ICANN73: What It Means for Brand Owners

Faisal Shah
Margie Milam
Mason Cole
Susan Kawaguchi

March 23, 2022

ICANN73: Topics of Interest

- Progress toward WHOIS registration data access (known as SSAD)
- Domain name system (DNS) abuse
- WHOIS data accuracy scoping effort
- Procedures for subsequent rounds of new generic top-level domains (gTLDs)
- Governmental interests in domain name policy outcomes
- Rights protection mechanisms (RPM) review

Domain name registration data (WHOIS) access

- Current situation regarding WHOIS access:
  - No standard process for making requests / often no responses
  - Disclosure success rates are spotty; some require subpoena or UDRP
  - More registrars have signed on to a “tiered model” to charge for data requests
  - Registrars continue to perform “balancing tests” for access decisions
  - Some registries are cooperative and will supply data
  - NOTE: Requestors must ask for underlying data if proxy employed

Domain name registration data (WHOIS) access

- What is the standardized system for access and disclosure (SSAD)?
  - Proposed SSAD would be a centralized system for requesting WHOIS data
  - Subject to “balancing test” by registrars
  - For brand holders, a potential gateway for addressing domain name abuse
- What is the status of development for SSAD?
  - ICANN’s Operational Design Assessment puts SSAD development and operation cost into the hundreds of millions
  - Implementation is stagnant – no progress after four years of policy work
  - Community working to persuade ICANN to move faster and cheaper

Domain Name System (DNS) Abuse

- How is DNS abuse being defined?
  - Extremely narrowly by registries and registrars: (malware, botnets, phishing, pharming, and spam as a delivery vehicle)
  - Security expert advice: No definition ever will be suitably comprehensive
  - EU Study on DNS Abuse: “Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity.”

Domain Name System (DNS) Abuse

- How are ICANN and the ICANN community addressing DNS abuse today?
  - ICANN Org taking little action, citing community initiatives
  - Registries and registrars (“contracted parties”) have implemented voluntary measures (DNS Abuse Institute, DNS Abuse Framework)
    - Unrelated to SSAD (though SSAD access will help combat DNS Abuse)
    - Framework calls for action on contracted party-defined abuse and certain types of content abuse (e.g., CSAM, human trafficking, etc.)
    - Voluntary measures have limited effect and don’t “reach” to the bad actors

Domain Name System (DNS) Abuse

- There is increasing scrutiny of the abuse problem outside the ICANN community (e.g., EU abuse study)
- Some contracted parties are dealing with abuse proactively
    - Example: One registry reviews registrations for potential abuse, and may cancel registrations, if:
        - a name violates a third party's rights, including trademark or copyright infringement, or
        - a name is found to have been registered as a set of pattern-based registrations which have shown abusive trends

Domain Name System (DNS) Abuse

- What are desired outcomes regarding DNS abuse for brand holders?
  - Continued expansion of industry-led voluntary measures
  - Ability to have ICANN enforce against known bad actor registrars
  - Better abuse intelligence to identify and mitigate threat vectors
- What happens next?
  - Exploration of contract amendments for “universal coverage” of contracted parties
  - Brand holders should explore and create “trusted notifier” relationships between content authorities and registries and registrars

Domain Name System (DNS) Abuse

- BEST PRACTICE: What should brand holders do when reporting DNS abuse?
  - Cite DNS Abuse Framework to participating registrars and registries when you send abuse and takedown notices – you may see better results.

Domain Name System (DNS) Abuse

- Sample reporting language (available at https://blog.appdetex.com):

> As you are aware, your registry is a signatory to the DNS Abuse Framework. A copy of the framework document is available at http://www.dnsabuseframework.org/media/files/2019-12-06_Abuse%20Framework.pdf. The framework defines abuse within the scope of the registry and registrar domain name system, and provides in pertinent part: DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming and spam (when it serves as a delivery mechanism for the other forms of DNS Abuse).
>
> The registration and use of the Abusive Domain Name constitute DNS Abuse as defined in the framework. Additionally, we believe that the registration and use of the Abusive Domain Name violates your company's terms of use, the Uniform Domain Name Dispute Resolution Policy, the Computer Fraud and Abuse Act, the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), and/or the Anti-cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d). Importantly, this use causes actionable harm to [COMPANY NAME].

WHOIS Data Accuracy Scoping

- What is this effort?
  - The ICANN community recognizes that WHOIS has inaccuracies.
  - GNSO Council has not made a decision to work toward a new policy on accuracy. A working group is simply discussing the potential scope of a policy development effort.

- What is the status of the work of the Accuracy Scoping Team?
  - Difficult for all SG/CPs to agree to a definition or description of the current state of accuracy requirements.
  - Contracted parties strictly define contractual requirements
  - However, ICANN Compliance notes that requirements aren't limited to "syntactic" accuracy – registrars have a duty to cure known bad data.

WHOIS Data Accuracy Scoping

- What are anticipated next steps and timeline for completion?
  - Scoping will complete in November 2022
  - GNSO Council will decide whether to open new policy development effort

- SUGGESTION: Submit WHOIS data inaccuracy complaints to ICANN: https://icannportal.force.com/compliance/s/registration-data

“SubPro” – New gTLD Rounds

- What are the outcomes of the Subsequent Procedures (“SubPro”) policy development process?
  - Working group made hundreds of affirmations and recommendations, most of which have been approved by the GNSO Council
  - Operational Design Phase (ODP) began in January 2022
  - Board will act on recommendations following ODP
- Will new rights protection mechanisms be granted in a new gTLD round?
  - Mandatory PICs are recommended to registries
  - Affirmed: Registries must include in their agreements with registrars prohibition on harms, including trademark/copyright infringement

“SubPro” – New gTLD Rounds

- Will a new round address DNS abuse in contracts?
  - Possibly, but wider community wants abuse dealt with first
- How soon can we expect a new application round?
  - ICANN work is severely backed up and the organization is struggling with prioritization
  - Unlikely to see applications open for at least two years

Governmental Interest In DNS Outcomes

- Where are governments involved in domain name policy outcomes?
  - GDPR severely limited WHOIS access in 2018
  - EU's NIS2 Directive may help clarify WHOIS-related obligations
  - Various US state-by-state laws are in development
- Why are governments regulating with respect to the domain name system?
  - ICANN hasn't implemented a new policy since 2016
  - Cybersecurity and law enforcement authorities need access to mitigate abuse

Governmental Interest In DNS Outcomes

- What is the current role of the Governmental Advisory Committee (GAC)?
  - The GAC formally advises the ICANN Board on policy matters
  - GAC is the formal channel for governmental advice, but governments aren't hesitating to impose policy independent of GAC.
- Should brand owners become involved, and if so, how?
  - Interact with ICANN representative bodies (e.g., the Intellectual Property and Business Constituencies) within ICANN
  - Monitor legislative and regulatory developments and make your voices heard

Review of Rights Protection Mechanisms

- What is the outcome of ICANN's review of rights protection mechanisms (RPMs)?
  - Phase 1: From 2016-2020, ICANN reviewed URS, Trademark Clearinghouse, Sunrise services, Trademark Claims notices
  - Most recommendations are slight adjustments to existing procedures
  - No progress on implementation since report issued in early 2021

Review of Rights Protection Mechanisms

- What is the status of the approaching review of the UDRP (Phase 2)?
  - ICANN issued policy status report (PSR) on UDRP on March 3
  - PSR organized to help the GNSO to assess the effectiveness of the UDRP in terms of:
    - **Efficiency**: Does the UDRP provide trademark holders with a quick and cost-effective mechanism for resolving domain name disputes?
    - **Fairness**: Does the UDRP allow all relevant rights and interests of the parties to be considered and ensure procedural fairness for all concerned parties?
    - **Addressing Abuse**: Has the UDRP effectively addressed abusive registrations of domain names?
- PSR now open for comment prior to commencement of review

Additional Questions

- Questions for the panel?

Thank You!

- Faisal Shah, Founder at Appdetex
- Margie Milam, IP Enforcement & Domain Name Policy Lead at Meta
- Mason Cole, VP Partnerships & Policy at Appdetex
- Susan Kawaguchi, Registrar Operations and Enforcement Strategy at Appdetex