

Consumer Trust

Preliminary brainstorming on scope of consumer trust/safeguard review

Consumer/end user behavior

- Navigate
 - Does not resolve
- Use
 - Are new gTLDs more or less likely to point to malware, phishing, botnet command and control, or high volume SPAM?
 - What safeguards are in place for new gTLDs to protect end users from DNS abuse?
- Consumer literacy
 - How the new gTLD string itself may impact user expectations. For instance consumers will look to the TLD as an indication of its content. There is a wide range of TLDs some of which have safeguards / are regulated at the one end of the spectrum to others that do not. Consumers will not necessarily know which they can trust or what they can expect.
 - Do consumers know where to go to report problems?
 - Are consumers aware of the additional safeguards present in the New gTLDs

Developing countries

- Awareness of process
 - Level of outreach (type of outreach, financial and other)
 - Funding for outreach
 - Implementation of outreach (timing)
- Confidence that the new gTLD application process is fair? (Trust in the process)
- Adequate access to assistance?
- Rules - as stated and as applied
- Data (obtain figures that compare how much was spent on outreach compared to other activities)

Procedural

- ICANN's role
 - Enforcement of safeguards and public interest commitments
 - PLACEHOLDER CARLTON
- Dispute resolution processes
- Sufficient data - is there enough data to make conclusions about the fairness of procedures, etc.
 - Public Interest Co~~o~~mmittment Dispute Resolution
 - Post Delegation Procedure Policy
 - Uniform Rapid Suspension

Confusion

- IDNs (homographic attacks)
- Can consumers distinguish a legacy gTLD domain name from a similarly-named new gTLD domain name?

DNS abuse (TBD)

- Is DNS abuse more or less prevalent in new gTLDs than legacy gTLDs?
- What enforcement mechanisms do new gTLDs use to curb DNS abuse ?

- What do DNS Abuse policies look like for new gTLD registries and registrars?
- Are there greater or fewer numbers of ICANN compliance issues with new gTLDs than with legacy gTLDs?

Registry privacy policy

- What type of personal information is collected?
- How long is personal information retained?
- How is personal information protected?
- When is personal information shared?

Trademark issues

Relative costs of defensive registrations

- Pricing models
 - How has the absence of price restrictions affected consumer trust?
 - What are the consequences of the policy? (i.e. increased or decreased trust in the perceived value of domain names? coercive pricing?)

Brands protection (i.e. brand dilution, infringement)

Risk of confusion for a brand

Sunrise pricing

- Creates trust for existing rights holders or harms trust about fairness for new marketplace entrants?

Rights protection mechanisms

- Effectiveness

Level of cybersquatting in new gTLDs

Level of take up in the TMCH

Impact of PICs and other safeguards

Compliance

Complaints

Reduces harm?

Other

What else do we need?

Divide into new gTLDs vs legacy (compliance)

of complaints to registries, registrars

Compare level of abuse among legacy, new gTLDs (Drew to define methodology)

- Select gTLDs to compare (legacy and new)
- Gather lists of all current registrations in those TLDs (zone files)
- Compare the lists of registrations to domain names associated with known DNS abuse (as determined by a reliable authority such as APWG, Spamhaus, etc.)
- Determine whether there is any correlation between findings new/legacy gTLDs, registry/registrar DNS abuse policies, 2013 RAA compliance, literacy about gTLDs from Nielsen study, etc.

Highly regulated sector domains

Data Needs

Developing countries - Resources devoted to outreach
Compliance - TBD (resource allocation)
