Cross-Community Working Party on
ICANN and Human Rights (**CCWP-HR**)
https://icannhumanrights.net/

ICANN Policy and Human Rights

A Primer on Current GNSO Policy Development Processes

Introduction

The Internet Corporation for Assigned Names and Numbers (ICANN) is an international non-profit organisation incorporated in 1998 to manage the Internet's unique identifier systems. Simply put, ICANN coordinates the directory linking website names with server numbers. This entails coordinating the allocation and assignment of names in the root zone of the domain name system (DNS) and the top-most level of Internet Protocol (IP) and Autonomous System numbers.

Such high-level coordination of unique identifiers allows people around the world to connect to the same global network. It also means that ICANN's policies — developed within the multistakeholder ICANN community and approved by ICANN's Board of Directors — can influence the privacy, free expression, access to information, and other rights of internet users on a massive scale.

From heated discussions around privacy and security as they relate to ICANN's Whois database, to high-profile cases like .amazon underscoring freedom of expression concerns, human rights are a frequent topic of conversation within the ICANN community. However, while ICANN has adopted a high-level policy commitment to respect human rights,[1] the so-called "Human Rights Bylaw" has not yet translated into the embedment of human rights considerations, principles, or standards into policy development processes. It is therefore the responsibility of ICANN community members to ensure that the rights of registrants and internet users remain central to discussions, and are upheld in policies.

This primer captures the current status of ICANN policy development processes relevant to human rights, aiming to facilitate newcomers' involvement while generating awareness within the broader ICANN community of the potential human rights impacts of forthcoming policies.

ICANN's Multistakeholder Model

ICANN's multistakeholder model is premised on community-based, bottom-up, consensus-driven policy development. The community is comprised of individuals, private companies, governments, and civil society that engage through two mechanisms: Supporting Organizations (SOs) and Advisory Committees (ACs). SOs develop and refine DNS policy and ACs consider policies and provide advice to the Board. It's important to note that only DNS policies are subject to formal policy development processes, or PDPs. ICANN typically seeks community feedback on operational policies and general practices though such input is not required.[2]

Policy development processes can be initiated anywhere with the ICANN ecosystem: from the Board, an Advisory Committee (AC), or a Supporting Organization (SO).

There are four ICANN **Advisory Committees**:

- The At-Large Advisory Committee (ALAC**)** is underpinned by its own hierarchical At-Large Community and provides advice on ICANN's activities as they relate to the interests of individual Internet users.
- The Governmental Advisory Committee (GAC) contains only acknowledged governmental representatives who provide advice on ICANN's policies and activities, particularly when they interact with laws, international agreements, or public policy issues.
- The Security and Stability Advisory Committee (SSAC) is an invite-only organization responsible for advising on matters relating to the security and integrity of the DNS.

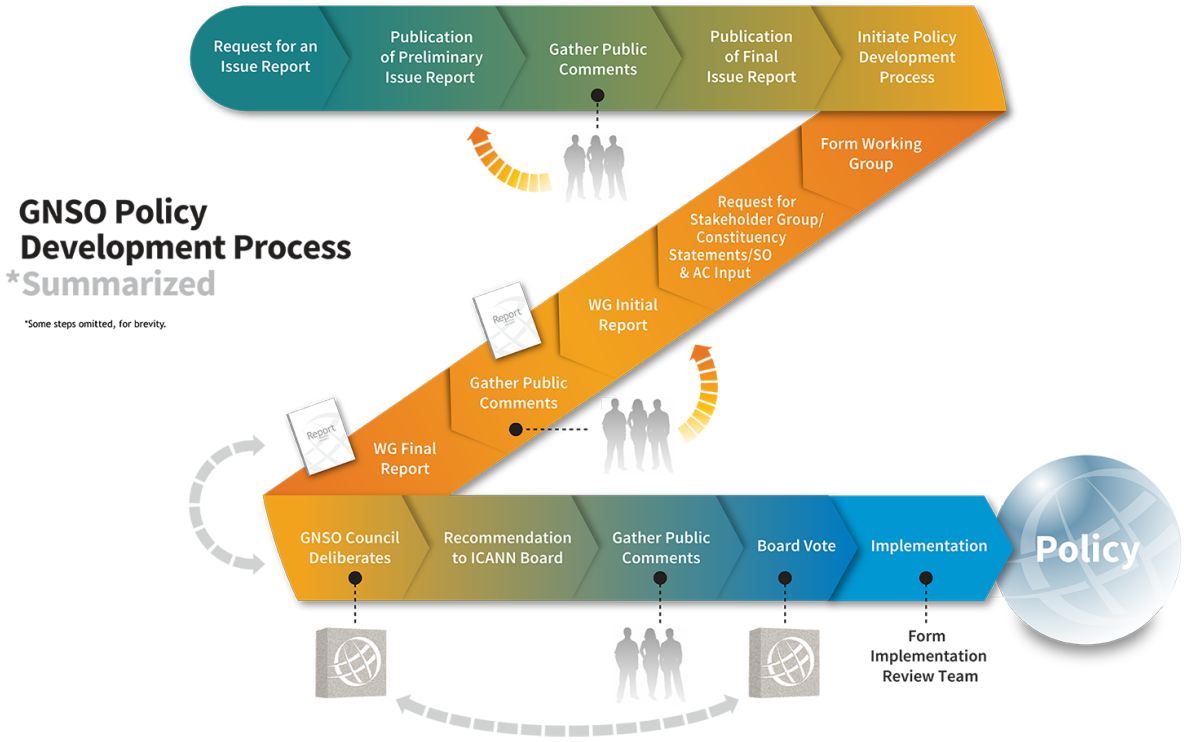
[1] See ICANN Bylaws, 1.2(b)(viii): https://www.icann.org/resources/pages/governance/bylaws-en
[2] Find more information about ICANN policy processes: https://www.icann.org/policy

- The Root Server System Advisory Committee (RSSAC) consists of representatives from root server system operators who advise on matters relating to its operation, administration, security, and integrity.

And there are three **Supporting Organisations**:

- The Address Supporting Organisation (ASO) is comprised primarily of representatives from the five Regional Internet Registries who advise the Board with respect to policy issues relating to the operation, assignment, and management of Internet addresses.
- The Country Code Names Supporting Organisation (ccNSO) is an association of ccTLD managers responsible for developing and recommending to the Board global policies relating to country code top level domains (ccTLDs).
- The Generic Names Supporting Organisation (GNSO) is a multistakeholder body responsible for developing and recommending substantive policies relating to generic top level domains (gTLDs).

Whereas the ASO and ccNSO have restricted membership, the GNSO is designed to accommodate broad participation through its four Stakeholder Groups (Commercial, Non-Commercial, Registrars, and Registries) and several special-interest Constituencies.[3] Of all the SOs, the GNSO has the most clearly defined Policy Development Process, summarized in the image below.



[3] Learn more about the GNSO Stakeholder Groups and Constituencies: https://gnso.icann.org/en/about/stakeholders-constituencies

Based on this unique combination of accessibility and predictability, this primer will focus exclusively on the GNSO's active and ongoing PDPs and the opportunities for engagement they present.

GNSO Policy Development Processes[4]

Within the ICANN ecosystem, the GNSO develops and recommend changes to policies for Generic Top Level Domains (gTLDs). More specifically, the ICANN bylaws carve out the role of the GNSO to primarily develop and recommend to the ICANN Board substantive policies relating to gTLDs.

According to its own mission statement, the GNSO intends to *"keep gTLDs operating in a fair, orderly fashion across one global Internet, while promoting innovation and competition."* This is done through Policy Development Processes (PDPs). This briefing paper is intended to present an overview of the various active PDPs within the GNSO, and outline human rights considerations that arise from them.

The GNSO PDP Process is formalized into various stages, as demonstrated by the diagram above. Each PDP begins when a particular issue is identified, *and* found to be intended to result in consensus policy. Once identified, GNSO staff and council prepare a report, conduct research, outreach, discussions as needed in order to have a preliminary analysis of the issue, as put together in the Preliminary Issue Report. After deliberation with the Council, and public comments, a final issue report is produced.

Once the final issue report is released, the Initiation stage begins, which asks one simple question: should we move ahead with this PDP based on this final report? If the GNSO Council votes 'yes', a PDP is initiated at this stage. A team drafts the PDP Charter which is subsequently adopted. The next stage is a Working Group Stage. Here, the WG in accordance with the Charter, deliberates on the issue, carries out SO/AC engagements, asks for input from constituencies and stakeholders within the ICANN community, opens up reports for public comments, and finally produces a WG Final Report. This report is then considered for adoption in the GNSO Council, and if adopted, sent for a Board vote. Board-approved policies are then implemented.

The table below outlines active GNSO PDPs.[5] This primer continues with an overview of each PDP's current status, relevant human rights impacts, and things to watch as the process progresses. The primer concludes with a few general tips for newcomer engagement.

---

[4] Find more information about GNSO PDPs here: https://gnso.icann.org/en/basics/consensus-policy/pdp
[5] ICANN GNSO Active Projects: https://gnso.icann.org/en/group-activities/active

Policy Development Process	Working Group	Council Deliberation	Board Vote	Implementation
PDP IGO-INGO Access to Curative Rights Protection Mechanisms		X		
PDP gTLD Registration Data Services	X*			
PDP Protection of IGO and INGO Identifiers in All gTLDs			X	
PDP Privacy & Proxy Services Accreditation Issues Working Group			X	
PDP 'Thick' Whois Policy Development Process				X
PDP Translation and Transliteration of Contact Information Policy Development Process				X
PDP Review of All Rights Protection Mechanisms in All gTLDs	X			
PDP New gTLD Subsequent Procedures	X			

* The RDS PDP is currently suspended indefinitely; see the corresponding section below for more details.

IGO-INGO Access to Curative Rights Protection Mechanisms[6]

Date of charter adoption: 15 November 2012
Current status: Board Vote
Progress: The Working Group Initial Report was published in January 2017, and the Final Issue Report is due at this time.

In 2014, the GNSO Council recognised that International Governmental and Non-Governmental Organisations (IGOs and INGOs) may have difficulties relying on current dispute resolution procedures like the UDRP and the URS. According to the PDP's own Executive Summary, *"This effort determines whether the curative rights protection mechanisms in place for both pre-2012 and new gTLDs should be amended*

[6] Project overview for the IGO-INGO PDP: https://gnso.icann.org/en/group-activities/active/igo-ingo

to permit their use by International Governmental Organizations (IGOs) and International Non-Governmental Organizations (INGOs). This page provides a summary of this WG's efforts."

This is mostly because of jurisdictional complications – traditional dispute resolution procedures rely on parties to submit to the jurisdiction of national courts, which is not in line with IGO's practice of claiming jurisdictional immunity from the countries in which they are situated. Specifically, the charter for this PDP required the Working Group to examine whether to amend the UDRP and URS to allow access to and use of these mechanisms by IGOs and INGOs, or if a separate, narrowly tailored dispute resolution mechanisms taking into account specific needs from IGOs and INGOs should be developed.

The Working Group's initial report recommends that no changes to the UDRP and URS should be made, and neither should new processes be created for INGOs. In context of IGOs, the Working Group suggested development of a policy guidance brief to explain ways in which IGOs could pursue claims under the UDRP and URS without jeopardizing benefits otherwise enjoyed. Indeed, the Working Group also decided to exclude INGOs as a protected classification of organisations, *inter alia,* because INGOs do not encounter problems in enforcing trademark rights and do not enjoy a claim to sovereign immunity.

Things to watch: Final recommendations from the Group have been submitted to the GNSO Council for review and approval.

---

gTLD Registration Data Services (RDS)[7]

Date of charter adoption: 19 November 2015
Current status: Indefinitely on hold between initiation and working group stages
Progress: The working group Initial Report is still due at this time.

This PDP is meant to define the purpose of collecting, maintaining and providing access to generic TopLevel Domain (gTLD) registration data and consider safeguards for protecting that data, determining if and why a next-generation Registration Directory Service (RDS) is needed to replace WHOIS, and creating policies and coexistence and implementation guidance to meet those requirements. According to the PDP's own Executive Summary, "*Comprehensive 'Whois' policy reform remains the source of long-running discussions within the ICANN as well as wider Internet community. Any discussion of 'Whois' – hereafter called gTLD registration data and directory services – typically includes topics such as purpose, accuracy, availability,*

[7] Project overview for the RDS PDP: https://gnso.icann.org/en/group-activities/active/rds

privacy, anonymity, cost, policing, intellectual property protection, security and malicious use and abuse.

On 8 November 2012, the ICANN Board passed a resolution that led to the creation of an Expert Working Group (EWG) and, in parallel, also launched this Board-initiated GNSO Policy Development Process (PDP). The Board specifically called out two of these topics in its request; purpose and accuracy. With regard to purpose, at a minimum the most basic purpose, which is commonly accepted, is that gTLD registration data allows domain name holders to be contacted. However, who would be granted the right to access the data under what circumstances and contact the holder and by which means, is a set of difficult follow-up questions that need to be answered. In relation to accuracy, There are many data elements in the Whois database required under the Registry Agreements and the Registrar Accreditation Agreements; if only one of these data fields is incorrect, does that mean the Whois information is inaccurate? And how can the accuracy of data be verified and/or measured, especially considering that if data is not accurate the purpose of gathering the data might be questionable in the first place".

This PDP was intended to be carried out in three phases. First, defining if and why a next generation RDS is needed. Second, looking into the details of what a next generation RDS should do. And third, considering how a next generation RDS should implement policy.

This necessarily involves a close and careful study of WHOIS, and ICANN's legacy of building policies and procedure around WHOIS. For the purposes of this scoping, however, we highlight complexities with respect to the main questions this PDP will be examining.

- **Users / Purposes**: This is a particularly timely question given the massive overhaul in data protection standards brought about by the GDPR. This question has implications beyond just the GDPR. Issues to consider here include: Who should have access to gTLD registration data and why? At what level should these users and purposes be defined? Is the current ambiguous approach enough? Should the recommendation to have purpose-based contacts, specific proposed users and purposes be taken forward?
- **Gated Access**: What steps should be taken to control data access for each user/purpose? Does a tiered model of access to data work? If yes, what would that model look like? How can access to data be used as a level to enhance accountability in re: disclosure of gTLD registration data?
- **Privacy**: This will be closely connected to the way in which ICANN moves forward with GDPR compliance and the ePDP on temporary specifications for gTLD registration data.
- **Data Quality**: Beyond data accuracy and access more broadly, the question of having accurate data will also need to be considered carefully. What privacy

protecting standards and processes can be put in place to ensure that data quality and granularity are optimum for detering fraudulent use, and promoting privacy, particularly that of end users?

All of the bullet points mentioned above are closely related to the compliance model discussion around the GDPR, and also have the potential to significantly strengthen or hinder the freedom of expression within ICANN's mandate. Pushing for policies that are human rights strengthening by design would mean having the minimum amount of personal information publicly displayed, and should ideally require registrants to "opt-in" to share sensitive data, as opposed to having these details stay as the default.

- **Coexistence**: What steps should be taken to enable next-generation RDS coexistence with and replacement of the legacy WHOIS system?
- **Compliance**: What steps are needed to enforce these policies?
- **System Model**: What system requirements must be satisfied by any next-generation RDS implementation?
- **Cost**: What costs will be incurred and how must they be covered?
- **Benefits**: What benefits will be achieved and how will they be measured?
- **Risks**: What risks do stakeholders face and how will they be reconciled?

Things to watch: Due to the GDPR coming into force, this particular PDP was temporarily put on hold in June 2018, while a new "Expedited" PDP launched the following month to review ICANN's Temporary Specification for GDPR compliance (see the EPDP section at the end of this primer for more information).[8]

Review of All Rights Protection Mechanisms in All gTLDs (RPMs)[9]

Date of charter adoption: 15 March 2016
Current status: Working Group stage
Progress: The working group's Initial Report is still due at this time.

This PDP explores the current state of all rights protection mechanisms implemented for both existing and new gTLDs, including, but not limited to the Uniform Dispute Resolution Policy (UDRP) and the Uniform Rapid Suspension Dispute Resolution Procedure (URS). The Final Issue Report was published by ICANN in January 2016, stating that it "is concerned with those policies and processes, developed in consultation with the ICANN community, aimed at combatting cyber-squatting and

[8] Find more information about the suspension of the RDS PDP here: https://gnso.icann.org/sites/default/files/file/field-file-attach/policy-briefing-next-gen-rds-05jun18-en.pdf
[9] Project overview for the RPM PDP: https://gnso.icann.org/en/group-activities/active/rpm

providing workable mechanisms for trademark owners to either prevent or remedy certain illegitimate uses of their trademarks in the domain name system (DNS)."

Despite divergence in views from the community, this PDP operates in two phases. The first phase is to study existing RPMs excluding the UDRP, namely: the Uniform Rapid Suspension Dispute Resolution Procedure (URS); the Trademark Clearinghouse (TMCH) including Sunrise periods and the Trademark Claims notification service; and the Post-Delegation Dispute Resolution Procedures (PDDRPs). The second phase involves studying the UDRP exclusively. This analysis will focus on the URS and TMCH as they have formed the bulk of current debate.

Uniform Rapid Suspension System (URS)

The URS is a rights protection mechanism intended to complement the UDRP as a budget friendly, nimble method for rights holders to seek relief in "the most clear-cut cases of infringement". A URS complainant must show that the alleged infringement is identical or confusingly similar to the complainant's mark (which is valid under national or regional registration or court proceedings). The complainant must also prove that the registrant has no interest in the domain name, and is being registered in bad faith. The fee for URS is usually lower than that for UDRP proceedings. The standard of proof for URS proceedings is kept high with the intention to expedite resolutions, i.e. the complaint is in and of itself considered all the necessary evidence at the initial stage.

If considered adequate, the domain is question is suspended for the remainder of the registration period. The appeal process allows either party to bring about an appeal within 14 days.

Perpetuation of power imbalances is a real risk within the URS system. Here complaint is merely "examined", i.e. a complaint is only considered on the basis of facts presented within it. This skews the probability of protection towards dominant players and well known complainants who by virtue of their standing have established marks already. This is a significantly shallower approach than what was contemplated in the UDRP, which has in place a Panel to study complaints in an in-depth fashion. This not only has competition implications, it also severely jeopardizes the freedom of expression of smaller players.

Current questions being considered by the PDP have profound implications for procedural fairness, the right to remedy, and balance of IP rights with human rights. Specifically, important issues that are chiefly discussed in the RPM Sub teams for URS Documents, Providers and Practitioners that advocates should consider include:

- Should the URS allow for additional remedies such as perpetual blocking or other remedies, e.g. transfer or a "right of first refusal" to register the domain name in question?
- Is the current length of suspension sufficient?

- Is the cost allocation model appropriate and justifiable?
- Should there be a loser pays model? If so, how can that be enforced if the respondent does not respond?

Trademark Clearinghouse (TMCH)

The TMCH was announced in 2012, at the same time as ICANN's new gTLD programme was being expanded. The TMCH is a centralised database of trademarks that have been verified, which will be put into use in respect of new gTLDs. If a rights holder's trademark is included in the TMCH, she is eligible for a fast lane registration option, before the gTLD is opened to the general public. Sunrise Periods refer to a 90 day window during which rights holders of verified trademarks in the TMCH can pre-register names) Trademark Claims Notice is a precautionary, proactive method by which registrants of potential infringements are discouraged from pursuing specidic domain names.

Before providing an overview of human rights implications, it is important to consider what the TMCH does not do: It does not prevent infringement, it only makes it easier to prove bad faith retrospectively. It is a repository of verified data, but does not evaluate the scope or rights arising from such data, i.e. it can have two trademarks that are valid and identical.

Concerns arising from the TMCH chiefly include a hesitation on ICANN's power to potentially inhibit freedom of expression by deciding what constitutes a valid entry into this database, given its wide discretionary powers in this regard. ICANN's internal policies for valid names, confusingly similar strings, community names etc have been a cause of concern in the past, independent of the TMCH as well. Competition concerns also abound, especially given sunrise periods and trademark claims notices. Gaining entry into the TMCH is a complicated, resourse-heavy exercise, and the benefits that arise from such inclusion entrench this systemic advantage.

There have been sub-groups formed within this PDP to look at data gathering,[10] sunrise registrations,[11] trademark claims,[12] and Private Protection Mechanisms are considering these issues.

A few important questions for consideration within the PDP charter that have particular human rights implications are as follows:

- Are recent and strong ICANN work to understand and incorporate human rights relevant to RPMs?
- How can costs be lowered so end users can easily access RPMs?
- Is the protection of the TMCH too broad?

[10] Data gathering mailing list: https://mm.icann.org/pipermail/gnso-rpm-tmch/

[11] Sunrise registrations mailing list: https://mm.icann.org/pipermail/gnso-rpm-sunrise/

[12] Trademark claims mailing list: https://mm.icann.org/pipermail/gnso-rpm-trademark/

- Does a Trademark Claims period create a potential "chilling effect" on genuine registrations, and if so, how should this be addressed?
- Is the TMCH providing too much protection for those with a trademark on a generic or descriptive dictionary word, thus allowing a trademark in one category of goods and services to block or postpone the legitimate and rightful use of all others in other areas of goods and services?
- How can TMCH provide education services not only for trademark owners, but for the registrants and potential registrants who are equally impacted by their services?
- Should sunrise periods continue to be mandatory? If so, should the current requirements apply or should they be more uniform?

Things to watch: Working Group Initial Report is due at this time.

New gTLD Subsequent Procedures (SubPros)[13]

Date of charter adoption: 21 January 2016
Current status: Initiation
Progress: Awaiting Initial Report from Work Track 5 to enter Working Group phase.

This group is tasked with determining whether changes or adjustments are needed to the 2007 *Introduction of New Generic Top Level Domains* policy recommendations.[14] According to ICANN's PDP summary, "*When the application submission period for the initial round closed in June 2012, the GNSO Council believed that it had a continuing interest and role to play in evaluating the experiences of the first round and proposing policy recommendations, if necessary, for changes to subsequent rounds. Thus, the GNSO created a Discussion Group to begin that evaluation process and possibly identify areas for future GNSO policy development.*"

Potential outcomes of this PDP are:

A. Amending or overriding existing policy principles, recommendations, and implementation guidelines;
B. Developing new policy recommendations; and
C. Supplementing or developing new implementation guidance.

The structure of this PDP stems from the efforts of a preceding Discussion Group, active from 2012 to 2015, which identified five issue areas, or Work Tracks, for consideration.

[13] Project overview of Sub Pros working group: https://gnso.icann.org/en/group-activities/active/new-gtld-subsequent-procedures
[14] https://gnso.icann.org/en/issues/new-gtlds/pdp-dec05-fr-parta-08aug07.htm

Specific human rights issues for each track are identified in the pages that follow. The degree and nature of each potential impact are based on existing and prior examples of a similar nature. Where this information is unavailable, the impacts are phrased as questions that should be addressed during the development process, or at a later stage through amendment and new PDPs.

Work Track 1: Overall Process, Support, and Outreach

In the context of gTLDs, the assignment and regulation procedures must aim to increase transparency and accountability. As a part of these efforts, uncontrolled discretion must be limited through reliance on due process. Rooted in the foundational issue of "Competition, Consumer Trust, and Consumer Choice," Work Track 1 seeks to make the process for applying for new gTLDs more clear and accessible for potential gTLD registries around the world.[15] The track covers the Applicant Guidebook and Accreditation Programs; application fees, communications, queuing, and submission periods; and support for applications from developing countries. Addressing these issues is key to increasing the transparency and accountability of gTLD creation and allocation, while minimizing the potential harms from processes that are unfair or unpredictable. The following issue areas are relevant to human rights advocates:

Inequality in Global Allocation of gTLDs

According to a study conducted by ICANN on the new gTLD program, more than 80% of the new gTLD applicants were from Europe or the USA.[16] Such limited representation of the global community demonstrates that the current system may be unable to bridge this divide. Increasing accessibility will therefore ensure that no group is unfairly privileged and create a level playing field for all those who wish to participate in the gTLD process.

As acknowledged in the Update to the Cost Considerations of the new gTLD Program, concern remain that $185,000 USD application fee is a deterrent to applicants from developing nations, non-profits, and others with limited financial resources. The question of whether this amount is a fair one was considered in the latest round of community input as well.

Support for Disadvantaged Applicants

ICANN's Applicant Support Directory allows gTLD applicants from developing economies to seek financial and technical assistance for their application. ICANN sets aside a certain amount for assisting these applications. However, the extent of the initiative's success is unclear. Increased transparency around procedures, particularly the outcome of requests and efficacy of the dedicated funds set aside by ICANN,

[15] Find more information about the New gTLD Program and application process: https://newgtlds.icann.org/en/about/program

[16] Of the 1,930 applicants 82% were from Europe or the US: https://newgtlds.icann.org/en/program-status/statistics

would allow the community to better understand the system and devise possible methods for its improvement.

First Come, First Served Approach

Presently, gTLDs are allotted on a first come, first served (FCFS) basis, as opposed to grouped approaches like regular application periods or periodic rounds. The FCFS system likely favours well-resourced applicants who have prior access to information over those who do not, as time spent procuring funds or seeking guidance on the application process raises the possibility that the preferred domain string would be unavailable by the time the application is ready to submit. As a result applicants with the advantage of knowledge or experience are more likely to receive their preferred allotments than less privileged parties seeking the same domain string. This may also impact the profile of applicants, encouraging those from more affluent nations where there are already many successful applicants for gTLD.

Consumer Welfare and Privacy

In order to ensure that the users are given prime importance and so as to not unduly impact their privacy and sensitive information, security forms an integral aspect and responsibility of ICANN assuring an unimpeded ability to access resources online. Article 12 of the UDHR refers to the right to privacy and protection against interference with the same. Since domain names can potentially cause harm to the user's privacy through WHOIS requirements it is ICANN's duty to protect against the same in the cases listed below.

Protection against TLD Squatting: The threat of TLD squatting refers to use of domain names similar to well-known existing names for the purpose of capitalizing on notoriety by misleading the public or selling the domain back to the trademark holder at an inflated price. Such squatting can cause users to unintentionally access gTLDs of similar names which may have malicious content or may collect sensitive information from them on this pretext. It is of great importance that ICANN protects internet users from confusing and malicious activities of this nature.[17]

Work Track 2: Legal, Regulatory and Contractual Requirements

Base Registry Contract

The Base Registry Agreement exists between the registrar and registry. The public comment to the Preliminary Issue Report suggested that some elements of the gTLD procedures, such as registry pricing, sunrise periods and practices, and other things have been perceived by some in the community to have circumvented the intended goals/protections developed by the community, especially in regard to potential registrants seeking to protect their rights in names. For example, the treatment of certain names as 'premium names' where registry operators can charge a greater

[17] See Laura DeNardis, *Hidden Levers of Internet Control*, available at http://www.tandfonline.com/doi/pdf/10.1080/1369118X.2012.659199

amount creates a potential for exploitation without ICANN ensuring oversight on registry pricing policies, with a clear guidance mechanism for registry pricing.[18]

Extent of reservation rights granted to IGOs

As the present framework stands, special rights are granted to non-governmental or intergovernmental organisations to prevent third party registration of any TLD string similar to their name. This protects such organisations from facing a loss of reputation or recognition from users, who might confuse their domain with that of the similar third party TLD string. However, it is suggested that this restriction must be narrow so that it does not cause an undue restriction on the extent of choice available to gTLD string applicants. Reservations are currently in place for IGOs as well as many names related to IOC, ICRC and the National Red Cross movements. The IOC and ICRC related reserved names list is very expansive and can affect one's potential to comment on their work through a .sucks or .fail domain, etc.

Trademark Clearing House

The priority mechanism of the Trademark Clearing House, whereby any applicant having an existing trademark in a related gTLD string is granted priority over other applicants, is a potentially restrictive process that can create monopolies. Due to the sunrise period clause, there is priority even if the trademark has not yet acquired a registration. As a result, the question of the validity of the trademark has not been properly addressed before the grant of the gTLD, leading to a concern of the absence of sufficient procedural safeguards.

Work Track 3: String Contention Objections and Disputes

Content-based gTLD String Evaluations

As a part of the procedure of new gTLD Application Evaluation for a particular string, there is a concern that validity of the string may come to depend on the evaluation of the content of the website. As ICANN has historically stayed away from content regulation (and it is, indeed, outside the scope of the organisation's mandate), this is an important consideration for freedom of expression. This concern was first expressed when ICANN's San Francisco GAC Communiqué March 16, 2011 stated that the Corporation may move on to a system "*assuming an ongoing management and oversight role regarding Internet content"*. The Council of Europe Report at ICANN 50 drew on this communiqué to suggest that this could mean that ICANN may extend its scope such that *"the approval or rejection of applied-for new gTLD strings may involve an evaluation process where judgments related to content are made."* In other words, ICANN could examine applications for a gTLD string and prioritise certain types of content or speech over others, which would amount to a denial of free speech. As a procedure that could potentially focus on content of a gTLD through value judgment,

[18] Report of Public Comments to the Preliminary Issue Report on New gTLD Subsequent Procedures: https://www.icann.org/en/system/files/files/report-comments-new-gtld-subsequent-procedures-04dec15-en.pdf

gTLD owners may face ICANN's procedural censure merely based on their website contents.

Community, Trademark and Public Interest Objections to gTLD strings

The Applicant Guidebook provides for four opposition mechanisms to gTLD string applications. One of these is the community objection, where there is a significant objection from the community to a certain proposed gTLD string, such that a panel of experts will review all objections designated by the applicable Dispute Resolution Service Provider (DRSP) to determine whether the objector has standing to object. Following this, the two parties either enter into dispute resolution process or the application/objection is withdrawn.

The is concerning because the definition of what amounts to 'significant objection from the community' is unclear, so that such objections can be made in an exploitative fashion against free speech even where there is no real or significant harm or effect accruing to any community.

The Trademark Objection may further allow for companies to take action against gTLD strings which are used to make fair criticism of existing organisations. Eg. The .sucks domain may be held as defamatory to an individual or company merely based on the domain name, and irrespective of the actual content of the website.
Similarly, the Public Interest based objection to strings can take place where a potential new gTLD is contrary to generally accepted legal norms relating to morality and public order that are recognized under principles of international law. This also can potentially overreach its mandate, resulting in harm to the right of free speech. Eg.- When two TLD strings are identical/very similar, the string which is of greater value to the public interest will receive priority in evaluation- however it is unclear what the specific standard of public interest will be in this case.

Censorship

There is a possibility that gTLDs could result in easier censorship by governments. For example, the Chinese government had made a proposal for a law which would allow only domain names registered in China to be accessed within the country, and for all others to be automatically blocked.[19] Additionally, there is a potential for automatic censorship of domain names blacklisted by governments, regardless of the location of registration. Such a procedure was suggested by .xyz,[20] and demonstrates how government pressure can affect the manner in which registries reserve or block domains.

Global censorship and seizure of international domain names also takes place through the United States government bodies, namely the Immigration and Customs

[19] https://thestack.com/world/2016/03/29/china-proposes-foreign-domain-name-censorship/

[20] https://www.eff.org/deeplinks/2015/10/accepting-chinese-censorship-domains-registry-xyzcom-invites-more

Enforcement, mainly on grounds of internet counterfeit trafficking and piracy. Domain names are disabled through the transfer of control of the domain by the registrar to the authority, however, efforts for greater control through filtering of domain names were proposed by the SOPA and PIPA Bills. The use of DNS for the control of intellectual property is disproportionate as it can have the technical effect of undermining the security of DNS, as well as causing global censorship on the basis of one country's IP laws.[21]

Cultural Relativism with respect to Offensiveness of gTLDs

Many governments have opposed new gTLDs on the ground of public interest, such as .catholic and .islam on the ground that the content associated with these domains may not be in line with the belief of these religions, thus affecting certain communities adversely. Saudi Arabia also made an opposition to .gay, .baby, .porn, .sexy, .adult, .hot, .sex, .dating and .virgin on the grounds that they are against public morality, particularly to its communities. While their opposition may not be viewed the same way globally, it raises the question of the weight to be given to each community's views in order to ensure diversity in participation and involvement.

Work Track 4: Internationalised Domain Names and technical and operational issues

Internationalised domain names, or IDNs, were created to promote multilingual participation on the Internet through the inclusion of native languages and scripts as a part of domain names. The new gTLD procedures intend to further the growth of IDN.

Access and Representation

However, while the IDN initiative is intended to be more inclusive globally, we must determine whether all countries and speakers of different languages in fact have an equal opportunity and access to IDN. This would allow for true representation of their language, country or dialect in the IDN system. While the demand for different IDNs may affect the supply of the resource, it is to be determined whether societies having more limited access to technology ought to be encouraged to increase demand through the creation of relevant IDNs.

Registry Security

Under the new gTLD regime, it is possible for the use of either existing accredited registries or any registry service of choice. While this increases the choices available to users, there is the concern that unsafe or unsecure registries may arise due to insufficient oversight into their security procedures.

Work Track 5: Geographic Names

[21] Further reading is available at http://www.gizmodo.com.au/2014/06/are-new-top-level-domain-names-a-squatters-dream/

The topic of geographic names in top-level domains was included under Work Track 2 of this PDP in its original charter. Due to the controversy and nuance of the subject, highlighted by high-profile debates such as those surrounding the use of the gTLD .amazon,[22] geographic names were broken out into Work Track 5 in late 2017.[23] Because of its late start, this Work Track is running slightly behind schedule. While the Initial Report for Work Tracks 1-4 was published for community review in July 2018, Work Track 5's Initial Report wont be ready until ICANN63 in October 2018 at the earliest.

Things to watch: The GNSO produces monthly Subsequent Procedures PDP Newsletters, outlining the current status and next steps of all five tracks. All of the newsletters can be found on the SubPros wiki.[24]

Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data (EPDP)

One high-profile PDP is notably absent from this primer: the Temporary Specification for gTLD Registration Data Expedited Policy Development Process, or EPDP.[25] This abnormal process kicked off in July 2018 with a mandate to revise ICANN's Temporary Specification for gTLD Registration Data23, a stop-gap solution to bring ICANN's contractual requirements regarding collection and publication of registrant data (formerly made public via the now-defunct Whois database) into compliance with the European Union's new General Data Protection Regulation. The process is also expected to produce an initial model for providing accredited access to non-public registration data. Ideally, the outputs of this working group will serve as the basis for a more permanent global policy to replace the Temporary Specification when it expires in May 2019.

Whereas other GNSO policy development processes have taken years to complete, a truncated version of the established GNSO Policy Development Process was devised to meet the EPDP's strict timeline, removing elements such as the first public comment period and staff issue report, and shortening input periods and expected report lengths.[26] In terms of participation, unlike other GNSO PDP efforts, which are open to

[22] See, for example: https://www.cfr.org/blog/case-amazon-and-what-it-means-icann

[23] Find more information in the GNSO's call for Work Track 5 volunteers: https://www.icann.org/news/announcement-2017-10-22-en

[24] Sub Pros wiki: https://community.icann.org/pages/viewpage.action?pageId=58001970

[25] More information can be found on the EPDP Wiki: https://community.icann.org/display/EOTSFGRD/EPDP+on+the+Temporary+Specification+for+gTLD+Registration+Data

[26] PDP vs EPDP Process Flow and Dependencies diagram: https://gnso.icann.org/sites/default/files/file/field-file-attach/pdp-epdp-process-flow-dependencies-14apr18-en.pdf

anyone, the EPDP restricted participation to appointed members, alternates, and liaisons. Finally, due to the high-profile and contentious nature of the topic at hand, inclusion in the process was expanded beyond GNSO Stakeholder Groups to include Advisory Committees, which usually comment on policies under development without engaging in the development process itself.

Because of the EPDP's divergence from standard GNSO practices in terms of timeframe, participation, and inclusion, it has been excluded from this primer as an exception to normal operating procedures. Nonetheless, this exceptional process has clear implications for human rights, particularly privacy, security, access to information, and free expression. Readers are therefore encouraged to monitor proceedings as they evolve.[27]

Final Tips

Most ICANN mailing lists are archived and publicly available. PDP working group email archives can be found on the GNSO PDP, or "Active Projects", landing pages.[28] Once you have identified a PDP or work tracks that you are interested in, perusing the group's recent conversations will give you a better understanding of the issues and state of play.

The following is a general blueprint for getting involved:

1. Visit the GNSO website, and head to PDP workspaces.
2. Check out different PDP workspaces to determine your areas of interest.
3. Once you have narrowed interests down to a specific PDP, clarify its status to ensure that meaningful engagement is possible. (If the PDP is in the late stages of Council Deliberations, Board Vote, or Implementation, it may be too late to join the process.)
   4. Review available reports (particularly Preliminary Issue Reports and other over-arching documents), subscribe to updates where possible, and join corresponding mailing lists to join the conversation.
4. Write to the PDP Chair (or Co-Chairs), or active members from the stakeholder group you identify with to identify concrete opportunities for engagement.

[27] In addition to the resources available on ICANN Org's website and the community wiki, internet industry sites are also reporting on the proceedings. Examples: https://www.theregister.co.uk/, http://domainincite.com/, or https://domainnamewire.com.
[28] https://gnso.icann.org/en/group-activities/active