing" is the malicious practice of obtaining someone's personal information (e.g. home address, phone number, etc) and making that information more readily and widely available. Doxing makes possible a wide range of crowdsourced harassment and intimidation, which includes everything from unwanted pizza deliveries to unrelenting barrages of rape- and death threats. Doxing also enables "swatting," or calling in false tips that send a fully armed SWAT team crashing through a targeted person's door. Public online directories give doxers, swatters, and stalkers alike easy access to their targets' personal information.

Our concern about doxing is not hypothetical. Randi Harper, a technologist, anti-harassment activist, and founder of the Online Abuse Prevention Initiative, was swatted based on information obtained from the WHOIS record for her domain. The only reason law enforcement did not draw their weapons and break down Harper's door was that she had previously warned her local police department about swatting.

Even the most limited definition of a "website handling online financial transactions for commercial purpose" will encompass a wide population that could be severely harmed by doxing, such as:

* women indie game developers who sell products through their own online stores

* freelance journalists and authors who market their work online

* small business owners who run stores or businesses from their homes

* activists who take donations to fund their work, especially those living under totalitarian regimes

* people who share personal stories online to crowdfund medical procedures

To make things worse, the proposed definition of what constitutes "commercial purpose" could be expanded to include other types of activity such as running ads or posting affiliate links.

If implemented, the current proposal will chill speech—especially speech from people who lack access to lavish legal resources. It will be a generous gift both to harassers and to oppressive regimes. It will curb economic activity by adding untenable risk to using a website to promote one’s business or to collect donations, and may even add this risk to hosting ads. Women, people of color, and members of other marginalized communities, who are the most frequent targets of doxing, will be forced to take costly, speech-restrictive steps in order to protect themselves.

***

Although the working group stakeholders' concerns about being able to verify consumer transactions and find information about businesses are valid, we did not find any evidence that Internet users are having difficulty getting information about businesses because of privacy and proxy services. Further, law enforcement agencies and copyright-holders are already able to access this information through existing legal processes. The unclear merits of this proposal cannot outweigh the inevitable harm that will follow from making millions of website owners' personal information public. Even an ICANN working group recognized (in 2013) that in cases "where identification of speakers would cause a threat to their lives or those of their families," individuals should be entitled to heightened privacy protection.

We strongly recommend that the proposed policy not be adopted. We further recommend that ICANN revisit its own findings from 2013 and move toward making WHOIS privacy the default for everyone. We believe that ICANN should not be complicit in making doxing, stalking, & swatting any easier than they already are. While ICANN certainly did not set out to exacerbate online harassment, that will ultimately be the result of this policy." [Bold added.]

- Category E – Additional reasons for/against the creation of the accreditation program

[Tonight I will list those for and against the accreditation program as a whole]

- Category F – Additional due process concerns not already covered by other Sub Teams, and

["Unintended consequences" comments of category D overlap with Category F with the call for "due process" requests to fix problems – both those the WG has foreseen and those we have not foreseen. As we know, thousands of comments call for the WG to adopt DP (due process) and I'll summarize.]

- Category G - Other specific topics within WG scope not captured by the above categories.

[There is a few here]