Competition, Consumer Trust and Consumer Choice (CCT): New Sections

New sections added to previous draft report

Competition, Consumer Trust and Consumer Choice (CCT) Review Team
27 November 2017

TABLE OF CONTENTS

1 Executive Summary

On 7 March 2017, the Competition, Consumer Choice and Trust Review Team released its draft report for public comment. A total of 24 comments were received. The team is currently in the process of reviewing them and attempting to integrate their insights into its final draft, as appropriate. Concurrent with the initial public comment period, three additional analytical efforts were underway: a discussion of parking, a survey of INTA members on the cost of the New gTLD Program to brand owners, and a study on DNS abuse in the new gTLDs. Each of these analyses has led to updates to the initial draft of the CCT Report on which the public had not yet had a chance to comment. Consequently, the decision was made to issue a draft report addendum to provide that opportunity.

Given the plethora of comments already in hand from the initial public comment period, the Review Team is currently requesting comments only on the changes wrought by the new analyses surrounding parking, brand management and DNS abuse. As stated above, the Review Team is simultaneously working to address the initial public comments and incorporate the feedback into the final report due to be released in early January 2018. For ease of reference, we ask that you include a reference to the recommendation(s) your comment(s) refer(s) to.

Finally, the Review Team would like to draw your attention to recommendation 4 related to DNS abuse. This recommendation for a DNS Abuse Dispute Resolution Policy (DADARP) procedure is the first recommendation by the CCTRT to fail to gain unanimous support from the Review Team. In fact, a significant minority of the team are associated with a "minority statement" with regards to the recommendation. The CCTRT were polled and the majority support the recommendation, particularly as it is worded as the need for a discussion. This recommendation may, or may not, make it to the final report, but the Review Team concluded it was worthy of submission for public comment. Please pay special attention to this recommendation and the justification for its suggestion when filing public comments so that the Review Team may better access the appetite of the community for such a measure. Rates of DNS abuse are unsettlingly high in some TLDs and Contract Compliance appears unable or unwilling to approach the issue holistically and a DADARP could be a solution, though it raises a number of red flags.

1.1 Parking

Given the high percentage of “parked” registrations in new gTLDs, even relative to the high percentage of parking in legacy gTLDs, the Review Team sought to understand whether this phenomenon would affect its conclusions regarding the competitive impact of the New gTLD Program. While several hypotheses as to potential impact of parking on competition were advanced, no conclusive evidence was available to support them in the near term. While the Review Team did not find definitive evidence of parking’s effect on competition, we found some differentiation between regions when it comes to parking. In particular, there appears to be more parked domains in Chinese language domains where more speculation seems to be occurring.

There may be some correlation between parking and malware distribution, but that is not as strong and indicative as the overall trend of lower malware distribution rates than those of legacy gTLDs. Nonetheless, the malware distribution rate gap between legacy and new gTLDs appears to be shrinking, and it behooves the community to further explore the correlation between parking and malware distribution.

The overall results of the Review Team's observations on parking are inconclusive and suggest the need for further research not limited to the impact of new gTLDs. Therefore, the Review Team recommends a more rigorous collection of data around various types of parking to facilitate further examination by the community of the impact of parking on competition, consumer trust and its proxy, DNS abuse.

1.2 Cost to Brand Owners

The International Trademark Association (INTA) conducted a study of its membership to begin to explore the experience of trademark holders. The Review Team examined this survey, and supplemented it with its own analysis. Despite the relatively low number of respondents, the INTA survey offers some interesting findings with respect to brand owners. The survey found that "new TLD registrations primarily duplicate legacy TLD or ccTLD registrations" and, in particular that only 17% of respondents had registered names in the new gTLDs for the first time in new gTLDs versus duplicating existing domains in legacy gTLDs or ccTLDs. This suggests that defensive registrations remain an issue in the New gTLD Program. While one of the stated purposes of the New gTLD Program was to create greater choice for brand owners, the overwhelming rationale for domain registration by brands appears to be defensive.

However, the survey also indicates that the expansion of the New gTLD Program has made defensive registrations a less efficient means of protection. Accordingly, monies have shifted to alternatives and expanded monitoring.

Furthermore, the survey reveals that more than 75% of cases involve privacy and proxy services, which suggests the need for further research.

Finally, there is an indication that enforcement costs have increased in the new domains, which suggests there is greater infringement in those new domains than in legacy gTLDs and ccTLDs.

The INTA survey suggests that, at the very least, further research is necessary, perhaps with a simplified survey with more respondents. But it is clear that brand owners have experienced some frustration with the New gTLD Program and the rights protection mechanisms that have been put in place.

1.3 DNS Abuse

To the extent possible, the CCTRT has sought to measure the effectiveness of the technical safeguards developed for the New gTLD Program in mitigating various forms of DNS abuse. As part of this process, the CCTRT commissioned a comprehensive DNS abuse study to analyze levels of technical abuse in legacy and new gTLDs to inform this review and potentially serve as a baseline for future analysis.

Generally, the DNS Abuse Study indicates that the introduction of new gTLDs did not increase the total amount of abuse for all gTLDs. Nonetheless, the results demonstrate that the nine aforementioned safeguards alone do not guarantee a lower rate of abuse in each new gTLD compared to legacy gTLDs. Instead, factors such as registration restrictions, price, and registrar-specific practices seem more likely to affect abuse rates.

The results of the study indicate that the introduction of new gTLDs has corresponded with a decrease in the number of spam associated registrations in legacy gTLDs, while malicious registrations have increased in new gTLDs

It is the conclusion of the report and the Review Team that existing safeguards do not represent sufficient protection against DNS Abuse and that creative solutions need to be evaluated. We welcome public comment on those submitted.

2 CCT Review Team Recommendations

Recommendations are summarized in this table. The full recommendation, with related findings and rationale, may be found in the cited chapters.

- **Prerequisite or Priority Level**: Per the ICANN Bylaws, the CCT Review Team indicated whether each recommendation must be implemented prior to the launch of subsequent procedures for new gTLDs. The Review Team agreed that those recommendations that were not categorized as prerequisites would be given a time-bound priority level:
- **High priority**: Must be implemented within 18 months of the issuance of a final report
- **Medium priority**: Must be implemented with 36 months of the issuance of a final report
- **Low priority**: Must be implemented prior to the start of the next CCT Review

#	Recommendation	To	Prerequisite or Priority Level
Chapter 3. Competition			
3	Collect parking data.	ICANN organization	High
Chapter 4. Consumer Choice			
9	Conduct periodic surveys of registrants.	ICANN organization	Prerequisite
Chapter 5. Safeguards			
A	Consider directing ICANN org, in its discussions with registries, to negotiate amendments to existing Registry Agreements, or in negotiations of new Registry Agreements associated with subsequent rounds of new gTLDs to include provisions in the agreements providing incentives, including financial incentives for registries, especially open registries, to adopt proactive anti-abuse measures.	The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization and the Subsequent Procedures PDP WG	High
B	Consider directing ICANN org, in its discussions with registrars and registries to negotiate amendments to the Registrar Accreditation Agreement and Registry Agreements, to include provisions aimed at preventing systemic use of specific registrars for technical DNS abuse.	The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization and the Subsequent Procedures PDP WG	High
C	Further study the relationship between specific registry operators, registrars and DNS abuse by commissioning ongoing data collection, including but not limited to, ICANN Domain Abuse Activity Reporting (DAAR) initiatives. This information should be regularly published for transparency purposes in order	The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting	High

	to identify registries and registrars that need to come under greater scrutiny and higher priority by ICANN Compliance. Upon identifying abuse phenomena, ICANN should put in place an action plan to respond to such studies, remediate problems identified, and define future ongoing data collection.	Organization and the Subsequent Procedures PDP WG, SSR2 Review Team.	
D	A DNS Abuse Dispute Resolution Policy ("DADRP") should be considered by the community to deal with registry operators and registrars that are identified as having excessive levels of abuse (to define, e.g. over 10% of their domain names are blacklisted domain names). Such registry operators or registrars should in the first instance be required to a) explain to ICANN Compliance why this is, b) commit to clean up that abuse within a certain time period, and / or adopt stricter registration policies within a certain time period. Should ICANN not take any action themselves, a DADRP can be invoked.	The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization, the Subsequent Procedures PDP WG and the SSR2 Review Team	High
40	An Impact Study in order to ascertain the impact of the New gTLD Program on the cost and effort required to protect trademarks in the DNS should be repeated at regular intervals to see the evolution over time as the New gTLD Program continues to evolve and new gTLD registrations increase. We would specifically recommend that the next Impact Survey be completed within 18 months after issuance of the CCTRT final report, and that subsequent studies be repeated every 18 to 24 months. The CCTRT acknowledges the fact that this was carried out in 2017 by Nielsen surveying INTA members and we encourage that to continue noting that the study needs to be more user friendly.	ICANN Organization	High
41	A full review of the URS should be carried out and consideration be given to how it should interoperate with the UDRP. However, given the PDP Review of All RPMs in All gTLDs, which is currently ongoing, such a review needs to take on board that report when published and indeed may not be necessary if that report is substantial in its findings and if the report fully considers potential modifications.	Generic Names Supporting Organization	Prerequisite
42	A cost-benefit analysis and review of the TMCH and its scope should be carried out to provide quantifiable information on the costs and benefits associated with the present state of the TMCH services and thus to allow for an effective policy review.	Generic Names Supporting Organization	Prerequisite

3 Competition

3.1 Potential Impact of "Parked" Domains on Measures of Competition.

Overall, in our discussion of the impact of new gTLDs on competition, we treat all domains as equal. However, it is worth noting that the majority of domains in both legacy and new gTLDs are not the primary identifiers of typical websites. Instead, these domains are forwarded to other domains (including sub-domains), used only for email, monetized via advertising or simply do not resolve, perhaps held in reserve by speculators or as premium domains by registries. For a high-level impact assessment, these domains, for lack of a better term, were considered "parked" by the Review Team. The Review Team simply attempted to consider if rates of these activities differed between legacy and new gTLDs and, if so, whether the difference suggests the need for further research. Our conclusion is that while further research is ideal, the context of the new gTLD program might not be the right fit. Using an expansive definition of parking, according to data compiled by nTLDstats, about 68% of registrations in new gTLDs are currently parked.[1] By way of comparison, 56% of registrations in legacy gTLDs are currently parked. Halvorsen et al ascribe parking to: (1) speculation in order to sell the domain later at a profit; (2) plans to develop the domain at a later date; or (3) unsuccessful development.[2]

Examples of behaviors that could be considered parking include:

- The domain name does not resolve.
- The domain name resolves but attempts to connect via HTTP return an error message.
- HTTP connections are successful but the result is a page that displays advertisements, offers the domain for sale, or both. These pages may also be used as a vector to distribute malware.
- The page that is returned is empty or otherwise indicates that the registrant is not providing any content.
- The page that is returned is a template provided by the registry with no customization offered by the registrant.
- The domain was registered by an affiliate of the registry operator and uses a standard template with no unique content.
- The domain redirects to another domain in a different TLD.

Of course, this represents a rather gross representation of "parking" as the implications for competition of each of these scenarios are likely different. Future research will require analyzing each of these categories individually to determine the impact on competition.

However, because the percentage of "parked" registrations in new gTLDs is so large, the Review Team sought to understand whether this phenomenon would affect its conclusions regarding the impact of the introduction of new gTLDs on the marketplace and thereby justify further research. Hypotheses could be advanced which suggest counting certain types of parked domains differently when computing market share and concentration. For example, one possible reason for taking parking rates into account is that registration renewal rates may be negatively correlated with rates of certain types of parking so that the current market

[1] "Parking in new gTLDs Overview" (viewed 21 March 2017), https://ntldstats.com/parking/tld
[2] T. Halvorson, M.F. Der, I. Foster, S. Savage, L.K. Saul, and G.M. Voelker, "From .academy to .zone: An Analysis of the New TLD Land Rush," Proceedings of the 2015 ACM Conference on Internet Measurement.

shares of TLDs with relatively high parking rates may overstate their long run competitive significance. For example, some early registrations in a new gTLD are the result of "land rush" behavior by speculators. Furthermore, there was an initial spike in registrations from China in both legacy and new gTLDs, some of which is the result of speculation and some the result of regulations that may change over time. Finally, differential pricing between initial registration and renewal could have a significant impact on renewals.[3] In such an instance, these new domains should be discounted at a rate commensurate to the correlation. In other words, if speculative registrations are isolated and determined to be half as likely to be renewed, their numbers should be discounted 50% in any calculation of market share and market concentration. Of course, one must leave room for the possibility that speculative behavior is fundamentally different between new and legacy gTLDs with established market expectations. Another hypothesis posits that domains used as pointers imply a transition away from an existing domain. In other words, a pointer could be an indication of provisional acceptance of a new gTLD by the market and the old domain is being maintained in the near term purely to smooth a transition. In this case, the domains to which others are pointed should be discounted at some rate. Of course, there are instances when redirects simply represent "over registration" either to capture typos and guesses, or protect brand identity. Future analysis of redirects would require determining which domain is being used to promote the site. Finally, it's possible that speculation has a pro-competitive effect, not captured directly by market share and concentration calculations, by bridging new entrants to maturity, which generally takes 3-5 years. Given the mandate to examine the impact of new gTLDs on competition, the first question is whether the rate of parking is substantially different in the new gTLDs than in the legacy gTLD space.

In order to better understand this topic, the Review Team used existing parking data for new gTLDs that nTLDstats routinely calculates. We also requested that ICANN contract with nTLDstats to develop parking data for legacy gTLDs especially for this project.[4] We used registration data for December 2016, the same month for which other statistics in this report are based, and the most comprehensive parking measure provided by nTLDstats, the aggregate of the 7 separate sources of parking that it identifies.[5]

Using this data, we made an initial comparison of overall parking rates between legacy and new gTLDs. nTLDstats estimated that the weighted average parking rate for legacy gTLDs in that month was approximately 56 percent and that the weighted average parking rate for new gTLDs in the same month was approximately 68 percent, a rate that is almost 20 percent higher than the parking rate for legacy gTLDs.[6] Again, we are not certain of the impact of parked domains on market rivalry but if parked domains are somehow less significant as markers of competition, this is a substantial difference that could affect the computation of our competition-related indicators.[7]

[3] For example, initial pricing on XYZ was free in many instances but renewal was full price.
[4] nTLDstats applied its parking analysis to each legacy gTLD based on the number of names in its zone file. For TLDs with 10,000 names or fewer, nTLDstats analyzed all registered names, for TLDs with 10,001-100,000 names, nTLDstats analyzed 10% of registered names, and for TLDs with more than 100,000 names, nTLDstats analyzed 1% of registered names. nTLDstats also conducted a manual review of 10% of the total sample to check for false positives.
[5] Specifically, we adjusted the number of registrations for each gTLD to reflect the number of registrations that were not parked, i.e., we calculated (1 minus the parking rate) times the number of registrations for each gTLD. 20 percent of 55.6=11.2 and 55.6 + 11.12= 66.72 (nearly 68%).
[7] At one extreme, if we were to exclude parked registrations from our market share analysis entirely, we find a "non-parked" market share of new gTLD registrations as a portion of all gTLDs of 10.9 percent, approximately 23 percent lower than the 14.2 percent share when parked domains are included. (Making a similar adjustment in our market concentration calculations did not make a meaningful difference between including or excluding parked domains.)

Taking a cursory stab at understanding the potential significance of parking rates on future market shares, we attempted to determine whether there was a relationship between parking and renewal rates. In order to perform this analysis, we compared parking rates in each TLD as of December 2016 with a renewal rate computed based on registries' monthly transaction reports[8] for the period of July – December 2016[9]. Using a Pearson correlation analysis, we were unable to find a statistically significant correlation between renewal rates and parking rates in either new or legacy gTLDs. While the identification of a relationship would have been interesting, the results of this test are, by no means, dispositive of a potential correlation. We recommend more robust studies of this topic to better understand whether such a relationship exists. Such studies could include, among other things, a closer examination of the following factors: 1) what parking measures best measure market rivalry; 2) what renewal rates should be used; 3) what factors other than parking are likely to affect renewal rates; 4) what is the functional form (e.g., linear, logarithmic, etc.) of the relationship between parking and renewals; 5) what is the "lag" between parking and non-renewals (i.e., how much time is there between the time that a domain name is parked and the time at which it is not renewed)?

3.2 Geographic Differences in Parking Behavior

The Review Team also sought to determine whether the quantity of parked domains varied based on region. For example, Latin American and Caribbean DNS Marketplace Study (LAC Study) reports that "across the entire region, 78% of the gTLD domain names are active, and 22% are not in use (either timing out, or no active services).[10] By comparison, according to nTLDstats, across all new gTLDs approximately 33% of domains had no valid DNS or returned invalid HTTP responses.

Although the Review Team did not have the ability to directly correlate registrant addresses with parked domains, we did identify six of the top 50 largest new gTLDs including TLDs operated by registries based in China showing markedly higher parking rates than the average across all new gTLDs, with parking rates ranging from 85% for .wang to 98% for .xin. Table A[11] below indicates the parking rate for each of the six:

	Parking Rate (%)
All New gTLDs	68 %
.XIN	97.77%
.WANG	85.08%
.TOP	85.08 %
网址 (xn--ses554g)	83.22%
.REN	82.82%

[8] Registries do not submit a renewal rate calculation to ICANN. Nevertheless, given that second level domains auto-renew, we computed a renewal rate for each TLD by dividing the number of renewal transactions by the sum of the deletion transactions (outside of the add grace period) plus renewal transactions.
[9] Monthly renewal rates can be quite volatile and represent only the portion of domains eligible for renewal that month, whereas parking rates are calculated across all domains in a TLD. Therefore, we used a six-month period to calculate renewal rates in order to minimize sample errors in our analysis.
[10] Oxford Information Labs, LACTLD, EURid and InterConnect Communications, Latin America and Caribbean DNS Marketplace Study (September 2016), accessed 23 October 2017, https://www.icann.org/en/system/files/files/lac-dns-marketplace-study-22sep16-en.pdf
[11] NTLDStats.com (accessed on 3 March 2017): Parking Analysis of Legacy gTLDs, https://community.icann.org/display/CCT/Studies%2C+Research%2C+and+Background+Materials?preview=/56135378/64074447/ICANN%20Parking%20Check.xlsx

According to data from nTLDstats, there were over 9 million registrations made in new gTLD strings that have their origin in China.[12] One possible reason for the higher levels of parking rates seen in new gTLDs that cater to Chinese registrants may be speculative domain registrations out of China, particularly with regard to short domain names (i.e., names containing five or less letters or numbers). In 2015, Chinese investors purchased a large number of short domain names as these were seen as especially interesting to Chinese investors.[13] Furthermore, it seems that Chinese buyers are also purchasing names with actual end-uses in mind that they think will go up in value. As a result, the increase in awareness of domain investment in China may have contributed to higher parking rates of Chinese based new gTLDs. This trend may also be indicative of a speculative bubble in the Chinese market as well as expected value of these domains.

These initial analyses of geographically-based parking rates are quite cursory and based on limited data, but they do seem to indicate that regional variations in parking rates exist and can be quite significant. Again, these figures represent a gross measurement of parking and future analysis will require a more granular exploration of behavior across geographic regions.

3.3 Relationship Between Parking and DNS Abuse

While the Review Team was not able to identify a direct relationship between parking rates and either competition or consumer choice, we also considered the possibility that parked domains may be linked to Consumer Trust, and in particular to the possibility that parking is associated with DNS Abuse. Previously, Vissers et al[14] studied over eight million parked domains and found that "users who land on parked websites are exposed to malware, inappropriate content, and elaborate scams."[15]

In conjunction with this Review, the "Statistical Analysis of DNS Abuse in gTLDs" study conducted for this report found that, in general, in new gTLDs the total number of registrations associated with malware is lower than in legacy gTLDs.[16] Whereas, the rate of malware associated domain names per volume in new gTLDs is occasionally higher than that of legacy gTLDs. However, if you look amongst the new gTLDs and look at parking rates, you'll see that of the malware that's occurring, it's marginally more likely to occur in

[12] NTLDStats.com (accessed on 31 October 2017): Parking Analysis of Legacy gTLDs, https://community.icann.org/display/CCT/Studies%2C+Research%2C+and+Background+Materials?preview=/56135378/64074447/ICANN%20Parking%20Check.xlsx

[13] Echo Huang, "China's newest investment craze is short domain names," Quartz, 10 January 2016, accessed 30 October 2017, https://qz.com/581248/chinas-latest-investment-craze-is-short-domain-names/

[14] Vissers, Joosen, and Nikiforakis, " Parking Sensors: Analyzing and Detecting Parked Domains," (paper presented at NDSS, San Diego, USA, 8-11 February 2015). http://dx.doi.org/10.14722/ndss.2015.23053

[15] It is not entirely clear to the Review Team whether malware propagation is intentional by the parked sites or parking services, or the result of compromised ad networks. Vissers et al raise this possibility in their paper: "Possibly, these complex chains are the consequence of a process similar to ad arbitration, a widely adopted practice performed by most ad syndicators [33]. During this process, the syndicator bids on available ad slots of other publishers or syndicators, allowing them to resell these slots to the next bidder. Often, ad slots are subjected to multiple iterations of this reselling process. As a consequence, ad slots are no longer under control of the syndicator that the original publisher partnered with. All these interactions and intermediate parties have the potential to blur the direct involvement of the parking service in serving malware. In some cases, however, we also see malware being delivered more directly, for example, by the parent company of Parking Service 8."

[16] SIDN Labs and the Delft University of Technology (August 2017), Statistical Analysis of DNS Abuse in gTLDs Final Report, accessed 23 October 2017, https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

zones with higher parking rates. There may be some correlation between parking and malware, but that is not as strong and indicative as the overall trend of lower malware distribution rates than those of legacy gTLDs. Nonetheless, the malware distribution rate gap between legacy and new gTLDs appears to be shrinking, and it behooves the community to further explore the correlation between parking and malware distribution.

3.4 Recommendations

While we observe that new gTLDs have higher parking (using the broadest possible definition) rates than legacy gTLDs and that there are regional variations in parking rates, it is so far unclear to us if parking has a meaningful effect on either competition or consumer choice. As a result, we recommend that ICANN consider undertaking further research into the potential competitive impact of domain parking and to use the results of that research to improve its analysis of developments in the DNS marketplace. In addition, we recommend that ICANN consider using data on upcoming registration deletes for the same purpose.

Recommendation 5: Collect parking data.

Rationale/related findings: The high incidence of parked domains suggests an impact on the competitive landscape, but insufficient data frustrates efforts to analyze this impact.

To: ICANN organization

Prerequisite or Priority Level: High

Consensus within team: Yes

Details: ICANN should regularly track the proportion of TLDs that are parked with sufficient granularity to identify trends on a regional and global basis. Future reviews should conduct further analyses of whether there is a correlation between parked domains and renewal rates or other factors that may affect competition. Further analysis should be performed on the relationship between parking and DNS abuse.

Success Measures: The availability of relevant data for use by the ICANN organization, contractors and the ICANN community for its work in evaluating competition in the DNS space.

4 Consumer Choice

The Review Team also considered the question of whether the introduction of new gTLDs increased the choices available to registrants. As discussed previously in this report, the expansion of the program gives registrants new options in terms of new languages, character sets, geographic identities, and new specialized categories. However, we sought to establish whether registrations in the new gTLDs represented a positive choice available to registrants or if a significant number felt obliged to register defensively in new gTLDs to protect their brand or identity. In particular, there has been considerable discussion of whether trademark holders would find it necessary to register those trademarks as domain names in new gTLDs in order to prevent others from doing so.

There have been a number of studies (see below) of the extent to which registrants have engaged in such "defensive" registrations. In anticipation of this Review, ICANN commissioned Nielsen to perform the Global Registrant Survey to gain insights from registrants. More recently, INTA conducted a study of its membership, which reflects the experience of trademark holders. The Review Team examined each of these studies, and supplemented them with our own analysis. We initially address the general topic of consumer choice and then perform a specific analysis related to trademark holders below.[17]

In evaluating these results, it is important to note that not all instances of duplicate registrations are necessarily "defensive" in nature. For example, a trademark holder might register the same mark in multiple domains in order to increase the probability that it will be found through user searches, a consideration that has become increasingly important as the number of domains has grown.[18] In fact, a total of 52% of registrants interviewed by Nielsen gave as one of the reasons for registering duplicate domain names "To help ensure my site gets found in searches."[19] However, 51% of the respondents indicated that they engaged in duplicate registrations "to protect my brand or organization name" and the same percentage gave as one of the reasons "to keep someone else from having a similar name."[20] The INTA Survey found that "new TLD registrations primarily duplicate legacy TLD or ccTLD registrations"[21] and, in particular, that only 17% of respondents had registered names in the new gTLDs for the first time versus duplicating existing domains in legacy gTLDs or ccTLDs. Thus, it appears that "defensive" registrations are a real phenomenon, apparently because the costs of challenging registrations by others can be considerably greater than the costs of registering their marks in multiple domains.[22]

4.1 Previous Studies

Krueger and Van Couvering surveyed 1,043 brand names of Fortune 100 companies and

17 In this chapter, the term consumers is used primarily to refer to domain name registrants and not consumer end-users, whose behavior and beliefs are largely covered in the Consumer Trust chapter.

18 Consider users that search for web sites by guessing Internet addresses. As the number of TLDs increases, finding the "correct" website by guessing becomes more difficult and, on average, the number of required guesses is substantially increased. Faced with this fact, one would expect that some "guessers" would use search engines more frequently than in the past. However, some registrants may still choose to register in several TLDs in order to reduce the number of guesses that a user must make in order to find them.

19 Nielsen, Registrant Survey Wave 2 (2016), p. 13.

20 Ibid. Many registrants chose both responses; a total of 60% of registrants of new gTLDs selected one of the two responses. It is worth noting that at least some respondents indicated that they were both registering domains to be more likely to be found in search and either to protect their brand or to prevent others from registering the name, indicating that it may not always be possible to categorize a registration as strictly "defensive" or not.

21 INTA Survey, Slide 19

22 Appendix G: Bibliography includes a series of questions that may be included in future surveys of domain name registrants to better understand the choices they make when registering domain names.

found the following registration percentages: (1) 100% in .com; (2) 76% in .org; (3) 84% in .net; (4) 69% in .info; (5) 65% in .biz and (6) 57% in .mobi.[23] Zittrain and Edelman found that, six months after open registration in .biz began, 91% of a sample of .biz domain names were also registered in .com, 63% were also registered in .net, and 49% were also registered in .org.[24] Strategies International analyzed the extent of duplicate name registrations and the presence of the same registered name holder between four of the then-new and three legacy TLDs and found that: "The statistics for .info indicate that only 11% of registrants hold the same name in .com, which suggests that .info has created significant new opportunities. With .biz, 42% of duplicate registrations appear to be registered to the same party, thereby suggesting that they are protective in nature."[25] Katz, Rosston, and Sullivan analyzed the overlap in domain registrations for 200 of the top 500 global brands as ranked by Brand Finance and found "that a very high percentage of them were registered in the different TLDs" that they examined.[26] However, they also found "a big range in the share of registered domains with content" and that the percentage of active sites "was quite low" except for .com. Finally, Halvorson et al, who employ a variety of measures to identify matches of registrants between .com and .biz, found "at least some degree of a match for around 40% of the [biz-com] pairs [they] could assess."[27] Using what they describe as "stronger indicators", they classified 11.6% of biz domains as "defensive."

4.2 CCTRT Analysis

The Global Registrant Survey, Wave 2, found that 35% of all surveyed registrants had registered at least one name in a new gTLD.[28] Of those, 60% indicated that they had registered to "protect existing domain(s) and ensure no one else got a domain similar" while 34% indicated that they registered to "appeal to new Internet users or new types of customers" and 6% registered because the "name I wanted was not available using older gTLDs."

We also performed an analysis of strings registered as second level domains in new gTLDs and comparable strings registered in .com, which is currently by far the most popular of the legacy gTLDs. Our analysis focused on two potential patterns. In the first case, we looked to see if the *identical string* registered as a second level domain in a new gTLD was registered as a second level domain in .com (e.g., if example.tld was registered, was example.com also registered?)[29] We found that 82% of registrations in new gTLDs had identical matches in .com. However, there was considerable variation in the percentages of identical matches across gTLDs. For example, among 414 gTLDs with at least 1000 registrations, 32 had at least 99% of their second level domains as exact matches in .com, including both .wang and .xin which are the third and eleventh largest new gTLDs in registration volumes, as of November 2016; and nearly two-thirds (271) had at least 95% of

23 F. Krueger and A. Van Couvering, "An Analysis of Trademark Registration Data in New gTLDs," Minds + Machines Working Paper, (2010-02): 51.

24 Berkman Center for Internet and Society Harvard Law School, Survey of Usage of the .biz TLD (June 2002), accessed 25 January 2017, https://cyber.law.harvard.edu/tlds/001/

25 Summit Strategies International, Evaluation of the New gTLDs: Policy and Legal Issues (July 2004), accessed 25 January 2017, 102. Same Registered Name Holder in .com/.net/.org, at 102 It is important to note, however, that the authors point out that "The data…is based on an extremely small sample of only 100 names for .biz and .info." This study was prepared for ICANN.

26 M.L. Katz, G.L. Rosston, and T. Sullivan, Economic Considerations in the Expansion of Generic Top-Level Domain Names, Phase II Report: Case Studies (December 2011), accessed 25 January 2017, https://archive.icann.org/en/topics/new-gtlds/phase-two-economic-considerations-03dec10-en.pdf, p. 61. These domains were .com, .net, .org, .biz, .info, .mobi, and .us. This study was prepared for ICANN.

27 T. Halvorson, J. Szurdi, G. Maier, M. Felegyhazi, C. Kreibich, N. Weaver, K. Levchenko, and V. Paxon, "The BIZ Top-Level Domain: Ten Years Later" in Passive and Active Measurement, eds N. Taft and F. Ricciato. (Germany: Springer Berlin Heidelberg, 2012), 221-230, 228. http://www.icir.org/vern/papers/dot-biz.pam12.pdf

28 Nielsen, Registrant Survey Wave 2 (2016), p. 164.

29 Analysis Group, Summary of Trademark Strings Registered in Legacy gTLDs Trademark Strings that are also Brand TLDs (October 2016), accessed 25 January 2017, https://community.icann.org/download/attachments/56135378/New%20gTLD%20Registrations%20of%20Brand%20TLD%20TM%20Strings%2010-18-16.pdf?version=1&modificationDate=1481305785167&api=v2

their second level domains as exact matches in .com. At the other extreme, 10 gTLDs had fewer than 50% of their second level domains as exact matches in .com. Of these, half were IDNs. In general, IDN gTLDs contained fewer identical matches to .com, with only about 70% of registrations in IDN gTLDs being identical matches to domains in .com. Unfortunately, because our analysis did not include WHOIS data we were unable to determine whether the same registrant had registered both domains.
In a second analysis, we examined whether the *combined string* representing both the TLD and the SLD was registered as a second level domain in .com (e.g., if example.tld was registered, was exampletld.com also registered?) In this analysis, we found that only 8% of registrations in the new gTLDs were also registered in .com in the combined form.

Overall, we conclude that while some registrants are motivated by defensive objectives in the new gTLDs, many registrants choose to register in new gTLDs to broaden the appeal or reach of their offerings even when similar options remain available in legacy gTLDs.

4.3 CCTRT Analysis: Trademarks

The INTA Survey indicated that amongst its respondents of trademark holders, "nearly all of the new domains registered as duplicates to a Legacy or ccTLD were intended primarily to prevent the name from being used by another registrant."[30] In order to better understand the prevalence of these defensive registrations by trademark holders, we, together with Analysis Group, used data from the most recent "round" of new gTLDs to analyze the same issue. Specifically, we began by identifying a number of trademarks for which one might expect some degree of "defensive" registrations together with the identity of the registrant. The data collected by Analysis Group were a 25% random sample of trademark holders that were obtained from a database administered by Deloitte that contains all recorded trademarks in the Trademark Clearinghouse Database. Identities of registrants were obtained from the WHOIS domain registration database.[31] The trademark strings analyzed were limited to verified or corrected Latin text strings in the Trademark Clearinghouse. Matches were identified as those involving an exact match in accordance with ICANN's matching criteria where the registrant was identified as the trademark holder associated with the registered string based on an approximate text comparison between registrant and trademark holder names.

Using these data, we determined: (1) whether each of the trademarks in our data was registered by the trademark holder in at least one legacy gTLD; (2) whether the same string was registered by the trademark holder in at least one new gTLD and (3) for those strings that were registered by the trademark holder in at least one new gTLD, the number of new gTLDs in which the trademark holder had registered the string. We found that 54% of the strings that were registered in a legacy gTLD were also registered in at least one new gTLD. We also found that, of these strings, 3 was the median number of registrations in new gTLDs. That is, half of the trademarks that were analyzed were registered in 3 or fewer new gTLDs.[32] We also found that three-quarters of these strings were registered in 7 or fewer new gTLDs and that 90% of these strings were registered in 17 or fewer new gTLDs.[33] At the same time, a small number of trademarked strings were registered in a large number of

30 INTA Survey, Slide 22

31 Analysis Group, Independent Review of Trademark Clearinghouse (TMCH) Services Draft Report (July 2016), accessed 25 January 2017, https://newgtlds.icann.org/en/reviews/tmch/draft-services-review-25jul16-en.pdf

32 The mean number of duplicate registrations was 8 but statistic is strongly influenced by a small number of trademarks that were registered in a very large number of domains. For example, one trademark was registered in 406 domains.

33 In assessing these findings, it is important to emphasize that the extent of duplicate registrations that we observe may have been influenced, to some degree at least, by the use by trademark holders of the blocking services described above. That is, to the extent that trademark holders obtained protection through blocking, they may have had less need to register their trademarks "defensively."

TLDs: 4% of trademarks were registered in at least 100 new gTLDs, and one was registered in 406 new gTLDs. Extrapolating the sample across all marks, we would expect that trademark holders would have made approximately 80,000 total registrations of their trademarks in new gTLDs as of September 2016, which represents 0.3% of all registrations within new gTLDs[34]. We conclude from this analysis that, although the direct cost of the New gTLD Program for most trademark holders related to defensive registrations appears to be lower than some had feared prior to the inception of the program, a small fraction of trademark holders are likely incurring significant costs.

In addition to defensive registrations, some registries offer a service through which a trademark owner can block others from using its marks without the need to purchase the domain name itself. For example, Rightside offers what it describes as "a cost-effective one-step, registry-wide solution to protecting your client's trademarks against cybersquatting…with our Domain Protected Marks List (DPML)" as an alternative to having "to defensively purchase trademarks and trademarks + terms on every TLD…." [35] Similarly, Donuts notes that its "Domains Protected Marks List (or DPML) protects trademark holders against cybersquatting at a fraction of the cost of defensively and individually registering the terms across all Donuts domains."[36] At the time of publication, we did not have any data related to the costs incurred by trademark holders making use of these blocking services, although we expect to obtain more information prior to the publication of our final report.

Recommendation 9: Conduct periodic surveys of registrants.

Rationale/related findings: The inability to determine registrant motivations and behavior frustrates efforts to study competition and choice in the TLD marketplace.

To: ICANN organization

Prerequisite or Priority Level: Prerequisite

Consensus within team: Yes

Details: The survey should be designed and continuously improved to collect registrant trends. Some initial thoughts on potential questions is in the previous draft report - Appendix F: Possible Questions for a Future Consumer Survey.

34 The TMCH review found a total of 19,642 registrations by trademark holders of their mark using a 25% sample. Extrapolating this to 100% gives us an expected total of 78,568 total registrations. In comparison, as of September 2016 there were a total of 24,814,734 registrations across all new gTLDs.

35 Rightside Registry, "DPML," accessed 21 September 2016, http://rightside.co/registry/dpml/

36 Donuts Registry, "DPML," accessed 21 September 2016, http://www.donuts.domains/services/dpml. According to domainname.com: "Three of the largest new top-level domain registries has [sic] created a new domain name blocking tool. Many clients prefer to avoid defensive registrations but these services offer some economies of scales and are worth considering for key brands. The service is offered by three new gTLD providers; Donuts (covering 172 TLDs) Rightside (covering 36 TLDs) and Minds + Machines (covering 16 TLDs) The blocking tool allows trademark owners to block their marks and related terms, at the second level, in all supported new gTLDs, for one fee per registry. The service is designed to be an economical way for trademark owners to protect their rights from cybersquatters. With the block it is not necessary for trademark owners to take out defensive registrations in each of the three providers TLDs In order to obtain a block, the term you want to block must be based on a trademark validated by the Trademark Clearinghouse."

"Cost Efficient Domain Name Protection!" Domain Info, 4 November 2015, accessed 28 September 2016, http://domainincite.com/21404-icann-retires-affirmation-of-commitments-with-us-gov

Recently, Donuts announced a new version of its blocking service that will allow brand owners the opportunity to obtain blocking in return for a fee of $10,000. [Jack Jack Elis, "Donuts unveils enhanced trademark protection offering; expert urges lower cost options in next gTLD round," World Trademark Review, 29 September 2016, accessed 29 September 2016, http://www.worldtrademarkreview.com/blog/Detail.aspx?g=fa934d21-cfa7-459c-9b1f-f9aa61287908

5 Safeguards

5.1 DNS Abuse

The accessibility of domain names as unique global identifiers has made them conduits of innovative technologies, including those used for malicious purposes. Consequently, bad actors misuse these universal identifiers for cybercrime infrastructure[37] and directing users to websites enabling other forms of crime, such as child exploitation, intellectual property infringement, and fraud. Each of these activities may constitute a form of DNS abuse. However, determinations depend largely upon local laws, the roles played by other infrastructure providers, and subjective interpretations. Nonetheless, greater consensus exists on many technical forms of DNS abuse as demonstrated by community findings associated with the development of the New gTLD Program.

Due to the misuse of domain names, the community initially expressed concerns about whether the vast expansion of available gTLDs would result in increased DNS abuse. The CCTRT was tasked with examining issues associated with the expansion of the DNS, including the implementation of safeguards designed to preempt identified risks.[38] Prior to the approval of the New gTLD Program, ICANN invited feedback from the cybersecurity community on DNS abuse and the risks posed from the expansion in the DNS name space.[39] The community identified the following areas of concern:

- How do we ensure that "bad actors" do not run registries?
- How do we ensure integrity and utility of registry information?
- How do we ensure more focused efforts on combating identified abuse?
- How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?[40]

[37] Bursztein et. al., "Framing Dependencies Introduced by Underground Commoditization," (paper presented at the proceedings of the 2015 Workshop on the Economics of Information Security, Delft, Netherlands, 22–23 June 2015), https://research.google.com/pubs/pub43798.html, p. 12.

[38] The US Department of Commerce and ICANN Affirmation of commitments specifies "malicious abuse issues" as one of the issues to be analyzed prior to expanding the top-level domain space. Furthermore, the AoC requires the CCT Review Team to analyze the "safeguards put in place to mitigate issues involved in the introduction or expansion" of new gTLDs. Consequently, the CCT Review Team Terms of Reference define the work of the team to include a review of the "effectiveness of safeguards" and "other efforts to mitigate DNS abuse." Furthermore, the GAC's 2015 Buenos Aires Communiqué requested "that the ICANN community creates a harmonised methodology to assess the number of abusive domain names within the current exercise of assessment of the New gTLD Program." See https://gacweb.icann.org/download/attachments/27132037/BA%20MinutesFINAL.pdf?version=1&modificationDate=1437483824000&api=v2; Likewise, the 2015 Dublin Communiqué requested that the ICANN Board "develop and adopt a harmonized methodology for reporting to the ICANN community the levels and persistence of abusive conduct...that have occurred in the rollout of the New gTLD Program." See https://gacweb.icann.org/display/GACADV/2015-10-21+gTLD+Safeguards+%3A+Current+Round

[39] "ICANN (3 October 2009), *Mitigating Malicious Conduct*, accessed 9 November 2016, https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf. Feedback came from groups such as the Anti-Phishing Working Group (APWG), Registry Internet Safety Group (RISG), the Security and Stability Advisory Community (SSAC), Computer Emergency Response Teams (CERTs), the banking/financial and wider Internet security communities.

[40] Ibid.

Based on the community's feedback, ICANN identified several recommendations for safeguards aimed at mitigating these risks.[41] Nine safeguards were identified and recommended:

- Vet registry operators
- Require Domain Name System Security Extension (DNSSEC) deployment
- Prohibit "wildcarding"
- Encourage removal of "orphaned glue" records[42]
- Require "Thick" WHOIS records
- Centralize Zone File access
- Document registry- and registrar-level abuse contacts and policies
- Provide an expedited registry security request process
- Create a draft framework for a high security zone verification program[43]

The CCTRT was tasked with analyzing the effectiveness of the nine recommended safeguards. To the extent possible, the CCTRT assessed the effectiveness of each of these safeguards using available implementation and compliance data.[44] The CCTRT examined the implementation of each. Additionally, the CCTRT commissioned a quantitative DNS abuse study to provide insight into the relationship, if any, that may exist between levels of abuse and implemented safeguards in the new gTLD name space.[45]

With regard to the first safeguard, vetting registry operators, all new gTLD applicants were required to provide full descriptions of the technical back-end services that they would use, even where these services were subcontracted, as part of the application process. This was an initial evaluation to ensure technical competence. These descriptions were evaluated only at the time of application.[46] Additionally, all applicants were required to pass Pre-Delegation Testing (PDT).[47] PDT included comprehensive technical checks of Extensible Provisioning Protocol (EPP), Name Server setup, Domain Name System Security Extensions (DNSSEC), and other protocols.[48] Applicants were required to pass all of these tests before a domain name would be delegated.

Upon delegation, registry operators were required to comply with the technical safeguards through their Registry Agreements with ICANN. The second safeguard mandated that new gTLD registries implement DNSSEC, with active monitoring of compliance and notices sent to non-compliant registries.[49] DNSSEC is a set of protocols intended to increase the security of the Internet by adding authentication to DNS resolution to prevent problems such as DNS

[41] Ibid.

[42] The Security Skeptic, "Orphaned Glue Records," 26 October 2009, accessed 2 February 2017, http://www.securityskeptic.com/2009/10/orphaned-glue-records.html. These are records remaining once a domain name has been deleted from a registry.

[43] ICANN, "Malicious Conduct."

[44] See ICANN, New gTLD Program Safeguards (2016).

[45] ICANN (2 August 2016), Request for Proposal For Study on Rates of DNS Abuse in New and Legacy Top-Level Domains, accessed 2 February 2017, https://www.icann.org/en/system/files/files/rfp-dns-abuse-study-02aug16-en.pdf. The DNS Abuse Study measures common forms of abuse – such as spam, phishing, and malware distribution – in all gTLDs from 1 January 2014 until December 2016. See SIDN Labs and the Delft University of Technology (August 2017), Statistical Analysis of DNS Abuse in gTLDs Final Report, accessed 23 October 2017, https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf

[46] Technical requirements change over time, which would make continual auditing difficult.

[47] ICANN, *Applicant Guidebook* (June 2012), Section 5-4.

[48] ICANN, "Pre-Delegation Testing (PDT)," accessed 2 February 2017, https://newgtlds.icann.org/en/applicants/pdt

[49] ICANN, "Registry Agreement," accessed 2 February 2017, https://www.icann.org/resources/pages/registries/registries-agreements-en, Specification 6, Clause 1.3.

spoofing[50] and DNS cache poisoning.[51] All new gTLDs are DNSSEC signed at the root level, which is not indicative of second level domain names in the zone being signed.[52]

For the third safeguard, the Registry Agreement for new gTLDs prohibits wildcarding to ensure that domain names only resolve for an exact match and that end users are not misdirected to another domain name by a synthesized response.[53] Complaints against registry operators for permitting wildcarding may be submitted to ICANN via an online interface.[54] A registry's use of wildcarding is easily detectable because every query will receive a response, instead of a "name error," even if the domain name is not valid.[55] This means that a user will be redirected to a similar domain name. It appears that all new gTLD operators are in compliance with this safeguard.[56]

To comply with the fourth safeguard, new gTLD registries are required to remove orphan glue records when presented with evidence that such records have been used in malicious conduct.[57] Unmitigated orphan glue records can be used for malicious purposes such as fast-flux hosting botnet attacks.[58] This requirement is reactive by design, but registry operators can make it technically impossible for orphan glue records to exist in the first place and some do. Since 2013 there have been no ICANN Compliance complaints related to orphan glue records.[59]

For the fifth safeguard, Registry Agreements require new gTLD operators to create and maintain Thick WHOIS records for domain name registrations. This means that registrant contact information, along with administrative and technical contact information, is collected and displayed in addition to traditional Thin WHOIS data at the registry level.[60] ICANN Compliance monitors adherence to the Thick WHOIS requirement on an active basis, for both reachability and format.[61] Syntax and operability accuracy are evaluated by the ICANN WHOIS Accuracy Reporting System (ARS) project.[62] The Impact of Safeguards chapter of this report further explains the ARS and related compliance issues.

[50] SANS Institute, *Global Information Assurance Certification Paper*, accessed 2 February 2017, https://www.giac.org/paper/gcih/364/dns-spoofing-attack/103863. DNS spoofing occurs "when a DNS server accepts and uses incorrect information from a host that has no authority giving that information" (p. 16).

[51] Sooel Son and Vitaly Shmatikov, "The Hitchhiker's Guide to DNS Cache Poisoning" (paper presented at the 6th International ICST Conference on Security and Privacy in Information Networks, Singapore, 7-9 September 2010), https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf. DNS cache poisoning occurs when the temporary cached data stored by a DNS resolver is intentionally altered to map DNS resolutions to IP addresses routed to invalid or malicious destinations (p. 1).

[52] ICANN, "TLD DNSSEC Report," accessed 26 April 2017, http://stats.research.icann.org/dns/tld_report/. This does not include .aero.

[53] ICANN, "Registry Agreement," Specification 6, Clause 2.2

[54] ICANN, "Wildcard Prohibition (Domain Redirect) Complaint Form," accessed 2 February 2017, https://forms.icann.org/en/resources/compliance/registries/wildcard-prohibition/form.

[55] https://www.icann.org/groups/ssac/documents/sac-015-en

[56] As of 1 January 2017, no complaints have been reported via this form. See also "DNSSEC Deployment Report," accessed 1 January 2017, https://rick.eng.br/dnssecstat/

[57] ICANN, "Registry Agreement," Specification 6, Clause 4.1

[58] ICANN Security and Stability Advisory Committee (March 2008), *SSAC Advisory on Fast Flux Hosting and DNS*, accessed 2 February 2017, https://www.icann.org/en/system/files/files/sac-025-en.pdf

[59] ICANN, Contractual Compliance Reports, https://www.icann.org/resources/pages/compliance-reports-2016-04-15-en

[60] ICANN, "What are thick and thin entries?", accessed 2 February 2017, https://whois.icann.org/en/what-are-thick-and-thin-entries

[61] ICANN, "Registry Agreement," Specification 10, Section 4.

[62] ICANN, "WHOIS Accuracy Reporting System (ARS) Project Information," accessed 2 February 2017, https://whois.icann.org/en/whoisars

Registry Agreements also require all new gTLD registry operators to post abuse contact details on their websites and to notify ICANN of any changes to contact information.[63] ICANN monitors compliance with this requirement and publishes statistics, including remediation measures, in its quarterly reports.[64] The Registry Agreements require registry operators to respond to well-founded complaints but do not mandate specific procedures for doing so. Consequently, there is no standard by which ICANN compliance can assess the particular means by which registry operators resolve complaints. There were 55 complaints related to abuse contact data in 2016,[65] 61 in 2015,[66] 100 in 2014,[67] and 386 in 2013.[68]

On the sixth safeguard, new gTLD operators are required via the Registry Agreement to make their zone files available to approved requestors via the Centralized Zone Data Service.[69] Centralizing these data sources enhances the ability of security researchers, IP attorneys, law enforcement agents, and other approved requestors to access the data without the need to enter into a contractual relationship each time. There were 19 complaints related to bulk zone file access in 2016,[70] 27 in 2015,[71] and 55 in 2014.[72] No data was available in the ICANN 2013 Contractual Compliance Report.

To enhance the stability of the DNS, ICANN created the Expedited Registry Security Request (ERSR) process, which permits registries "to request a contractual waiver for actions it might take or has taken to mitigate or eliminate" a present or imminent security incident.[73] As of 5 October 2016, ICANN reports that the ERSR has not been invoked for any new gTLD.[74]

In addition to the aforementioned safeguards, ICANN, in response to community input, proposed the creation of the High Security Zone Verification Program whereby gTLD registry operators could voluntarily create high security zones.[75] An advisory group conducted extensive research to determine standards by which registries would abide to be deemed a High Security Zone. However, the proposals never reached the implementation stage due to a lack of consensus.

The technical safeguards, enforced through contractual compliance, imposed requirements upon new gTLD registries and registrars that purportedly mitigated risks inherent in the

[63] ICANN, "Registry Agreement," Specification 6, Section 4.1.
[64] ICANN, "Contractual Compliance Reports 2016," accessed 2 February 2017, https://www.icann.org/resources/pages/compliance-reports-2016-04-15-en
[65] https://www.icann.org/en/system/files/files/annual-2016-31jan17-en.pdf
[66] ICANN, "Contractual Compliance Reports 2015," accessed 2 February 2017, https://www.icann.org/resources/pages/compliance-reports-2015-04-15-en
[67] ICANN, "Contractual Compliance Reports 2014," accessed 2 February 2017, https://www.icann.org/resources/pages/compliance-reports-2014-2015-01-30-en
[68] ICANN, "Contractual Compliance Reports 2013," accessed 2 February 2017, https://www.icann.org/resources/pages/reports-2013-02-06-en
[69] ICANN, "Registry Agreement," Specification 4, Section 2.1; ICANN, "Centralized Zone Data Service," accessed 2 February 2017, https://czds.icann.org/en
[70] ICANN, "Contractual Compliance Reports 2016."
[71] ICANN, "Contractual Compliance Reports 2015."
[72] ICANN, "Contractual Compliance Reports 2014."
[73] ICANN, "Expedited Registry Security Request Process," accessed 2 February 2017, https://www.icann.org/resources/pages/ersr-2012-02-25-en.
[74] ICANN Registry Services, email discussion with Review Team, July 2017.
[75] ICANN (18 November 2009), *A Model for a High-Security Zone Verification Program*, accessed 2 February 2017, https://archive.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf; icann.org, "Public Comment: High Security Zone TLD Final Report," 11 March 2011, https://www.icann.org/news/announcement-2011-03-11-en

expansion of the DNS. The CCTRT's DNS abuse study[76] provides insight into whether the overall implementation of these safeguards reduced the levels of DNS abuse compared to legacy gTLDs.

5.1.1 DNS Abuse Study

In preparation for the CCTRT's review of "safeguards put in place to mitigate issues involved in…the expansion" of gTLDs, ICANN issued a report analyzing the history of DNS abuse safeguards tied to the New gTLD Program.[77] In doing so, the report assessed the various ways to define DNS abuse. Some of the challenges to defining DNS abuse arise because of the various ways that different jurisdictions define and treat DNS abuse. Certain activities are considered to be abusive in some jurisdictions but not others. Some of these activities, such as those solely focused on intellectual property violations, are interpreted differently not only in terms of substance but also in terms of remedies available in the applicable jurisdiction. Another challenge is the lack of data available regarding certain types of abuse. Nonetheless, there are core technical abuse behaviors for which there is both consensus and significant data available. These include spam, phishing, malware distribution, and botnet command and control.

The ICANN report acknowledged the absence of a comprehensive comparative study of DNS abuse in new gTLDs versus legacy gTLDs. Nonetheless, some metrics suggest that a high percentage of new gTLDs might suffer from DNS abuse. For example, Spamhaus consistently ranks new gTLDs amongst its list of "The 10 Most Abused Top-Level Domains" based on the ratio of the number of domain names associated with abuse versus the number of domain names seen in a zone.[78] Whereas, using a different methodology, previous research from Architelos and the Anti-Phishing Working Group named .com the TLD with the largest number of domain names associated with abuse.[79] A 2017 report from PhishLabs also concluded that half of all phishing sites are in the .com zone, with new gTLDs comprising 2% of all phishing sites.[80] However, the same report found that phishing sites in new gTLD zones have increased 1000% since the previous year. This appears to have coincided with an overall significant increase in phishing attacks during 2016.[81]

[76] ICANN, *Request for Proposal*. SIDN Labs and the Delft University of Technology, "DNS Abuse in gTLDs".
[77] ICANN, *New gTLD Program Safeguards* (2016)
[78] Spamhaus, "The World's Most Abused TLDs," accessed 2 February 2017, https://www.spamhaus.org/statistics/tlds/
[79] Anti-Phishing Working Group (29 April 2015), *Phishing Activity Trends Report: 4th Quarter 2014*, accessed 2 February 2017, http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf; Architelos (June 2015), *The NameSentry℠ Abuse Report: New gTLD State of Abuse 2015*, accessed 2 February 2017, http://domainnamewire.com/wp-content/Architelos-StateOfAbuseReport2015.pdf
[80] PhishLabs, 2017 Phishing Trends & Intelligence Report, p. 23-24, https://pages.phishlabs.com/rs/130-BFB-942/images/2017%20PhishLabs%20Phishing%20and%20Threat%20Intelligence%20Report.pdf. New gTLDs comprised 8% of the overall TLD market during this time period when .tk is excluded from the data universe. See Kevin Murphy, Phishing in new gTLDs up 1,000% but .com still the worst, Domain Incite, Feb. 20, 2017, http://domainincite.com/21552-phishing-in-new-gtlds-up-1000-but-com-still-the-worst
[81] Lindsey Havens, APWG & Kaspersky Research Confirms Phishing Trends & Intelligence Report Findings, March 2, 2017, available at https://info.phishlabs.com/blog/apwg-kaspersky-research-confirms-phishing-trends-investigations-report-findings; Darya Gudkova, et. al., Spam and phishing in 2016, Kaspersky Security Bulletin, February 20, 2017, available at https://securelist.com/kaspersky-security-bulletin-spam-and-phishing-in-2016/77483/; APWG, Phishing Trends Activity Report, Feb. 23, 2017, available at http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

Domain names are often a key component of cybercrime and enable cybercriminals to quickly adapt their infrastructure.[82] For example, spam campaigns often correlate with phishing and other cybercrime.[83] Domain names are also used to assist with malware distribution and botnet command and control. Troubling statistics and incidents observed by network operators have led to perceptions that many new gTLDs offer nothing more than abuse.[84] In fact, some Internet security companies have advised customers to block all network traffic to specific TLDs.[85] Such practices run counter to ICANN's Universal Acceptance efforts. Whereas, beyond the safeguards, efforts to combat domain name abuse vary greatly amongst registries and registrars. Some entities do not act until a complaint is received. In contrast, other registrars take proactive steps to check registrant credentials, block domain name strings similar to known phishing targets, and scrutinize domain name resellers, which are not ICANN-contracted parties.[86]

In light of the dynamic DNS environment, snapshots of new gTLD abuse do not account for the full variety of registration rules and safeguards in the hundreds of new gTLDs that have been delegated since 2013. Accordingly, it is difficult to ascertain definitive distinctions between abuse rates in legacy and new gTLDs without performing a comprehensive assessment. To the extent possible, the CCTRT has sought to measure the effectiveness of the technical safeguards developed for the New gTLD Program in mitigating various forms of DNS abuse. As part of this process, the CCTRT commissioned a comprehensive DNS abuse study to analyze levels of technical abuse[87] in legacy and new gTLDs, to inform this review and potentially serve as a baseline for future analysis.[88] The ICANN-selected vendor, a joint team comprised of researchers from Delft University of Technology in the Netherlands (TU Delft) and the Foundation for Internet Domain Registration in the Netherlands (SIDN), delivered a final report on 9 August 2017.[89]

DNS Abuse Study Methodology

The DNS Abuse Study relied upon zone files, Whois records, and 11 distinct domain name blacklist feeds to calculate rates of technical DNS abuse from 1 January 2014[90] through the end of 31 December 2016.

The analysis includes:

[82] Symantec (April 2015), *Internet Security Threat Report*, accessed 2 February 2017, https://its.ny.gov/sites/default/files/documents/symantec-internet-security-threat-report-volume-20-2015-social_v2.pdf

[83] Richard Clayton, Tyler Moore, and Henry Stern, "Temporal Correlations between Spam and Phishing Websites" (paper presented at the LEET'09 Proceedings of the 2nd USENIX Conference on Large-Scale Exploits and Emergent Threats, Boston, MA, 21 April 2009) https://www.cl.cam.ac.uk/~rnc1/leet09.pdf.

[84] Tom Henderson, The new internet domains are a wasteland, Network World, July 5, 2016, http://www.networkworld.com/article/3091754/security/the-new-internet-domains-are-a-wasteland.html

[85] In a 2015 report, Blue Coat advised network operators to block all traffic to or from ".work, .gq, .science, .kim and .country". See Blue Coat, DO NOT ENTER Blue Coat Research Maps the Web's Shadiest Neighborhoods, September 2015, p. 7, available at https://www.bluecoat.com/documents/download/895c5d97-b024-409f-b678-d8faa38646ab

[86] Secure Domain Foundation, The Cost of Doing Nothing, June 2015, p. 8, https://securedomain.org/Documents/SDF_Report1_June_2015.pdf; Registrars must impose flow down contractual requirements onto resellers with which they contract. However, the resellers are not ICANN-accredited. See Registration Accreditation Agreement, 3.12 Obligations Related to Provision of Registrar Services by Third Parties

[87] Phishing, malware hosting, and spam. Initially, the RT sought to include botnet domains in the analysis. However, discrete historical data on botnets was unavailable for the timeframe of the study. Nonetheless, botnet associated domain names (hosting and command and control) were included in the malware blacklists.

[88] ICANN, Request for Proposal.

[89] SIDN Labs and the Delft University of Technology, "DNS Abuse in gTLDs".

[90] The first new gTLD delegations began in October 2013.

1. Absolute counts of abusive domains per gTLD and registrar from 1 January 2014 until 31 December 2016, taking into account sunrise periods and dates of general availability for registration
2. Abuse rates, based on an "abused domains per 10,000" ratio (as a normalization factor to account for different TLD sizes), per gTLD and registrar from 1 January 2014 until 31 December 2016
3. Abuse associated with privacy and proxy services
4. Geographic locations associated with abusive activities
5. Abuse levels distinguished by "maliciously registered" versus "compromised" domains
6. An inferential statistical analysis on the effects of security indicators and the structural properties of new gTLDs, (i.e. number of DNSSEC-signed domains, parked domains, number of domains in each new gTLD, as well as the number of domains resolving to content)

DNS Abuse Study Findings

The report makes many significant findings regarding DNS abuse associated with new gTLDs compared with legacy gTLDs. Generally, the DNS Abuse Study indicates that the introduction of new gTLDs did not increase the total amount of abuse for all gTLDs. Nonetheless, the results demonstrate that the nine aforementioned safeguards alone do not guarantee a lower rate of abuse in each new gTLD compared to legacy gTLDs. Instead, factors such as registration restrictions, price, and registrar-specific practices seem more likely to affect abuse rates.[91]

Abuse is migrating to new gTLDs

Legacy gTLDs still account for most domain name registrations and, perhaps consequently, the highest volume of phishing and malware associated domain names.[92] Nonetheless, the overall rates of abuse in legacy and new gTLDs were similar by the end of 2016, and there are distinct trends with regard to specific types of abuse. For example, by the end of 2016, spam registrations in legacy gTLDs had declined while those in new gTLDs saw a significant increase. In the last quarter of 2016, 56.9 of every 10,000 legacy gTLD domain names were on spam blacklists whereas the rate for new gTLD domain names was 526.6 domain names per 10,000 registrations.[93]

Some abuse trends showed overlap. The top five legacy gTLDs with the highest rates of phishing also had the highest rates of domain names tied to malware distribution.[94] Phishing and malware abuse rates in legacy gTLDs more often resulted from compromised domain names rather than malicious registrations. There are much higher rates of compromised legacy gTLD domain names than new gTLDs.

Specific to malware distribution,[95] the top 5 new gTLDs with the highest rates of abusive domain names were .top, .wang, .win, .loan, and .xyz. Since the end of 2015, the .top TLD has had the highest rate of abusive registrations for all legacy and new gTLDs.[96] Each of these TLDs offered low priced registrations, usually at levels lower than those for a .com registration.

[91] P.24-25
[92] P.24
[93] p.24
[94] p.12
[95] Based on the StopBadware data feed
[96] p.13

The DNS Abuse Study distinguishes between domain names registered specifically for malicious purposes and domain names registered for legitimate purposes that were subsequently compromised.[97] The results of the study indicate that the introduction of new gTLDs has corresponded with a decrease in the number of spam associated registrations in legacy gTLDs, while malicious registrations have increased in new gTLDs.[98] This, along with the fact that the total number of spam registrations remains stable,[99] suggests that perhaps miscreants are shifting from registering domain names in legacy gTLDs to new gTLDs. Within this trend, there are specific new gTLDs that serve as primary targets of opportunity for abusive registrations, whether due to lax registration policies and abuse enforcement or price. In fact, some registrars are almost entirely associated with abusive, rather than legitimate, registrations.

Abuse is not universal in new gTLDs

Even though abuse is growing in new gTLDs, it is by no means rampant across all new gTLDs. Instead, by the end of 2016, this phenomenon was highly concentrated. Five new gTLDs, suffering from highest concentration of domain names used in phishing attacks (APWG last quarter 2016), accounted for 58.7% of all blacklisted new gTLD domain names.[100] Whereas, Spamhaus blacklisted at least 10% of all domain names registered within 15 new gTLDs. Nevertheless, approximately a third of all new gTLDs did not have a single instance of abuse, as reported on blacklists, in the final quarter of 2016.

Two registrars highlighted by the Study had overwhelming rates of abuse. Alarmingly, more than 93% of the new gTLD registrations sold by Nanjing Imperiosus Technology, based in China, appeared on SURBL's blacklists. For much of 2016, abuse rates associated with this registrar grew at significant rates. ICANN eventually suspended Nanjing in January 2017, citing its failure to comply with the RAA.[101] However, the sustained, unabated, high abuse rates were not the actionable reason.

Another registrar, Alpnames Ltd., based in Gibraltar, was associated with a high volume of abuse from .science and .top domain names. The Study notes that this registrar used price promotions that offered domain name registrations for $1 USD or sometimes even free.[102] Moreover, Alpnames permitted registrants to randomly generate and register 2,000 domain names in 27 new gTLDs in a single registration process. Bulk domain names using domain generation algorithms are commonly associated with cybercrime.[103] At the time of this report, Alpnames remained ICANN-accredited.

Many attributes can play a role in the volume or rate of abuse in a particular TLD. In terms of absolute size, new gTLDs are no different than legacy gTLDs in that the larger the size of the TLD, the higher the total number of domain names associated with abuse.[104] Whereas, analyzing attributes of cross-TLD registry operators, the Study suggests that many of the operators associated with the highest rates of abuse had low priced domain registration offerings.

[97] Compromised domain names include domain names for which the domain name registration or the website may have been hacked.
[98] p. 2
[99] See DNS Abuse Study, figures 24, 36, and 38, corresponding to the absolute number of spam domains for different spam feeds
[100] P.11
[101] https://www.icann.org/uploads/compliance_notice/attachment/895/serad-to-hansmann-4jan17.pdf
[102] p.20
[103] Aditya K. Sood, Sherali Zeadally, "A Taxonomy of Domain-Generation Algorithms", IEEE Security & Privacy, vol. 14, no. , pp. 46-53, July-Aug. 2016, doi:10.1109/MSP.2016.76
[104] p.15

The Study concluded that domain names registered for malicious purposes often contained strings related to trademarked terms.[105] Specifically, of the 88 .top domain names associated with abuse in the fourth quarter of 2015, 75 of them included exact or misspelled versions of Apple, iCloud, or iPhone, implying that the domain names were used in a phishing campaign against users of Apple, Inc. products and services.

The Study found a statistically weak but positive correlation between the number of parked domains in a new gTLD zone and the rate of abuse.[106] Oddly, there was also a weak positive correlation between the number of DNSSEC signed domain names and abuse in a new gTLD zone.[107] The use of privacy/proxy services to mask registrant Whois data is more common in legacy than new gTLDs. Regardless, the Study did not find any statistically significant relationship between the use of such services and domain name abuse. Above all, the Study identified a relatively stronger correlation between restrictive registration policies and lower rates of abuse. Nonetheless, even new gTLDs with open registration policies varied greatly in abuse rates, suggesting that among other key variables, such as price, differences in registry and registrar anti-abuse practices may also influence abuse rates.

DNS abuse is not random

Price and registration restrictions appear to affect which registrars and registries cybercriminals will choose for DNS abuse, making low priced domain names with easy registrations attractive attack vectors.[108] Nonetheless, the same qualities may be appealing for registrants with legitimate interests and the overarching goal of a free and open Internet. Consequently, monetary incentives may exist for registry and registrar operators to prevent systemic DNS abuse by proactively screening registrations and detecting malfeasance. For example, there is precedent for ICANN adjusting its fee price structure to address behavior harmful to the DNS, such as abolishing the automatic fee refund for domain tasters.[109] Similarly, the CCT Review Team proposes the development of incentives to reward best practices preventing technical DNS abuse and strengthening the consequences for culpable or complacent conduits of technical DNS abuse. These recommendations may be applicable to curb other misuse of domain names to the extent the community reaches consensus on other forms of DNS abuse.

We are concerned at the high levels of DNS abuse concentrated in a relatively small number of registries and registrars and geographic regions; this DNS abuse appears to have gone on unremedied for an extended amount of time in some cases.

Recommendations 1 to 5 are designed to address the reality that the new gTLD safeguards did not, on their own, prevent technical DNS abuse. In addition to means available today to prevent and mitigate DNS abuse, we propose new incentives and tools to combat abuse that will:

- Encourage and incentivize pro-active abuse measures as per Recommendation 1
- Introduce measures to prevent technical DNS abuse as per Recommendation 2
- Ensure that the data collection is ongoing and acted upon as per Recommendation 3

[105] p. 12
[106] p.16
[107] p.16
[108] p. 25
[109] http://www.washingtonpost.com/wp-dyn/content/article/2008/01/30/AR2008013002178.html

- Consider an additional mechanism where, despite Recommendations 1, 2 and 3, registry operators or registrars that have not effectively mitigated the technical DNS abuse. A dispute resolution process should be considered to enable injured parties to take action as in Recommendation 4 (note this lacks Review Team consensus. See Minority Statement in Appendix 6). Indeed, there should be more emphasis on ICANN Compliance and where a clean-up is identified as being necessary. If the level of abuse has not come down, as per the commitment of the Registry, then the failure of the contracted party to implement the plan should constitute a breach of the RAA/RA. If a level of obligation is there, then not only does the DADRP become less necessary, but also less likely to be used. This translates to positive outcomes for all parties due to decreased levels of DNS Abuse.

Recommendation A: Consider directing ICANN org, in its discussions with registries, to negotiate amendments to existing Registry Agreements, or in negotiations of new Registry Agreements associated with subsequent rounds of new gTLDs, to include provisions in the agreements to provide incentives, including financial incentives, to registries, especially open registries, to adopt proactive anti-abuse measures.[110]

Rationale/related findings: The new gTLD safeguards alone do not prevent technical abuse in the DNS. Abuse rates are correlated to registration restrictions imposed on registrants and registration prices may influence rates too. Some registries are inherently designed to have strict registration policies and/or high prices. However, a free, open, and accessible Internet will invariably include registries with open registration policies and low prices that must adopt other measures to prevent technical DNS abuse. Registries that do not impose registration eligibility restrictions can reduce technical DNS abuse through proactive means such as identifying repeat offenders, monitoring suspicious registrations, and actively detecting abuse instead of merely waiting for complaints to be filed. Therefore, ICANN should incentivize and reward the implementation of proactive anti-abuse measures by such registry operators to reduce technical DNS abuse in open gTLDs.

To: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization and the Subsequent Procedures PDP WG

Prerequisite or Priority Level: High

Consensus within team: Yes

Details: The ICANN Board should consider urging ICANN org to negotiate with registries to include in the registry agreements fee discounts available to registry operators with open

[110] The CCTRT looked for examples of practices that could assist in proactively minimizing abuse. One such example has been proposed by EURid, the operator of the .EU registry, which will soon test a delayed delegation system. See https://eurid.eu/en/news/eurid-set-to-launch-first-of-its-kind-domain-name-abuse-prevention-tool/ and https://eurid.eu/media/filer_public/9e/d1/9ed12346-562d-423d-a3a4-bcf89a59f9b4/eutldecosystem.pdf. This process will not prevent registrations but instead delay activation of a registration if a domain name is identified as being potentially abusive by machine learning algorithms. Future review teams could study this effort to consider its effectiveness and whether it could serve as a potential innovative model to help foster trust and a secure online environment. In addition, the .XYZ registry may provide another example of proactive measures to combat abuse. The .xyz registry purports to have a zero-tolerance policy toward abuse-related activities on .xyz or any of their other domain extensions using a sophisticated abuse monitoring tool enabling proactive monitoring and detection in near real-time, suspending domains engaging in any of the abusive activities set out. Future review teams could explore the effectiveness of this approach by examining abuse rates over time and comparing the levels of abuse both before and after this policy.

registration policies that implement proactive measures to prevent technical DNS abuse in their zone.

Recommendation B: Consider directing ICANN org, in its discussions with registrars and registries, to negotiate amendments to the Registrar Accreditation Agreement and Registry Agreements to include provisions aimed at preventing systemic use of specific registrars for technical DNS abuse.

Rationale/Related Findings: Current policies focus on individual abuse complaints. However, registrars and registry operators associated with extremely high rates of technical DNS abuse continue operating and face little incentive to prevent technical DNS abuse. Moreover, there currently exist few enforcement mechanisms to prevent systemic domain name abuse associated with resellers. Systemic use of particular registrars and registries for technical DNS abuse threatens the security and stability of the DNS, the universal acceptance of TLDs, and consumer trust.

To: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization and the Subsequent Procedures PDP WG

Prerequisite or Priority Level: High

Consensus within team: Yes

Details: The ICANN Board should consider directing ICANN org to negotiate amendments to the Registrar Accreditation Agreement and Registry Agreement provisions aimed at preventing systemic use of specific registrars for technical DNS abuse. Such language should impose upon registrars, and their affiliated entities such as resellers, a duty to mitigate technical DNS abuse, whereby ICANN may suspend registrars and registry operators found to be associated with unabated, abnormal and extremely high rates of technical abuse. ICANN must base such findings on multiple verifiable reliable sources and such findings may be rebutted by the registrar upon sufficient proof that the findings were inaccurate. The following factors may be taken into account when making a determination: whether the registrar or registry operator 1) engages in proactive anti-abuse measures to prevent technical DNS abuse, 2) was itself a victim in the relevant instance, 3) has since taken necessary and appropriate actions to stop the abuse and prevent future systemic use of its services for technical DNS abuse.

Recommendation C: Further study the relationship between specific registry operators, registrars and DNS abuse by commissioning ongoing data collection, including but not limited to, ICANN Domain Abuse Activity Reporting (DAAR) initiatives. For transparency purposes, this information should be regularly published in order to be able to identify registries and registrars that need to come under greater scrutiny and higher priority by ICANN Compliance. Upon identifying abuse phenomena, ICANN should put in place an action plan to respond to such studies, remediate problems identified, and define future ongoing data collection.

Rationale/Related Findings: The DNS Abuse Study commissioned by the CCT-RT identified extremely high rates of abuse associated with specific registries and registrars as well as registration features, such as mass registrations, which appear to enable abuse. Moreover, the Study concluded that registration restrictions correlate with abuse, which means that there are many factors for which to account in order to extrapolate cross-TLD abuse trends for specific registry operators and registrars. The DNS Abuse Study has highlighted certain behaviors that are diametrically opposed to encouraging consumer trust in the DNS. Certain registries and registrars appear to either positively encourage or at the

very least willfully ignore DNS abuse. Such behavior needs to be identified rapidly and action must be taken by ICANN compliance as deemed necessary.

To: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization and the Subsequent Procedures PDP WG, SSR2 Review Team.

Prerequisite or Priority Level: High

Consensus within team: Yes

Details: The additional studies need to be of an ongoing nature, collecting relevant data concerning DNS abuse at both the registrar and registry level. The data should be regularly published, thereby enabling the community and ICANN compliance in particular to identify registries and registrars that need to come under greater compliance scrutiny and thereby have such behavior eradicated.

Recommendation D: A DNS Abuse Dispute Resolution Policy ("DADRP") should be considered by the community to deal with registry operators and registrars that are identified as having excessive levels of abuse (to define, e.g. over 10% of their domain names are blacklisted domain names). Such registry operators or registrars should in the first instance be required to a) explain to ICANN Compliance why this is, b) commit to clean up that abuse within a certain time period, and / or adopt stricter registration policies within a certain time period. Failure to comply will result in a DADRP, should ICANN not take any action themselves.

Rationale/Related Findings: The DNS Abuse Study commissioned by CCT-RT identified extremely high rates of abuse associated with specific registries. It is important to have a mechanism to deal with this abuse, particularly if it's prevalent in certain registries. Abusive behavior needs to be eradicated from the DNS and this would provide an additional arm to combat that abuse.

To: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization, the Subsequent Procedures PDP WG and the SSR2 Review Team

Prerequisite or Priority Level: High

Consensus within team: Majority consensus but not unanimity (see Minority Statement in Appendix 6.1 Minority Statements)

Details: ICANN Compliance is one route to dealing with this high level of DNS abuse, enforcing existing and any amendments to the Registrar Accreditation Agreement to prevent systemic use of specific registrars for technical DNS abuse as per Recommendation 2. However, in addition, a specific DADRP should be considered as it could also be very helpful in dealing with such DNS abuse, and it could also serve as a significant deterrent and help prevent or minimize such high levels of DNS abuse. Registry operators or registrars that are identified as having excessive levels of abuse (to be defined, for example where a registry operator has over 10% of their domain names blacklisted by one or more heterogeneous blacklists (StopBadware SDP, APWG, Spamhaus, Secure Domain Foundation, SURBL and CleanMX). A DADRP should set out specific penalties. Examples from the DNS Abuse Study of new gTLDs with over 10% of their domain names blacklisted, according to Spamhaus for example are .SCIENCE (51%), .STREAM (47%), .STUDY

(33%), .DOWNLOAD (20%), .CLICK (18%), .TOP (17%), .GDN (16%), .TRADE (15%), .REVIEW (13%), and .ACCOUNTANT (12%). Thus, each of these registries should be obliged to review their second level domain names being used for DNS abuse and explain why this is, commit to cleaning these up within a certain timeframe, and adopt stricter registration policies if necessary to ensure that there exist relevant contractual terms to effectively handle such registrations. If the domain names at issue are not cleaned up satisfactorily, and in the event ICANN does not take immediate action, then a DADRP may be brought by an affected party. The process should involve a written complaint to the registry, time allotted for a response from the registry, and an oral hearing. Final decisions should be issued by an expert panel which could recommend one or more enforcement mechanisms to be agreed upon by the community.

For purposes of this recommendation, a registrar acting under the control of a registry operator would be covered by the DADRP so it is important to ensure that "registry operator" shall include entities directly or indirectly controlling, controlled by, or under common control with, a registry operator, whether by ownership or control of voting securities, by contract or otherwise where 'control' means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether by ownership or control of voting securities, by contract or otherwise.

5.2 Rights Protection Mechanisms

New rights protection mechanisms (RPMs) were specifically developed in connection with the introduction of the New gTLD Program alongside existing rights protection mechanisms. The CCT Review Team examined whether these RPMs help encourage a safe environment and promote consumer trust in the DNS, and also sought to measure the costs impact of the New gTLD Program to intellectual property owners.

The RPMs themselves are firstly described for completeness before we move on to a consideration of these mechanisms and whether they have helped mitigate the issues around the protection of trademark rights and consumers in this expansion of gTLDs. It was clear that the CCT Review Team faced difficulties in obtaining reliable data to make this assessment, turning primarily to the data obtained by ICANN under the CCT Metrics Reporting[111] and the INTA Impact Study[112] as well as existing data and commentary from the ICANN Rights Protection Mechanisms Review and the Independent Review of Trademark Clearinghouse (TMCH) Services Revised Report[113].

The CCT Review Team also noted the parallel work by the ongoing Working Groups currently looking into RPMs and sought not to duplicate or undermine that work and thus looks forward to the reports from those groups.

5.2.1 Background to the RPMs

Prior to the 2012 gTLD expansion in the number of gTLDs, aside from action taken by courts, the main rights protection mechanism for the DNS was the UDRP, an alternative

[111] ICANN, "Competition, Consumer Trust and Consumer Choice (CCT) Metrics Reporting," accessed 10 October 2017, https://www.icann.org/resources/reviews/cct/metrics
[112] Nielsen, INTA New gTLD Cost Impact Survey (April 2017), accessed 14 September 2017: community.icann.org/download/attachments/56135378/INTA Cost Impact Report revised 4-13-17 v2.1.pdf
[113] Analysis Group, Independent Review of Trademark Clearinghouse (TMCH) Services Revised Report (February 2017), accessed 10 October 2017, https://newgtlds.icann.org/en/reviews/tmch/revised-services-review-22feb17-en.pdf

dispute resolution procedure (adopted by ICANN on 26 August 1999) that applied to all generic top-level domains. However, the existence of issues concerning trademark protection were identified prior to the 2012 gTLD expansion. In particular the trademark community had voiced concerns that this mechanism alone would be insufficient to adequately protect trademark rights and consumers in an expanded DNS. The ICANN Board therefore resolved (2009.03.06) that an internationally diverse group of persons with knowledge, expertise and experience in the fields of trademark, consumer protection, competition law and the interplay of trademarks and the DNS be convened to propose solutions to the overarching issue of trademark protection in connection with the introduction new gTLDs[114]. This group was named the Implementation Recommendation Team (IRT).

A set of new rights protection mechanisms were proposed by IRT, namely: Uniform Rapid Suspension System (URS); Post-Delegation Dispute Resolution Procedures (PDDRP); the Trademark Post-Delegation Dispute Resolution Procedure (TM-PDDRP); Registry Restriction Dispute Resolution Procedure (RRDRP); Public Interest Commitments Dispute Resolution Procedure (PICDRP); and the Trademark Clearinghouse (Sunrise and Claims Service)[115].

5.2.2 Description of the RPMs

5.2.2.1 Uniform Domain Name Dispute Resolution Policy (UDRP)

The Uniform Domain Name Dispute Resolution Policy (UDRP) is an alternative dispute resolution procedure adopted by ICANN on 26 August 1999 that applies to all generic top-level domains (gTLDs), including legacy gTLDs (such as .com, .net, .info) as well as new gTLDs, and certain country code top-level domains (ccTLDs) that have adopted it. To be successful under the UDRP, a complainant must demonstrate by preponderance of the evidence the following three requirements: (i) the domain name registered by the respondent is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and (ii) the respondent has no rights or legitimate interests in respect of the domain name; and (iii) the domain name has been registered and is being used in bad faith.

A procedure under the UDRP takes approximately 2 months, from the filing of a complaint to a decision. Costs for filing a complaint under the UDRP range between USD 1,500 for 1 to 5 domain names (single-member panel) and USD 4,000 for 1 to 5 domain names (three-member panel), excluding lawyers' fees. The remedies available under the UDRP are limited to the transfer or cancellation of a domain name. No damages are awarded and there is no appeal mechanism in place. A decision is generally implemented after 10 business days following the notification of the decision, unless court proceedings are initiated in a court of competent jurisdiction.

UDRP complaints are filed electronically with an ICANN-approved dispute resolution provider. To date, the following providers have been approved by ICANN: the Asian Domain Name Dispute Resolution Centre (ADNDRC), the Forum (NAF), World Intellectual Property

[114] ICANN, "Adopted Board Resolutions: Mexico: Protections for Trademarks in New gTLDs," 6 March 2009, https://www.icann.org/resources/board-material/resolutions-2009-03-06-en#07.

[115] In addition, string contention processes were introduced for applications for the gTLDs themselves, relating to string confusion, limited public interest, community objection and legal rights objection. These are discussed in more detail in the Application and Evaluation section.

Organization (WIPO), the Czech Arbitration Court Arbitration Center for Internet Disputes (CAC) and the Arab Center for Domain Name Dispute Resolution (ACDR).

5.2.2.2 Uniform Rapid Suspension System (URS)

The Uniform Rapid Suspension System (URS) is an alternative dispute resolution procedure launched in 2013 that was originally designed for clear-cut cases of cybersquatting under new generic top-level domains (gTLDs), although it has been voluntarily adopted by a handful of ccTLDs and "sponsored" TLDs (such as .pw, .travel, .pro and .cat). The substantive requirements under the URS are similar to those under the UDRP, although the required burden of proof is heavier ("clear and convincing evidence," as opposed to "preponderance of the evidence"). A complainant must thus prove the following three requirements: (1) that the domain name is identical or confusingly similar to a word mark: (a) for which the Complainant holds a valid national or regional registration and that is in current use or (b) that has been validated through court proceedings or (c) that is specifically protected by a statute or treaty in effect at the time the URS complaint is filed (1.2.6.1 of the URS); (2) that the registrant has no rights or legitimate interests in the domain name; and (1.2.6.2 of the URS) and (3) the domain name was registered and is being used in bad faith (1.2.6.3 of the URS). Complaints are limited to 500 words. The URS is intended for the most clear-cut cases of cybersquatting and so it is generally not appropriate for domain name disputes involving more complex, genuine contestable issues (such as fair use).

The only remedy available under the URS is the suspension of the domain name, as opposed to the transfer or cancellation (which are remedies available under the UDRP).

Under the URS a domain name may be suspended in as quickly as three weeks from the filing of a complaint. In the event of a favourable decision for the complainant, the domain name is suspended for the remainder of the registration period (which may be extended for an additional year). The website associated with the domain name in question will display a banner stating, "This Site is Suspended" but the WHOIS for the domain name will continue to display the information of the original registrant (except for the redirection of the name servers). If the decision in favor of the complainant was a judgment by default, the registrant may seek a de novo review by filing a response up to six months after the notice of default (which may be extended by six additional months upon request by the registrant).
In the event the decision is denied, the URS provides for an appeal mechanism based on the existing record.

Costs for filing a URS complaint are around USD 375 (for 1 to 14 domain names).

Only three providers have so far been accredited for the URS: the Asian Domain Name Dispute Resolution Centre (ADNDRC), the Forum (NAF) and MSFD Srl (based in Milan, Italy).

5.2.2.3 Post-Delegation Dispute Resolution Procedures (PDDRP)

5.2.2.4 Post-Delegation Dispute Resolution Procedures are rights protection mechanisms that have been designed to provide relief against a new gTLD registry operator's conduct (as opposed to a domain

name registrant or registrar). There are three PDDRPs:

The Trademark Post-Delegation Dispute Resolution Procedure (TM-PDDRP) allows a trademark holder to file a complaint against the registry operator for its involvement in trademark infringement either at the top or second level of a new gTLD.

At the top-level, a complainant must demonstrate by "clear and convincing evidence" that "the registry operator's affirmative conduct in its operation or use of a new gTLD that is identical or confusingly similar to the complainant's trade mark, causes or materially contributes to the gTLD doing one of the following: (1) taking unfair advantage of the distinctive character or the reputation of the complainant's trade mark or (2) impairing the distinctive character or the reputation of the complainant's trade mark; or (3) creating a likelihood of confusion with the complainant's mark" (paragraph 6.1 of the TM-PDDRP).

At the second level, complainants are required to demonstrate by "clear and convincing evidence" that "through the registry operator's affirmative conduct: (a) there is a substantial pattern or practice of specific bad faith intent by the registry operator to profit from the sale of trade mark infringing domain names; and (b) the registry operator's bad faith intent to profit from the systematic registration of domain names within the gTLD that are identical or confusingly similar to the complainant's mark, which: (i) takes unfair advantage of the distinctive character or the reputation of the complainant's trade mark; or (ii) impairs the distinctive character or the reputation of the complainant's trade mark, or (iii) creates a likelihood of confusion with the complainant's trade mark" (paragraph 6.2 of the TM-PDDRP).

If the registry operator is found liable by the expert panel, a number of remedies may be recommended, including remedial measures to prevent future infringing registrations; suspension of accepting new domain name registrations in the gTLDs at stake until the violation has ceased or for a set period of time prescribed by the expert; or termination of the Registry Agreement, in extraordinary circumstances, where the registry operator has acted "with malice" (paragraph 18 of the TM-PDDRP). Ultimately, ICANN has the authority to impose the remedies it deems appropriate, if any.

To date, ICANN has appointed the following dispute resolution providers to resolve disputes under the TM-PPDRP: the Asian Domain Name Dispute Resolution Centre (ADNDRC), the Forum (NAF), and World Intellectual Property Organization (WIPO).

Registry Restriction Dispute Resolution Procedure (RRDRP), allows an established institution to file a complaint against a community-based new gTLD registry operator for failing to meet registration restrictions set out in its Registry Agreement. For a claim to be successful, a complainant must demonstrate by "preponderance of the evidence" that: "(i) the community invoked by the objector is a defined community; (ii) there is a strong association between the community invoked and the gTLD label or string; (iii) the TLD operator violated the terms of the community-based restrictions in its agreement; (iv) there is a measureable harm to the Complainant and the community named by the objector." The remedies recommended by the expert panel are similar to those prescribed under the TM-PDDRP. Ultimately, ICANN has the authority to decide whether to impose such remedies.

Public Interest Commitments Dispute Resolution Procedure (PICDRP), allows any person or entity (the "reporter") to file a complaint against a new gTLD registry operator for failure to comply with the Public Interest Commitment(s) in Specification 11 of its Registry Agreement. The Reporter must file a "PIC report" with ICANN by completing an online form.

The PIC Report must (1) identify which PIC(s) form the basis for the report; (2) state the grounds for non-compliance with one or more PICs and provide supporting evidence and (3) state how the reporter has been harmed by the alleged noncompliance. ICANN may undertake a compliance investigation or invoke a "Standing Panel." If the registry operator is found to be not in compliance with its PIC, it will have 30 days to resolve its noncompliance. If the registry operator fails to resolve the noncompliance issues, ICANN will determine the appropriate remedies.

5.2.2.5 Trademark Clearinghouse (TMCH)

The TMCH is a centralized database of verified trademarks from all over the world mandated by ICANN to provide protection to trademark holders under the new gTLDs, established in March 2013. The TMCH performs several important functions, including authenticating and verifying trademark records, storing such trademark records in a database and providing this information to new gTLD registries and registrars. The data contained in the TMCH supports rights protection mechanisms such as Sunrise Services (which provide an opportunity to trademark holders to register domain names corresponding to their trademarks prior to general availability) and the Trademark Claims services (a notification service to domain name registrants and trademark holders of potentially infringing domain name registrations). Registration of a trademark with the TMCH is required to be able to participate not only in the Sunrise Period and Trademark Claims services but also in other registry-specific rights protection mechanisms such as domain name blocking mechanisms like the Donuts' Domain Protected Marks List (DPML) (although it is optional for other RPMs, such as the URS). The TMCH is therefore an important tool to protect trademark rights under the New gTLD Program.

5.2.3 Consideration of these mechanisms: Have they helped mitigate the issues around the protection of trademark rights and consumers in this expansion of gTLDs?

The CCT Review Team looked at whether these mechanisms have helped to mitigate the issues around the protection of trademark rights and consumers in this expansion of gTLDs and have sought to obtain data to help assess the impact of ICANN's New gTLD Program on the cost and effort required to protect trademarks in the Domain Name System.

The CCT Review Team turned primarily to the data obtained by ICANN under the CCT Metrics Reporting[116] and the INTA Impact Study[117] which, it was hoped, would provide additional data on the new gTLD cost impact to brand owners as well as existing data and commentary from the ICANN Rights Protection Mechanisms Review. The CCT Review Team also noted the parallel work by the ongoing Working Groups currently looking into RPMs and sought not to duplicate or undermine their efforts, and looks forward to the reports from those groups.

[116] ICANN, "Competition, Consumer Trust and Consumer Choice (CCT) Metrics Reporting," accessed 10 October 2017, https://www.icann.org/resources/reviews/cct/metrics
[117] Nielsen (April 2017), INTA New gTLD Cost Impact Survey, accessed 24 October 2017, community.icann.org/download/attachments/56135378/INTA Cost Impact Report revised 4-13-17 v2.1.pdf

5.2.3.1 ICANN Rights Protection Mechanisms (RPM) Review

Preliminary conclusions from the ICANN Rights Protection Mechanisms (RPM) Review, conducted by the ICANN organization reporting on 11 September 2015, found that overall the URS has produced positive results in certain limited cases. The speed and low cost caters to those who have clear-cut cases and are indifferent towards the solution of a suspended domain name. However, some rights holders have not opted to use this service due to the "clear and convincing" standard being seen as too strict and the URS remedy being limited to suspension only. There is also concern voiced over the possibility of the domain name being registered once more by another potential infringer once it is released, thus some rights holders feel more comfortable having the domain name in their portfolio, which can be achieved via a UDRP. Indeed, the value of a suspended domain name is questioned.

5.2.3.2 INTA Impact Study

The results of the International Trademark Association (INTA) Impact Study contain important information that more fully informs the community on the impact of ICANN's New gTLD Program on the cost and effort required to protect trademarks in the DNS. INTA members and intellectual property owners have expressed concern on multiple occasions about the New gTLDs on the basis that such expansion would likely create additional and increased costs in enforcing intellectual property rights. The survey sought to assess what additional costs and efforts have been required to protect trademarks in the DNS.
The INTA is a global organization of 6,600 trademark owners and professionals from over 190 countries. As such, it was well placed to respond to a survey from Nielsen which was based on CCTRT input, and INTA members were asked to capture all costs over the past 2 years (2015 and 2016). Their cost estimates include:

- Both in-house and outside legal fees,
- Filing fees,
- Investigation costs,
- The total costs, including benefits, of personnel responsible for these activities.

Respondents who completed this survey reported that compiling the data necessary to properly respond was a significant task. There were 33 respondents in total, including one not-for-profit. Whilst the response rate for the survey is actually above the norm for a similar sample[118] and when considering the level of required effort in completing what was an onerous questionnaire, the sample size of completed interviews is small from a statistical standpoint and requires some caution in its interpretation. Nevertheless, the results are indicative of key themes and trends.[119]

Key Takeaways from the Impact Study:

1. While one of the goals of the New gTLD Program is to increase choice for brand owners, choice does not seem to be a prime consideration for why brand owners elect to register in new gTLDs. Rather, the principal reason why the overwhelming majority (90%) of

[118] This statement is based on Nielsen's general experience with samples of customers or members.
[119] The total sample is sufficient to give directional information about those trends, according to Nielsen, but the exact numbers would still be subject to a high margin of error (the +/- percentage one regularly hears about with polls).

trademark owners are registering domain names in new gTLDs is for defensive purposes - to prevent someone else from registering.

2. Domain names registered by brand owners in new gTLDs are commonly parked and not creating value other than preventing unauthorized use by others.

3. The New gTLD Program has increased the overall costs of trademark defense with internet monitoring and diversion actions being the largest expenditure. These costs have impacted small companies and big companies alike with the most relevant cost-driving factor being the number of brands.

4. Respondents reported that the average total enforcement costs related to TLDs generally (both legacy and new) per company is $150,000 per year. Having said this, the costs varied widely among the survey respondents.[120] This is something that would benefit from further investigation in future surveys.

5. Regarding disputes, more than 75% of cases brought now involve privacy and proxy services and close to 2/3 encounter some level of inaccurate or incomplete WHOIS information.

6. Whilst the new gTLDs account for 1/6 of the enforcement costs they do not yet represent 1/6 of domain name registrations. Otherwise put, the cost of enforcement actions in new gTLDs is approximately 18% of overall TLD enforcement costs whilst the total numbers of new gTLD registrations compared to all TLDs is 10% at the time of the impact study.[121] This data indicates that there is a disproportionate cost associated with new gTLD enforcement actions compared to overall enforcement actions. We therefore have a further indication that there may be proportionately more trademark infringement in new gTLDs than in the legacy gTLDs.[122]

7. RPMs are generally considered to have been helpful in mitigating the risks anticipated with new gTLDs. In response to the question: "Please tell us why you feel the Rights Protection Mechanisms listed above have or have not mitigated the risks involved with new TLDs," the responses were varied but provided a useful insight into the mindset of brand owners responding.[123] Two-thirds of the respondents surveyed feel that the UDRP

[120] The range of total costs reported ran from zero to $5.2 million.
[121] Nielsen, New gTLD Cost Impact Survey (2017). The average costs for all TLDs for 2 years = $292,000. The average costs for new gTLDs for 2 years = $53,690 (approximately 18%).
[122] Nielsen, New gTLD Cost Impact Survey (2017). “Nielsen explains that the figures for internet monitoring being one of the main costs should be qualified—these costs are general overall costs and not specific to new gTLDs. An entity will pay for monitoring across all TLDs. There is likely to be some incremental increase in monitoring costs given additional new gTLDs being ion scope, and indeed there is anecdotal evidence that more brands have started monitoring since the introduction of new gTLDs. However, these costs were not broken down in the questionnaire, monitoring was basically treated as a sunk cost. It would thus be reasonable to assume that these costs have gone up rather than down" Thus the total costs are likely to be above 18%.”
[123] Sunrise - often come with a major cost to the brand owner: Claims - the name is already registered before we are notified; URS - name does not get transferred; narrow criteria for action; PDDRP - criteria are so narrowly drawn that circumstances extremely unlikely to arise; UDRP - criteria are well-defined; there is now a body of helpful case law; transfer of the name is an option. However, price is a deterrent for all but the most egregious cases.
Sunrise period and trademark claim periods are too short; companies need to implement additional measures to watch their portfolio in numerous gTLDs being published week per week.
Some we use and they work. Other not.
URS: it is costly only to suspend (and not transfer) the litigious domain; Post Delegation: very interesting, but difficult and heavy to put in place (joint actions from various TM holders almost required).
Sunrise periods have only a minor effect because many registries target brand owners with discriminatory pricing while at the same time many offer the same domain name to non-brands at a much cheaper price. Claims

and required Sunrise periods have helped mitigate risks, with 90% of respondents registering in new gTLDs during a Sunrise period. Of those who think that RPMs are effective the ranking is as follows:

a. Sunrise 79%
b. UDRP 73%
c. Claims 66%
d. URS 49%
e. PDDRP/RRDRP/PICDRP 27%

There is nevertheless fairly substantial anecdotal evidence that brand owners are reluctant purchasers of Sunrise registrations and many see it as a cost that is overly expensive:

> "Sunrise Periods have quickly become more a money-making product than a protective tool"[124],
> "Sunrise periods have only a minor effect because many registries target brand owners with discriminatory pricing while at the same time many offer the same domain name to non-brands at a much cheaper price"[125]
> "The .top registry raised the Sunrise fee by $30,000 for [company].top. We refused to register"[126]

1. TMCH registrations are used by a majority of the respondents. Looking at the data, the majority of respondents (approximately 9 in 10) registered at least 1 trademark in the TMCH, with 6 in 10 registering 1-10. With regard to associated costs, these vary considerably across the respondents from less than $1,000 to $48,000, with the average being approximately $7,700.

2. The introduction of the URS process has provided an alternative to the UDRP but it is less used. The most cited reasons for why it is less popular include the inability to transfer the domain name after a successful decision and the higher burden of proof.

---

notices do not prevent squatters from registering domain names despite notice of existing rights, which means that the same problems as exist in the legacy TLDs persist in the new gTLDs after registration has occurred. The URS has a fairly high burden of proof compared to the less cost effective UDRP. The PDDRP, RRDRP, and PICDRP can be effective, but are not well understood as available options, leading them to have minor impacts on mitigating risks.
Most of what we have done is defensive registration.
These are good, but incomplete mechanisms. URS is faster than UDRP, but it is more than a matter of "days," - ineffective with really bad malware - and you don't get the domain. UDRP takes a few months. Both are costly. Businesses still need to register defensively at significant cost to protect our customers from misuse of our trusted brands.
We would prefer to have a blocking procedure for trademarks which would greatly mitigate the risks, but in the absence of blocking, the TMCH at least provides a mechanism for us to register domains with our marks before they are squatted. The TMCH claims procedure works only to a minor extent because it only captures filings for a very limited period of time. We find the URS of limited value because of the requirement for multiple domains.
We use UDRP but only have done so with legacy TLDs because an overwhelming volume of infringing domains are in .com.
The Sunrise Period allows trademark owners to purchase a domain incorporating a key trademark before anyone else can. The other mechanisms, however, do not seem that effective and require a significant outlay of resources from trademark owners.
We've not had the opportunity to use.
Registrants are willing to risk a small registration fee to use a domain name with a famous trademark in it." (p. 59).

[124] Nielsen, New gTLD Cost Impact Survey (2017), p. 52.
[125] Ibid. p. 59.
[126] Ibid. p. 50.

3. With regard to premium pricing, three-quarters of the respondents evaluate premium pricing for domain names on a case-by-case basis and 2/3 of their domain name registration decisions have been affected by premium pricing, with .sucks being mentioned the most as a TLD that respondents paid premium pricing for. However, 15% of respondents refuse to pay premium pricing at all.

5.2.4 ICANN Competition, Consumer Trust and Consumer Choice (CCT) Metrics Reporting

5.2.4.1 Numbers of Cases Filed (UDRP and URS)

It is clear from the data obtained by ICANN across all domain name dispute resolution providers,[127] that the total cases filed (UDRP + URS) has increased considerably since the introduction of new gTLDs. Concerning the UDRP, there has been a fairly substantial increase in the number of UDRP complaints filed whilst the use of the URS has been more limited and we have seen a slight decline in cases filed since its introduction and first use in new gTLDs in 2014.
The first new gTLDs entered the root in 2013,[128] but it was not until 2014 that we saw the first UDRP case involving a new gTLD in "Canyon Bicycles GmbH v. Domains By Proxy, LLC / Rob van Eck" and concerning the domain name <canyon.bike>[129] on 14 March 2014. The first URS decision involved the domain name <aeropostale.uno> on 28 April 2014.[130] Taking into account the previous year without any new gTLD related disputes as the baseline, we had a total of 3,371 disputes decided all of which were UDRPs and all of which concerned only legacy gTLDs.

Table 13: The number of cases filed with UDRP and URS providers. [Updated Quarterly] [As of: 3 August 2017]

Year	Total split UDRP and URS	Total cases combined
2013	3,371 (UDRP)	3,371
2014	4,056 (UDRP) & 231 (URS)	4,287
2015	4,130 (UDRP) & 213 (URS)	4,343
2016	4,368 (UDRP) & 222 (URS)	4,590
2017 Q1/Q2	2,112 (UDRP) & 104 (URS)	2,216 (NB for half a year)

Source: Arbitration provider databases
CCT Review Category: Consumer Trust

[127] ICANN, "Competition, Consumer Trust and Consumer Choice (CCT) Metrics Reporting: Rights Protection Mechanisms," accessed 10 October 2017, https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en#1.12
[128] ICANN, "First New gTLD Registries Receive Tokens for Root Zone Management System," accessed 10 October 2017, https://newgtlds.icann.org/en/announcements-and-media/announcement-22oct13-en, first new gTLDs enter the root in October 2013.
[129] WIPO, "Arbitration and Mediation Center Administrative Panel Decision: Canyon Bicycles GmbH v. Domains By Proxy, LLC / Rob van Eck Case No. D2014-0206," accessed 10 October 2017, http://www.wipo.int/amc/en/domains/search/text.jsp?case=D2014-0206, first UDRP decision involving a new gTLD.
[130] ADR, "National Arbitration Forum URS Appeal Determination: Aeropostale Procurement Company, Inc. v. Michael Kinsey et al. Claim Number: FA1403001550933," accessed 10 October 2017, http://www.adrforum.com/Domaindecisions/1550933A.htm, first URS decision involving a new gTLD.

In 2014, we saw the total cases (UDRP and URS combined) rise to 4,287, representing a 27% increase. In 2015, the total cases increased slightly again to 4,343 (1.3% higher than 2014) and in 2016 we saw a further 5.7% increase taking the total cases to 4,590. Thus, comparing total cases in 2013, the year before the first new gTLD dispute, and in 2016, we have a considerable increase of 36% in cases filed across all providers.

If we only look at UDRP cases, we see a 20% rise from 2013 to 2014, a further 2% rise from 2014 to 2015, and a 5.8% rise from 2015 to 2016. If we look at URS cases alone, the first thing to note is that their popularity as an RPM is and remains low with 231 cases in 2014, 213 cases in 2015 and 222 cases in 2016. Thus, around only 5% of the total cases are filed under the URS. In addition, there appears to be no significant rise in the number of complaints filed year on year. We saw a decrease in URS cases filed when comparing 2015 to 2014, and even in 2016 the total number of URS cases filed remained lower than in 2014, the first year of operation for new gTLDs. Thus, this leads one to question whether URS is meeting its potential as a useful RPM.

It is important to note that the number of UDRP and URS cases filed reflect only part of the costs incurred by trademark owners in defending their brands and the bulk of enforcement costs may have been incurred in the form of defensive registrations / blocking/ watching / cease and desist letters and court action, for which we do not presently have data. However, the INTA Impact Study does give some insight into this.

5.2.4.2 Complaints to ICANN Concerning Implementation of UDRP and URS Decisions

ICANN's role is to ensure that the registrars comply with the UDRP and UDRP Rules as well as the URS procedure and rules.

For example, a UDRP provider may file a UDRP complaint that a registrar did not lock a domain subject to a UDRP or respond to the provider's verification request in a timely manner. The Complainant may then submit a complaint to ICANN when the registrar fails to implement a UDRP decision in a timely manner.

With regard to the URS, for example, the registry operator must also lock in a timely manner, and if applicable, suspend the relevant domain name in accordance with the URS determination and the URS procedure and rules. The prevailing Complainant in the URS proceeding and the URS Provider may submit a URS complaint regarding such alleged violations to ICANN via the URS compliance web form.

Looking at the number of complaints made to ICANN concerning the implementation of UDRP and URS decisions,[131] the number of complaints concerning the UDRP declined between 2012 and 2014 by some 65% and since then has remained fairly static at between 250 and 227 complaints annually. URS complaints were relatively high in 2014, the first year in which the URS was available for new gTLDs, but in the last two years (2015 and 2016) the number of complaints has roughly halved.

Table 14: Total UDRP/URS Complaints to ICANN[132]

[131] It should be noted that Complaints regarding the merits of the decision are outside of ICANN's contractual scope.
[132] ICANN, "Competition, Consumer Trust and Consumer Choice (CCT) Metrics Reporting: Rights Protection Mechanisms," accessed 18 October 2017, https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en#1.9.b

Year	UDRP Complaints	URS Complaints
2012	658	
2013	408	
2014	227	19
2015	250	11
2016	235	9
2017 Q1/Q2	122	10

Table 15: Comparing the % of complaints to ICANN in each RPM compared to total number of domain name decisions in each RPM.

Year	URS	UDRP
2014	8%	5.5%
2015	5.1%	6%
2016	4%	5.4%

In 2014, the year that the URS was introduced, there was a relatively high number of complaints to ICANN. When compared to the total number of URS complaints that year, the level was at 8%. This compares to the complaint level for the UDRP in 2014 of 5.5%. The higher level of implementation complaints concerning the URS compared to the UDRP may have been down due to a number of factors including its relative newness, the complexity of the process and recent adoption by registrars.
If we move through 2015 and 2016, we see that the relative number of complaints for the URS decreases and in 2016 the relative number of URS related complaints compared to the UDRP was actually less at 4% compared to 5.4% for the UDRP. It may be that over time, the complexities of the URS had been understood by both registrars, registries and end users.[133]

5.2.4.3 Trademark Clearinghouse (TMCH)

ICANN commissioned Analysis Group to undertake an independent review of TMCH services based on the Governmental Advisory Committee ("GAC") recommendation in May 2011 that a comprehensive, post-launch review be performed.[134] The review sought to assess the strengths and weaknesses of the TMCH services in the light of that recommendation and was based on an analysis of TMCH and third-party data sources, as well as interviews and surveys of TMCH stakeholders. The revised report[135] incorporated public comments into the original report and analyses published on 25 July 2016.[136] According to the report, the data obtained allowed for meaningful observations to be made about the use of the TMCH services studied. The research did not provide quantifiable information on the costs and benefits associated with the present state of the TMCH services. Indeed, the potential costs and benefits of expanding or altering the way the services function, needed a concrete cost-benefit analysis which was outside the scope of the Analysis Group report.

Summary of Findings
With regard to the possibility of extending the Claims Service period or expanding the matching criteria used for triggering the Claims Service notifications, the report found that

[133] ICANN, "Competition, Consumer Trust and Consumer Choice (CCT) Metrics Reporting: Rights Protection Mechanisms," accessed 4 March 2017, https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en
[134] ICANN (26 May 2011), GAC comments on the Applicant Guidebook (April 15th, 2011 version), accessed 15 October 2017, https://archive.icann.org/en/topics/new-gtlds/gac-comments-new-gtlds-26may11-en.pdf
[135] Analysis Group, Independent Review of Trademark Clearinghouse (TMCH) Services Revised Report (2017).
[136] Analysis Group, Independent Review of Trademark Clearinghouse (TMCH) Services Draft Report (July 2016), accessed 10 October 2017, https://newgtlds.icann.org/en/reviews/tmch/ draft-services-review-25jul16-en.pdf

this may actually be of limited benefit to trademark holders. Indeed, such an extension would potentially be associated with increased costs to other stakeholder groups such as registries, registrars, and non-trademark-holder domain registrants. Data limitations prevented definitive conclusions being drawn.

The report noted that given the fact that a cost-benefit analysis had not been performed, a potential extension of the Claims Service or expansion of the matching criteria should consider the inevitable tradeoffs felt by different stakeholder groups. Indeed, the report stressed that when evaluating whether the Claims Service period should be extended, the number of potential registrations affected by the extension needs to be assessed. The effectiveness of the Claims Service notifications depends on how many registration attempts are being made; if there are few registration attempts, then there are fewer potentially-infringing registrations being made.

The report found that registration activity declined after the 90-day Claims Service period ends, thus any additional months added to the Claims Service period will likely have diminishing value.

The report also found that according to the data, trademark holders appeared less concerned about variations of trademark strings and thus felt that an expansion of the matching criteria may in fact bring little benefit to trademark holders. On the contrary, the potential harm towards non trademark-holder domain registrants could be increased. The latter could find themselves deterred from registering trademark string variations that would not be considered trademark infringement.

The report finally considered the Sunrise period and the questionnaire feedback. It seems that whilst trademark holders felt that there is value in the Sunrise periods, and many do use them, having recorded their marks in the TMCH, many trademark holders in fact do not utilize the Sunrise period. The report concluded that this could be due to the expense of Sunrise domain name registrations or because other protections of the TMCH service such as the Claims Service, reduce the need for trademark holders to utilize Sunrise registrations. The CCT Review Team feels that it is also likely due to the sheer number of new gTLDs. Defensive registrations when multiplied across many new gTLDs becomes cost prohibitive and few brand owners are willing to engage in the same way with large scale defensive domain name registrations. The CCT Review Team asked the question whether the extra expense of the TMCH was actually bringing value and not acting as a deterrent itself, being an additional cost for brand owners.

5.2.4.4 Trademark Post-Delegation Dispute Resolution Procedure (TM-PDDRP)

ICANN Contractual Compliance has received no complaints regarding a registry operator's non-compliance with the PDDRP. However, it should be noted that there is currently a GNSO Working Group conducting a Policy Development Process (PDP) to Review all RPMs in all gTLDs that is exploring possible impediments to implementation of the PDDRP since there are no known PDDRP filings with such providers to date.

5.2.4.5 Registry Restrictions Dispute Resolutions Procedure (RRDRP) Decisions

The RRDRP is intended to address circumstances in which a community-based new gTLD registry operator deviates from the registration restrictions outlined in its Registry Agreement. As of, 3 August 2017 there have been no RRDRP cases.

5.2.4.6 Share of Sunrise Registrations and Domain Blocks to Total Registrations in Each TLD

As of 3 August 2017, the only available data on the number of Sunrise registrations compared to total registrations in new gTLDs are from ICANN. According to ICANN there are no consolidated data available regarding commercial blocking services offered by registries. The CCTRT remains open to receive any such data.

Conclusion

The data we have certainly points to increasing numbers of disputes since the introduction of new gTLDs, with disputes rising year-on-year after the introduction of new gTLDs. Indeed, in 2016 the total number cases filed (UDRP and URS combined) was 36% higher than in the year that the first new gTLD entered the route in 2013. (25% if use the baseline as the average of 2012 and 2013)

However, a rising number of domain name disputes is not in itself surprising, with the increased number of domain name registrations worldwide continuing to increase as new gTLDs are introduced to the root and registrations occur.
A more pertinent question to ask is whether there is proportionately more trademark infringement in new gTLDs than in legacy TLDs. This is a more difficult question to answer, as there are many factors involved in assessing trademark infringement where there is simply no data available. The INTA Impact Study is a good example of the complexities of obtaining such information.

In addition to the UDRP and URS, trademark owners also use a variety of other means to deal with abusive domain name registrations, such as court action and cease and desist letters, which are not tracked centrally, nor are the costs associated with such actions available. It is not for ICANN to track or attempt to track such data either. However, ICANN does indeed collect data on the usage of the dispute resolution mechanisms, the UDRP and the URS, across all domain name dispute providers. This data shows that domain name disputes are on the rise. We also have data from ICANN on the number of new gTLD registrations compared to total gTLD registrations (including both legacy and new gTLDs). This data also shows that gTLD domain name registrations are on the rise. However, what we do not have with ICANN metrics is a breakdown of the relative use of UDRPs, that is to say the use of UDRPs in new gTLDs as opposed to legacy TLDs.

Thus, in order to attempt to answer the question of whether there is proportionately more trademark infringement in new gTLDs than in legacy TLDs, we can look at the data from the major dispute resolution provider, WIPO, as this data is publically available.
The WIPO data for 2016, demonstrated that cybersquatting disputes relating to new gTLDs rose to 16% of WIPO's 2016 caseload. Among these, the new gTLDs .XYZ, .TOP and .CLUB were the most common new gTLDs involved in domain name disputes. The legacy gTLDs accounted for 70% of WIPO's caseload. As such, looking at WIPO alone, 18.6% of their gTLD caseload involved new gTLDs. Turning to ICANN statistics on domain name registrations for the end of 2016 we have 196,493,430 gTLD registrations and 27,659,702 new gTLD registrations. Thus new gTLDs account for 14% of the registration volume of gTLDs. From this data, we have a good indication that there is proportionately more trademark infringement presently in new gTLDs than in legacy TLDs.

There is a question mark over whether the URS is a valuable RPM given its low usage compared to the UDRP.
The fact that the TM-PDDRP and Registry RRDRP have not been used to date may on the one hand also bring their existence into question, but may equally underline that their mere existence is acting as a deterrent.[137]

5.2.5 Recommendations

Recommendation 40: An Impact Study in order to ascertain the impact of the New gTLD Program on the cost and effort required to protect trademarks in the DNS should be repeated at regular intervals to see the evolution over time as the New gTLD Program continues to evolve and new gTLD registrations increase. We would specifically recommend that the next Impact Survey be completed within 18 months after issuance of the CCTRT final report, and that subsequent studies be repeated every 18 to 24 months. The CCTRT acknowledges the fact that this was carried out in 2017 by Nielsen surveying INTA members and we encourage that to continue noting that the study needs to be more user friendly.

Rationale/related findings: Costs will likely vary considerably over time as new gTLDs are delegated and registration levels evolve. Repeating the Impact Study would enable a comparison over time.

To: ICANN Organization

Prerequisite or Priority Level: High

Consensus within team: Yes

Details: The evolution over time will provide a more precise picture of costs as they evolve and track the effectiveness of RPMs generally in the DNS.

---

[137] Sources:
Compilation of procedures related sources:
Competition, Consumer Trust, and Consumer Choice Review Team Community Wiki, "Procedures," accessed 5 March 2017, https://community.icann.org/display/CCT/Procedures
ICANN, "Rights Protection Mechanisms Review."
ICANN GNSO, "PDP Review of All Rights Protection Mechanisms in All gTLDs," accessed 5 March 2017, https://gnso.icann.org/en/group-activities/active/rpm
Analysis Group, Independent Review of Trademark Clearinghouse (TMCH) Services Draft Report (July 2016), accessed 5 March 2017, https://newgtlds.icann.org/en/reviews/tmch/draft-services-review-25jul16-en.pdf

Competition, Consumer Trust, and Consumer Choice Review Team Community Wiki, "Procedures," accessed 5 March 2017, https://community.icann.org/display/CCT/Procedures.

Compilation of impact of safeguards and PICs related sources:
ICANN, "Competition, Consumer Trust and Consumer Choice (CCT) Metrics Reporting: Rights Protection Mechanisms," accessed 5 March 2017, https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en

Success Measures: The results of such Impact Studies would provide significantly more data to the relevant working groups currently looking into RPMs and the TMCH as well as future ones, thereby benefitting the community as a whole. Recommendations would then also be able to evolve appropriately in future CCT Review Teams.

Recommendation 41: A full review of the URS should be carried out and consideration be given to how it should interoperate with the UDRP. However, given the PDP Review of All RPMs in All gTLDs, which is currently ongoing, such a review needs to take on board that report when published and indeed may not be necessary if that report is substantial in its findings and if the report fully considers potential modifications.

Rationale/related findings: The uptake in use of the URS appears to be below expectations, so it would be useful to understand the reasons for this and whether the URS is considered an effective mechanism to prevent abuse. It is also important for all gTLDs to have a level playing field. The PDP Review of All RPMs in All gTLDs, which is running in parallel to this CCT Review Team, will contribute to this consideration with its report due in 2018. That Working Group's report needs to be considered to set the scope of any review and potential modifications.

To: Generic Names Supporting Organization

Prerequisite or Priority Level: Prerequisite

Consensus within team: Yes

Details: A review of the URS consider inter alia (1) whether there should be a transfer option with the URS rather than only suspension; (2) whether two full systems should continue to operate (namely UDPR and URS in parallel) considering their relative merits, (3) the potential applicability of the URS to all gTLDs and (4) whether the availability of different mechanisms applicable in different gTLDs may be a source of confusion to consumers and rights holders.

Success Measures: Based on the findings, a clear overview of the suitability of the URS and whether it is functioning effectively in the way originally intended.

Recommendation 42: A cost-benefit analysis and review of the TMCH and its scope should be carried out to provide quantifiable information on the costs and benefits associated with the present state of the TMCH services and thus to allow for an effective policy review.

Rationale/related findings: It seems likely that a full review of the TMCH is necessary including a cost-benefit analysis. The effectiveness of the TMCH appears to be in question. The Independent Review of Trademark Clearinghouse (TMCH) Services Revised Report[138] has not been able to make definitive conclusions due to data limitations and indeed specifically noted that it was unable to perform a cost-benefit analysis of extending the Claims Service or expanding the matching criteria. The PDP Review of All RPMs in All gTLDs, which is running in parallel to this CCT Review Team, will contribute to this consideration with its report due January 2018. That Working Group's report needs to be considered to set the scope of any review and potential modifications.

To: Generic Names Supporting Organization

Prerequisite or Priority Level: Prerequisite

[138] Analysis Group, *Independent Review of Trademark Clearinghouse (TMCH) Services Revised Report* (2017).

Consensus within team: Yes

Details: There appears to be considerable discussion and comment on whether the TMCH should be expanded beyond applying to only identical matches and if it should be extended to include “mark+keyword” or common typographical errors of the mark in question. If an extension is considered valuable, then the basis of such extension needs to be clear.

Success Measures: The availability of adequate data to make recommendations and allow an effective policy review of the TMC.

6 Appendices

6.1 Minority Views on DNS Abuse Paper, rec. 4

While the CCT-RT has been able to achieve unanimous support for most of our recommendations, some members of the RT disagree with the proposal to create a DNS Abuse Dispute Resolution Procedure (DADRP). This statement documents the various rationales for this disagreement:

1. The CCT-RT adopted as a guiding principle that our analysis and recommendations would be based on data. However, there is simply no data supporting the idea of a DADRP. There is nothing to indicate that registry operators are responsible (either directly or indirectly) for abuse within their TLDs; no data that ICANN compliance is incapable of enforcing contractual requirements; and no data indicating that DNS abuse from certain TLDs is targeted at specific third parties who might initiate a DADRP. This recommendation is therefore inconsistent with the data-driven model of the CCT-RT.

2. If anything, the DNS abuse report makes it clear that attempting to mitigate DNS abuse through DNS registries is misguided and ineffective. None of the safeguards required of new gTLD operators appear to have had any effect in reducing the prevalence of abuse, and one of them (DNSSEC adoption) actually appears correlated with *increased* abuse. The fact that abuse prevention through DNS registries is ineffective should not be surprising since registries have no direct relationship with registrants and no mechanism other than suspending a domain (which is not the appropriate approach in all cases) to address abuse. A DADRP that seeks to punish registries for behavior they have no control over by registrants that they have no relationship to is fundamentally misguided and will not address DNS abuse.

3. To the extent that there is a concern that ICANN Compliance may be ineffective at enforcing registries' contractual obligations, the solution should be to improve ICANN Compliance rather than creating a new dispute resolution procedure. Improving ICANN compliance has the benefit of addressing issues across the entire range of registries' and registrars' contracts, whereas the creation of this DADRP at best improves enforcement in one particular area. Creating unique dispute resolution procedures for different portions of the contract is inherently not scalable, as it is not possible to do so for every major component of the contract. Just as importantly, this approach creates a great amount of uncertainty for contracted parties who may find that even though ICANN has investigated an issue and found that they are in compliance with the contract, a third party now disagrees with that assessment and can launch a costly and complex dispute procedure of their own.

4. While DNS abuse is an important topic, the charter of the CCT-RT is only to "examine (A) the extent to which the expansion of gTLDs has promoted competition, consumer trust and consumer choice and (B) the effectiveness of the New gTLD Round's application and evaluation process and safeguards put in place to mitigate issues arising from the New gTLD Round". It is therefore within our scope to review the existing safeguards put in place in the 2012 round, but not to develop completely new mechanisms to address DNS abuse.

Jordyn Buchanan, Carlos Raul Gutierrez, Carlton Samuels, Waudo Siganga

6.2 Individual Statement

Jonathan Zuck
Chairman, CCT-RT

Drew Bagley
Leadership, CCT-RT

October 25, 2017
Re: Submission of draft recommendation for public comment period

Dear CCT-RT Chairman Zuck,

I present for your awareness and broader consideration by the Competition, Consumer Trust and Consumer Choice Review Team (CCT-RT) and the Community, a draft recommendation (hereinafter "Recommendation 5") related to the CCT-RT's findings in the present draft chapter on DNS abuse. Recommendation 5 was not included in the chapter prepared for public comment because the CCT-RT did not have time to adequately discuss, analyze, or determine whether to adopt the recommendation prior to the public comment period. Nonetheless, I request that you please present Recommendation 5 as an addendum to the draft report so that the Community is aware of this potential recommendation and afforded adequate opportunity to provide feedback that may guide the CCT-RT's future analysis of the proposal.

Sincerely,

Drew Bagley

Recommendation 5: ICANN should collect data about and publicize the chain of parties responsible for gTLD domain name registrations.

Rationale/Related Findings: At present, there is no consistent mechanism for determining all of the ICANN contracted and non-contracted operators associated with a gTLD domain name registration. Whois records often do not distinguish between registrars and resellers. The DNS Abuse Study commissioned by the CCT-RT, for example, was unable to discern resellers from registrars to determine the degree to which technical DNS abuse rates may be driven by specific-resellers may affect levels of technical DNS abuse. This data should be available to enhance data-driven determinations necessary for recommendations proposed the CCT-RT, supplement new gTLD program safeguards, and improve ICANN Contractual Compliance determinations.

To: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization, the Subsequent Procedures PDP WG and the SSR2 Review Team, Registration Directory Service Review Team
Prerequisite or Priority Level: High
Consensus within team: ???

Details: Whois information is an important source of data for technical DNS abuse analysis. Safeguards, such as the Thick Whois requirements, do not mandate that resellers are listed in Whois records. Consequently, the full chain of parties to a registration transaction is not readily discernable. Without such information, it is difficult to determine the extent to which technical abuse is correlated to individual resellers, rather than registrars. For example, with

such data obfuscated, it would be possible for a reseller associated with extremely high levels of abuse to remain in operation under a registrar with relatively normal levels of technical abuse. This would, in effect, permit systemic technical abuse by a non-contracted party, though bound by flow down requirements, to go unabated. Whereas, collecting and publicizing such information would enable end users to readily determine the registry, registrar, and reseller associated with a domain name registration to remove the opaqueness of parties responsible for mitigating technical DNS abuse. This would allow for more granular DNS abuse analysis and transparency for Internet users, thereby enhancing community accountability efforts, and contractual compliance enforcement.

6.3 Appendix C: Surveys and Studies

Several surveys and studies were commissioned prior to the launch of the CCTRT to inform its work:

- An Implementation Advisory Group was convened by the ICANN Board in 2013 to examine a series of potential metrics that were proposed by the Generic Names Supporting Organization (GNSO) and the At-Large Advisory Committee (ALAC). This team, referred to as the IAG-CCT, evaluated the feasibility, utility and cost-effectiveness of adopting several recommended metrics produced by these two groups and issued a set of 66 metrics, which the ICANN Board adopted for the CCTRT to consider.[139] ICANN has been collecting data on many of these metrics.[140] Of the 66 recommended metrics, several included baseline figures that capture a snapshot of behaviors and activity in the domain name marketplace prior to the saturation of new gTLDs. Depending on the metric, the baseline period may span from one year to multiple years prior to the delegation of new gTLDs.
    - The IAG-CCT determined that a subset of the metrics was best evaluated using a consumer and registrant survey. Nielsen's Wave 2 Consumer Survey results were released in June 2016.[141] The study measured Internet users' current attitudes about the gTLD landscape and the DNS, as well as changes in these consumers' attitudes from Nielsen's Wave 1 Consumer Survey, which was conducted in 2015.[142] Internet users were asked about aspects of consumer awareness, consumer choice, experience and trust. The consumer survey's respondents included a representative sample of Internet users from all five ICANN regions and was conducted in each sampled country's relevant language. Results of the Phase 2 study revealed more than half of respondents (52%) were aware of at least one new gTLD, and overall, trust of the domain name industry relative to other technology-related industries has improved.
    - Similarly, Nielsen conducted a global domain name registrant survey, which targeted those who have at least one registered domain name. Survey participants were questioned about their awareness of new gTLDs, as well as their perceived sense of choice, experience and trust related to the current gTLD landscape. Nielsen's Wave 1 Registrant Survey results were issued in September 2015.[143] The CCTRT received the Wave 2 Registrant Survey results on 15 September 2016.[144] Results revealed that new gTLDs included in both phases of the survey have similar awareness levels, with higher awareness reported in South America and Asia Pacific, and that trust in the industry generally remains high, particularly in Asia.

[139] Implementation Advisory Group for Competition Consumer Trust and Consumer Choice (26 September 2014), *Final Recommendations on Metrics for CCT Review*, accessed 20 January 2017, https://community.icann.org/display/IAG/IAG-CCT+report
[140] ICANN, "Competition, Consumer Trust and Consumer Choice (CCT) Metrics Reporting," accessed 25 January 2017, https://www.icann.org/resources/pages/cct-metrics-rpm-2016-06-27-en
[141] Nielsen, *ICANN Global Consumer Research Wave 2* (June 2016), accessed 30 January 2017, https://www.icann.org/news/announcement-2-2016-06-23-en
[142] Nielsen, *ICANN Global Consumer Research* (April 2015), accessed 30 January 2017, https://www.icann.org/news/announcement-2015-05-29-en
[143] Nielsen, *ICANN Global Registrant Survey* (September 2015), accessed 30 January 2017, https://www.icann.org/news/announcement-2015-09-25-en
[144] Nielsen, *ICANN Global Registrant Survey Wave 2* (August 2016), accessed 30 January 2017, https://www.icann.org/news/announcement-2-2016-09-15-en

- A second subset of IAG-CCT metrics aims to measure competition in the new gTLD space based on an analysis of pricing data and other, non-price-related indicia. ICANN engaged Analysis Group to conduct an economic study which had two primary aims: gauge the pricing practices for domains in new gTLDs against those in the legacy space; and provide a qualitative analysis of other non-price competition indicators, like technical or other business innovations. Analysis Group's Phase 1 Assessment results were delivered in September 2015.[145] Analysis Group's Phase II Assessment describes how the competition metrics established in the Phase I Assessment have changed (or remained the same) as the New gTLD Program expanded over the course of one year.[146] Results of the Phase II economic study, which were delivered in October 2016, revealed a decline in the share of new gTLD registrations attributable to the four and eight registries with the most registrations, and also revealed volatility in the registration shares held by registry operators. CCTRT members provided feedback to Analysis Group on its methodology and approach prior to beginning the Phase II analysis.

- To help the CCTRT assess the effectiveness of the New gTLD Program's application and evaluation processes, as well as safeguards put in place to mitigate abuse, ICANN collaborated with the community to generate the following reports:
  - The "Revised Program Implementation Review" published in January 2016 examines the effectiveness and efficiency of ICANN's implementation of the New gTLD Program from the staff perspective;[147]
  - The "Revised Report: New gTLD Program Safeguards Against DNS Abuse" explores methods for measuring the effectiveness of safeguards to mitigate DNS abuse that were implemented as part of the New gTLD Program. It outlines which activities may constitute DNS abuse and provides a preliminary literature review examining rates of abuse in new gTLDs and the DNS as a whole.[148]
  - The "Revised Report: Rights Protection Mechanism Review" evaluates data on key protection mechanisms such as the Trademark Clearinghouse, the Uniform Rapid Suspension System and Post-Delegation Dispute Resolution. The interaction between Rights Protection Mechanisms and other elements of the New gTLD Program are also considered.[149]

- To supplement the existing data, the CCTRT requested additional surveys and studies to further inform its work:

[145] Analysis Group, *Phase I Assessment of the Competitive Effects Associated with the New gTLD Program* (September 2015), accessed 30 January 2017, https://www.icann.org/news/announcement-2-2015-09-28-en
[146] Analysis Group, *Phase II Assessment of the Competitive Effects Associated with the New gTLD Program* (October 2016), accessed 30 January 2017, https://www.icann.org/news/announcement-2016-10-11-en
[147] ICANN, *Program Implementation Review* (January 2016), accessed 30 January 2017, https://www.icann.org/en/system/files/files/program-review-29jan16-en.pdf
[148] ICANN Operations and Policy Research, *New gTLD Program Safeguards Against DNS Abuse: Revised Report* (July 2016), accessed 30 January 2017, https://www.icann.org/news/announcement-2016-07-18-en
[149] ICANN, *Rights Protection Mechanisms Review: Revised Report* (September 2015), accessed 30 January 2017, https://newgtlds.icann.org/en/reviews/rpm/rpm-review-11sep15-en.pdf

- The Competition and Consumer Choice subteam requested from Analysis Group and the ICANN organization additional data points on pricing and registration analyses to help answer research questions on the effectiveness of new gTLDs' expansion in promoting price competition among gTLD operators as well as among registrars and resellers.

- The Competition and Consumer Choice subteam sought legacy gTLD parking data to complement the new gTLD parking data available on ntldstats.com. The parking data allowed the subteam to carve out a more accurate picture of registrations in each registry, by removing those registration numbers which do not reflect "active" registrations. On a separate note, the Competition and Consumer Choice subteam obtained ccTLD registration data from CENTR and Zooknic.

- At the request of the Review Team, ICANN contracted with SIDN to conduct a study analyzing rates of abusive, malicious and criminal activity in new and legacy gTLDs. The "Statistical Analysis of DNS Abuse in gTLDs" study compares rates of these activities between new and legacy gTLDs, as well as employs inferential statistical analysis to measure the effects of DNSSEC, domain parking, and registration restrictions on abuse rates using historical data covering the first three full years of the New gTLD Program (2014 – 2016).[150]

- At its third face-to-face meeting in June 2016, the CCTRT requested that an applicant survey be commissioned. In addition to addressing topics pertaining to competition, consumer choice and trust, the survey was also tasked with reviewing the effectiveness of the application and evaluation process of the New gTLD Program. The CCTRT sought answers to gain a better understanding of applicants' views on the application process among those who completed the process, are actively in progress, and those who withdrew their applications.

- To help inform its assessment of the application and evaluation process, the CCTRT requested that AMGlobal research and conduct interviews with firms, organizations and other institutions that did not apply for new gTLDs, but who may have been considered good candidates for the program as cohorts of similar entities that did apply from the developed world.[151] The purpose of this research was to obtain a deeper understanding of consumer awareness of the New gTLD Program, as well as why more firms from the developing world did not apply to the program. The report was delivered in November 2016 and included recommendations such as creating outreach tools for non-expert audiences answering their key questions on cost, application process, timing and ICANN itself, another recommendation was to provide the community with a full explanation on the different uses for new gTLDs, answering business model/use case questions

[150] SIDN Labs and the Delft University of Technology (August 2017), *Statistical Analysis of DNS Abuse in gTLDs Final Report*, accessed 23 October 2017, https://www.icann.org/en/system/files/files/sadag-final-09aug17-en.pdf
[151] AMGlobal Consulting, New gTLDs and the Global South: Understanding Limited Global South Demand in the Most Recent New gTLD Round and Options Going Forward (October 2016), accessed 25 January 2017, https://community.icann.org/pages/viewpage.action?pageId=56135383

the community might have. Regarding future application rounds, the report proposed to develop additional research on the best ways to reach the general public in the Global South and build dialogue around new gTLDs in the public-private sphere; to the greatest extent possible, start preparing the public for the next round as soon as possible.

- In addition, the CCTRT used the results from a survey commissioned by the International Trademark Association (INTA). The survey, conducted between January and February 2017, assembled information from 33 INTA corporate members, non-INTA corporate members and IP owners who responded to questions on the costs incurred by their clients related to the expansion of the TLD space. The survey, which was sent to 1,096 potential respondents, provided insight into these trademark holders' experiences with the Program.[152]

[152] Nielsen (April 2017), INTA New gTLD Cost Impact Survey, accessed 24 October 2017, community.icann.org/download/attachments/56135378/INTA Cost Impact Report revised 4-13-17 v2.1.pdf

6.4 Appendix E: Participation Summaries

Name	Affiliation	Meetings Attended (Total # of Plenary Meetings & Face-to-Face Meetings: 65 - through September 2017)
Calvin Browne	GNSO	52
Carlos Raul Gutierrez	GNSO	46
Carlton Samuels	ALAC	48
David Taylor	GNSO	47
Dejan Djukic	ccNSO	51
Drew Bagley	Independent Expert	61
Fabro Steibel	Independent Expert	28
Gao Mosweu	ccNSO	49
Jonathan Zuck	GNSO	55
Jordyn Buchanan	GNSO	61
Kaili Kan	ALAC	59
Laureen Kapin	GAC Chair rep.	58
Megan Richards	GAC	48
N.Ravi Shanker (resigned 10/18/17)	Independent Expert	2
Stanley Besen (resigned 6/25/17)	Independent Expert	33
Waudo Siganga	GNSO	53
Jamie Hedlund	ICANN President and CEO rep.	49

Name	Affiliation	Competition and Consumer Choice Subteam (22 Meetings through Sept. 2017)	Safeguards and Trust Subteam (26 Meetings through Sept. 2017)	Nielsen Subteam Meetings (4 meetings through Sept. 2017)	Application and Evaluation Process (3 meetings through Sept. 2017	INTA Subteam Meetings (3 meetings through Sept. 2017)
Calvin Browne	GNSO	2	14			
Carlos Raul Gutierrez	GNSO	5	13	2		0
Carlton Samuels	ALAC		17			2
David Taylor	GNSO	1	14			3
Dejan Djukic	ccNSO	19			1	2
Drew Bagley	Independent Expert	2	23		0	
Fabro Steibel	Independent Expert		11	3		
Gao Mosweu	ccNSO		22		1	
Jonathan Zuck	GNSO	18	18	3	2	
Jordyn Buchanan	GNSO	22		3	1	3
Kaili Kan	ALAC	16				
Laureen Kapin	GAC Chair rep.		22	2	2	
Megan Richards	GAC	12			0	
N.Ravi Shanker (resigned 10/18/2017)	Independent Expert					
Stanley Besen (resigned 6/25/17)	Independent Expert	13	1	1		
Waudo Siganga	GNSO	16		2	1	1
Jamie Hedlund	ICANN President and CEO rep.	6	13		0	

The statements of interest of the Review Team members can be found at https://community.icann.org/display/CCT/Composition+of+Review+Team.
The email archives can be found at https://community.icann.org/display/CCT/Email+Archives.