



# NEW gTLD Program

## CONSULTATION SUMMARY

### SYDNEY, NEW YORK AND LONDON EVENTS

#### EXECUTIVE SUMMARY

Following a public forum and new gTLD consultation session conducted during the ICANN meeting in Sydney (June 24, 2009), ICANN conducted two additional one-day live consultation events, one in New York on July 13, 2009 and one in London on July 15, 2009, to engage the global Internet community in discussions on workable solutions to the outstanding matters identified for consideration regarding the New gTLD program, with particular focus on trademark protection and malicious conduct. Each session had an estimated number of attendees ranging from 140 to 170. All events were broadcasted live with an average of 45 remote participants.

At these sessions, ICANN staff provided attendees with an overview of the progress made to date in developing the New gTLD Program and then attendees heard from speakers who have been actively participating in the process. With respect to trademark protection, speakers included members of the Implementation Recommendation Team (IRT) who reported to the ICANN Board with proposed measures for protecting intellectual property, the World Intellectual Property Organization (WIPO), Paul Keating and Demand Media. The IRT group was formed per ICANN Board Resolution in June 2009, but is not the only source of input ICANN is considering. The malicious conduct discussions included presentations from a number of information security experts, including Registry Internet Safety Group (RISG), Afilias, Anti-Phishing Working Group (APWG), HSBC's Fraud Risk and Intelligence Group and other banking/finance associations. Presentations at each session were followed by an extensive question and answer segment with oral and written feedback opportunity.

The purpose of this posting is to provide a summary of the transcripts for each of these sessions, organized by the new gTLD topics and subtopics that were discussed. The full texts of the transcripts of the Sydney, New York and London global consultation sessions are also posted on ICANN's website. Also included here are compilations of the written feedback forms completed by attendees of the New York and London events. A short summary of the responses received can be viewed below.

ICANN has analyzed and considered the community feedback received to date during these global consultations, together with public comment forums and other input from the global Internet community. The proposed solutions under consideration are published for community input alongside the Applicant Guidebook version 3.

## Summary Feedback Forms – New York and London Consultation Events

<b>Proposal</b>	<b>Feedback Forms Summary (NYC/London)</b>
<b>IP Clearinghouse</b>	Broadly Support - 58 Broadly Opposed - 6 Undecided - 0
<b>Globally Protected Marks List</b>	Broadly Support - 40 Broadly Opposed - 24 Undecided - 0
<b>Uniform Rapid Suspension System</b>	Broadly Support - 54 Broadly Opposed - 7 Undecided - 0
<b>Post-Delegation Dispute Resolution</b>	Broadly Support - 48 Broadly Opposed - 4 Undecided - 2
<b>Thick Whois</b>	Broadly Support - 57 Broadly Opposed - 2 Undecided - 1
<b>Expansion of String Comparison</b>	Broadly Support - 43 Broadly Opposed - 1 Undecided - 2

## General

### Sydney

#### Free speech concerns

With regard to how much the IRT considered the bounding of the IRT/trademark issues by free speech law (inquiry by G. Chynoweth), the IRT considered public comments as well as discussions with and presentations by a diverse set of groups. M. Wong. Free speech was very much a part of the concern that the IRT was trying to accommodate in doing its balancing. The best example of how the IRT kept in mind freedom of expression concerns is shown by the GPML not being a “reserved list.” Many trademark owners wanted it to be. The GPML was intentionally designed to provide opportunities at the top and second level for those who may have a right or legitimate interest in using a term that corresponds, based on free speech or some other right or legitimate use that is protected under the respective national law. *K. Rosette.*

#### Broader policy concerns

There could be an increase in child pornography and criminal activity following release of the new registries. Other e-crime problems need to be looked at, including web hosting security issues and cybersquatting scenarios. *P. Foody.*

#### IDN

It is important to keep in mind the IDN perspective as these issues are debated, not just the pure trademark perspective, and to ensure fair processes. *K. Fattal.*

#### IRT recommendations

The IRT recommendations are up for discussion, they are not perfect and the IRT team looks forward to comments on the final report. *D. Taylor.*

### New York

#### Transcript Summary

#### Trademark and TLD strings

You cannot trademark a string, and the policy of the U.S. Patent and Trademark Office is that a TLD string cannot, in and of itself, be a trademark. That’s not saying that a three-letter designation can’t infringe on someone’s trademark. Further, the reality is not that the GPML will take a lot of generic words out of circulation. Rather, if there is a match to a GPML at the top level, it’s initially blocked, but there is a reconsideration process so that if someone wants to use, e.g., a .time that has nothing to do with Time magazine, then they could through reconsideration get the use of it. There is a lot of rhetoric around, but that is not the reality of what is in the report. *J. Neuman responding to D. Younger.*

#### Registry responsibility

Policies development should lead to registries policing their own space; it should not be incumbent on trademark owners only. When we have registries that care about their space then they will take enforcement measures on their own. *A. Van Couvering.*

#### Cybersquatting

Cybersquatting is not limited just to big corporations; many other organizations (e.g., nonprofits) can be victims as well and that activity also impacts consumers. *L. Goodendorf.* Cybersquatting initially referred to registering the dead-on mark in a domain name, and then calling the trademark owner asking about

the sale of it. It has morphed beyond that into other practices, such as typo squatting. **Male unidentified** responding to P. Fudey.

### **New gTLD timing**

The processes that the IRT recommended need to be in place before an unlimited number of new gTLDs are opened up. L. Goodendorf. The protection mechanisms worked on by the IRT should be implemented in the next Applicant Guidebook so that we have a chance to evaluate whether they will actually protect consumers and brands. F. Feldman. All of the IRT recommendations should get implemented, but with additional protections for trademark owners. Further, all of the overarching issues should be fully addressed before ICANN moves forward to roll out new TLDs. P. Flaherty. ICANN is taking steps to ensure that the right amount of thought occurs and amendments are made to the Applicant Guidebook before the new TLD process is implemented. K. Pritz.

### **Protection of company names**

Protection of company names should be looked at, because opportunistic domainers who can afford the filing fees will go out and try to grab them. Before you open Pandora's box you better make sure that good protections are in place. D. Neuger.

### **Problems for brand holders outside the domain space**

Brand owners likely will not disagree that there are problems outside the domain space –e.g., the root cause of the problems that are being dealt with at the string level, i.e., some search engine practices (typo squatting and pay per click); those issues were not within the IRT's scope but could be raised before ICANN and others. R. Panghorn responding to E. Brunner-Williams.

### **Define top-level domain**

We need a logical expansion of the namespace and we should be looking for apex names rather than allowing just any name to come forward. It is important for ICANN to define what a top level domain is; it should be the apex of a well-defined human activity, community or sector. The Applicant Guidebook needs to be clear on this issue. It can be addressed and clarified with regard to confusingly similar strings. This issue has a lot to do with trademark holders, Internet security and stability, and the ICANN compliance dealing with all of that. R. Andruff.

### **Purpose of IP law**

Trademark law is actually consumer protection law, allowing consumers to see the origin of goods and services so that there is credibility on what consumers are buying. F. Vayra responding to P. Fudey.

### **Economic studies**

We don't have a very good economic analysis of what the true impact of new gTLDs is not only for registries and registrars but also for individuals and companies. Given that this is a marketplace that serves trillions of dollars of e-commerce, ICANN needs to help us there. F. Feldman.

### **Costs**

The new gTLD program raises substantial concern about costs to businesses, such as a need to file many defensive registrations, making this program like a nuisance tax which many companies cannot afford. P. Lee. It has not been the case with the TLDs other than .com that there has been a lot of defensive activity. R. Tindal. About 80% to 90% of Time Warner's registrations are defensive, which is a lot of dead space that among other problems is costing money year after year. F. Vayra.

### Costs study

A study should be conducted of how much this will cost trademark owners over time using all of the additional protections that are being offered. *P. Flaherty*.

### Fee shifting - escrow

ICANN should consider requiring some type of escrow or other account where registrants pay in so that if they are later challenged there is money to compensate the trademark owners appropriately. At present there is a disproportionate fee burden on trademark owners. *B. Solomon*. That escrow proposal would be a blunt instrument that would penalize the 99% of registrants who are not infringers. *R. Tindal*. The system could involve a mechanism like a credit card – you don't get charged if you don't infringe.

### Male unidentified.

### Costs to brand owners

The IRT report provides that brand owners would pay into the clearinghouse, which would get them onto things like the GPML, and brand owners have to pay again to basically recertify that their brands are in continuing registration form. *K. Pritz* responding to *chat room* query.

### German companies issue

In its deliberations about the regions for the GPML, the IRT did not consider the situation of German companies that cannot do business in the U.S. and Canada due to treaty issues coming out of WWI.

**Female** responding to *R. Horowitz*.

### Auctions

If an auction is used to settle competition among applicants, the highest bidder might not be the most legitimate owner. Are big corporations always the most legitimate? *J. Carr*. That is a question for ICANN in the broader context of the new gTLD program. With regard to the GPML that the IRT dealt with, if there is an initial rejection there would be opportunity for reconsideration. As I understand it you can only have one TLD for a particular string; you cannot have different people using the same string in 30 different places. *K. Rosette*.

### Opposition to new gTLD rollout

The National Basketball Association and other sports leagues (Major League Baseball, the NFL and National Hockey League) do not support the proposed rollout of unlimited gTLDs. If they are rolled out on this scale, it is critical to adopt comprehensive solutions and effective tools aimed at preventing the infringement of trademarks and allowing effective enforcement against those who violate IP rights. *S. Tarrant*.

### GPML: ownership of registrations by multiple companies within same corporate family

There should be a mechanism whereby at least within ownership among the same corporate family that you would have one entity applying for the GPML status and then referring to all the other marks owned by related entities and you would have to have supporting documentation. There is acute awareness of some of the holding company structures put into place for tax purposes. *K. Rosette* responding to *R. Max*.

### Closed TLDs

A closed TLD could have rights protection mechanisms that are much stronger than the rights protections being recommended by the IRT and therefore wouldn't necessarily need what the IRT is recommending. *J. Neuman* responding to *D. Tobin*.

## Background on new gTLDs process

New gTLDs have been talked about since the beginning of ICANN. One of the objectives of ICANN's formation was to open up the domain space to provide increased competition both for registrars and gTLD registries. There were two trial runs where new TLDs were introduced into the DNS, one in 2001 and one in 2003. ICANN's main policymaking body, the Generic Name Supporting Organization, undertook a two-year intensive policy development process about the introduction of new TLDs, and made 19 recommendations that were approved by the ICANN Board.

Four themes of the GNSO recommendations were: (1) new TLDs should benefit registrants; (2) there should be increased user choice; (3) there should be increased competition; and (4) the introduction of internationalized domain names should be allowed so that communities can participate fully in their regions. A further consideration was that new TLDs should not disrupt DNS stability or security, and to primarily address that through formulation of string criteria. Also, it was made clear that certain very important interests would need to be identified with specificity and be protected through appropriate objection and dispute resolution processes. Also, the process should be cost-neutral and that the process for applying should be clear and predictable.

The Applicant Guidebook seeks to be straightforward, while at the same time taking very specific instances and making them the subject of scrutiny and objection as appropriate (e.g., strings that incite malicious behavior, infringe the rights of others, or are misappropriation of a community label). If an application fails at the initial evaluation an applicant can enter into an extended evaluation. Independent bodies can settle disputes and there is an avenue for resolution if applicants apply for the same string.

ICANN so far has published two versions of the Guidebook, both of which have been subject to extensive public comment. ICANN intends to have another version of the Guidebook published in September which will be open to another round of public comment, targeting toward publishing the final version of the Guidebook in December where we can launch the TLD process.

ICANN also identified four overarching issues—those where we recognize that considerably more community discussion needs to be held and about which consultations with experts are appropriate. Those four issues are trademark protection, ensuring that the new TLDs don't become an amplifier for malicious conduct, the market impacts of increased numbers of gTLDs, and the impact on the root zone of what's turned out to be nearly the coincident introduction of new TLDs, IDNs, IPv6 and DNSSEC. This session will review the activities that ICANN staff has undertaken with expert groups and with community input regarding the development of solutions for each of the four overarching issues. *K. Pritz.*

## Unaddressed but important items

IRT wanted to put a marker down on some issues it did not have time to address but which it deems important, such as development of universal standards and practices for proxy domain services, and that applicants be allowed to apply for more than one character string in an application (e.g., apply for .toys in ASCII and Kanji or Arabic and Cyrillic, rather than having to file multiple applications for essentially the same string of different characters). *K. Rosette.*

## London

### Transcript Summary

With the imminent introduction of new gTLDs, ICANN is holding conferences focused on a few very important issues—i.e., protection for trademark holders, and prevention and mitigation of malicious conduct. These meetings are intended to discuss the merit of various solutions that have been proposed

or to develop new solutions. One of ICANN's missions is to define and implement a strategy for the introduction of new gTLDs, and fostering choice and competition is one of ICANN's key objectives.

After two trial rounds of introducing some new TLDs (in 2000 and 2003) some general principles were developed by the GNSO and approved by the ICANN Board to guide the process of introducing more gTLDs. The whole new gTLD process is to be cost neutral to ICANN.

The Applicant Guidebook is the instruction manual for how to apply for new gTLDs. It is meant to be as clear and predictable as possible but also has to be robust enough to deal with edge cases (e.g., a string that might incite malicious behavior or infringe someone's rights). The guidebook is divided into modules that mirror the process. The guidebook has been put out in draft form and is subject to comment by the community.

These conferences are addressing higher level overarching issues raised by the new gTLD process that require further community consultation – e.g., trademark protection, ensuring that malicious conduct won't be multiplied with the new gTLDs, marketplace issues and the impact of new TLDs on the root zone. It is not for ICANN staff to resolve these issues; rather ICANN convened experts to aid in the process of considering these issues and through them ICANN is reaching out to the community to have this discussion.

In the trademark area the discussion is not new, so a lot of the work is refinement and improvement and regularization. Regarding malicious conduct we have had many participating groups. For the root zone scaling study we will provide a status report. Finally, economic studies have been undertaken. They indicate that there are costs associated with the introduction of new TLDs and that ICANN should act to mitigate those having to do with trademark protection and malicious conduct. The economic study also identified benefits associated with new TLDs. *G. Rattray.*

### **Next steps and next version of Guidebook**

What goes into the Draft Applicant Guidebook is a proposal for community discussion. If policy work is one of the recommendations that come out of the staff analysis so that the recommendations are adopted by all gTLDs, then there are lots of ways of triggering policy development work in ICANN. Different entities can request it. *K. Pritz* responding to *P. Corwin* query.

### **Overarching issues**

Three of the overarching issues are spurious. The issue is trademarks. There has been no evidence that malware is going to function better in new gTLDs than in old. ICANN has already conducted studies on root scaling. Regarding the economic study, it would be extremely shortsighted to look at economic value as a threshold for introducing new gTLDs. E.g., regarding IDNs, there may be very little economic value to some of them, but there is a strong value in them from other perspectives. We all want one Internet and we need to respond to people who want to be part of that Internet. Trying to read the tea leaves of the future and prove economic demand, when in fact we have lots of indicators that there is, is a spurious issue. *A. Van Couvering.*

### **User education**

Users need to be educated about what they can and cannot do on the Internet. They don't all know the legal background on brands, so having a new rule and linking the new gTLDs to a new legal means for everyone to defend their rights is very important. *C. Perrion.*

## Global engagement and advance thinking about impact of new gTLDs

It is important to consider how implementation of the new gTLD program, and all its component parts, will play out in different parts of the world, in different jurisdictions. This should be thought through in advance. ICANN should engage with non commercial and human rights and civil society groups around the world (e.g., perhaps do case studies on certain language groups and geographical regions) about how the new Applicant Guidebook and IRT recommendations would play out around the world. Will this result in facilitating greater communication of people around the world in different languages and give disadvantaged communities a voice, or will there be unintended consequences. *R. MacKinnon.*

## Demand for new gTLDs

There seem to have been a lot of statements from ICANN that there's a tremendous demand for new TLDs, but we find that it's unsupported except from registrars and registries supporting new gTLDs. The IRT seems to be used as a buffer between ICANN and the dissatisfied trademark community. *K. Christiansen.*

## New gTLD demand and timing

Regarding claims that the new gTLDs process is "rushed," the process for new gTLDs has been going on in a detailed way for three years and a lot of trademark owners know about this process. The plan is that the application window would open in the first quarter of next year but ICANN has said that the four overarching issues, one of which is trademark protection, need to be properly addressed. The Board has said it will not force the timeline if those issues aren't properly resolved. Regarding demand, it exists and is coming from a wide range of interests. *R. Tindal.*

## Costs of remediating abuse

Costs of domain name system abuse go beyond what rights owners have to expend to defend their brands; they extend to lasting and immeasurable harm to consumers who collectively lose billions of dollars and in extreme cases their health and safety. *C. Jamieson.*

## ICANN mission and trademark protection

When ICANN was formed the white paper did state that it should take into account the protection of trademarks and trademark rights. The reason the UDRP was brought in was due to rampant cybersquatting which was threatening the stability of the Internet. *J. Cohen* responding to *chat room* query. One of the 19 implementation guidelines for new TLDs addresses protecting the rights of others. The JPA also puts the issue of rights protection in the charter writing. The debate is not whether or not there should be trademark protection but about the form of the protection. *R. Tindal.*

## Process dominance by large trademark interests

The experience of the UDRP has shown that people with deeper pockets tend to win. There has not been enough effort to push back against this. If the process is dominated by trademark interests there will be a real problem for legitimate registrants that "offend" the sensibilities of well-heeled trademark owners who will beat up on them. The promise of the Internet is that it flattens the world so that people from small communities can take their place in the world. If there is a trademark threat over them, that does not serve ICANN's mission and the mission of the Internet very well. *J. Levine.*

## Focus on pay per click

There are only two or three pay per click clearinghouses in the world. Efforts should be directed at them, rather than trying to figure out some enormous process that will touch every single one of the many millions of domain names throughout the world. *J. Levine.*



## ICANN role

There is a lack of clarity about what problem is to be solved. It is unclear why ICANN has to manage the IP Clearinghouse and GPML, which are basically of benefit to trademark holders. *J. Levine.*

## Clarify role of proxy registrants

Thick Whois will not be very effective unless the role of proxy registrants is clarified. *J. Levine.*

## Timing of new gTLD launch and establishing policies

It is important that we have proper controls in place before the launch of new gTLDs, instead of playing catch up later. *M. Sutton.*

## Trademark Protection

### IRT

#### New York

#### Transcript Summary

#### IRT process and input from constituencies

ICANN is taking input from all constituencies on the IRT recommendations and will synthesize that input and publish it in a version of the guidebook that is available for public comment. [**K. Pritz?**] responding to *S. Johnson.*

#### IRT members' travel expenses

ICANN is reimbursing some IRT members' travel expenses to attend these consultations. *K. Pritz* responding to *chat room* query.

#### IRT recommendations

The IRT, which was formed by the ICANN Intellectual Property Constituency at the request of the ICANN Board, made a number of key recommendations: the IP Clearinghouse, the Globally Protected Marks List and IP Claims, the Uniform Rapid Suspension System (URS), the Post Delegation Dispute Resolution Mechanism, Thick Whois and the expansion of tests for string comparison during initial evaluation. *C. Chicioine.* Many of the IRT recommendations are things that exist today in various forms with existing areas on the Internet. E.g. the IP Clearinghouse was successfully used with the .eu and .asia rollouts. The URS exists in another form with Nominet and .uk. Thick Whois is not a very controversial norm. So implementing the IRT recommendations generally would not require blazing new trails. [**Male not identified.**]

#### IRT recommendations put registrants' domain names at risk

The IRT proposals account for only trademark infringement abuses but not trademark lawyer abuse. Both sides of the abuse issue must be investigated and both sets of abuses must be mitigated in the next version of the trademark protection proposals. The IRT proposals also go beyond ICANN's mission and the bounds of existing trademark law. *C. Climen.* The IRT suffers from trademark abuse. It is also important to note that proposed policies of the IRT are administrative and are not intended to give trademark owners greater rights than they have in the real world. *J. Berryhill.* The IRT is entirely slanted toward interests of very large corporations, and it has proposed to take the place of national courts and bodies that deal with international trademark treaties, and to also create two classes of trademark holders (i.e., the rich get treated differently from those who are not rich). *J. Saltzberger.* The IRT recommendations do not go far enough; they do not prevent the most rampant form of cybersquatting,

which is typosquatting or use of your mark with a generic term that is relevant to your business. *B. McMurtrey.*

## Feedback Form Summary

### IRT recommendations—support

We support the thrust of the IRT report with one major caveat—that it should be a baseline for what are the protections. If new gTLDs go forward, there have to be at least the level of confidence-building measures found in the IRT report, or else there will be chaos, economic damage, and a lot of frustrated users and consumers. *M. Bohannan.*

### Closed gTLDs

While the IRT professes a desire to protect rights of trademark owners, it suggests that closed gTLDs can be exempt from rights protection mechanisms for second level domains. This registry for a closed gTLD could permit the use of a second level name that incorporates a world famous one. For example, if Panasonic .gTLD were the subject of a closed registration system the IRT approval would permit registration of Sony.Panasonic. *Law Firm.*

### Support with comments

Verizon supports the IRT recommendations as modified by our filings on the record. *P. Flaherty & M. McKeenan, Verizon—Large Corporation.*

I am in support of these IRT recommendations (broadly) - Electronic data clearing house. - Rapid takedown. Against: - Global marks list. - Post-delegation procedure. *Registry.*

Many brand owners oppose the gTLD expansion, and I agree that there is reason for skepticism about whether the costs of this expansion will outweigh any benefits. In any event, if the expansion is to happen, the IRT report reflects a well considered, balanced set of proposals to try to prevent some of the most inappropriate behavior and balance trademark interests with due process needs. *D. Bernstein, Debevoise & Plimpton LLP—UDRP Panelist.*

### Process

Thanks for the opportunity to see the transparency of the process. *J. LeMan, Lord, Abbett & Co.—Small Business.*

### Push back new gTLD proposed launch date

ICANN should strongly consider pushing back the current proposed launch date of first quarter 2010 for the initial round of new gTLD registrations given the substantial number of issues, both in IP/Trademark and other areas, that require further study. In the alternative, the initial rollout should be limited to community-based and/or geographic gTLDs and should not include so-called “open” gTLDs until the overarching issues have been thoroughly reviewed and necessary protective structures put in place. *Hearst Communications, Inc.—Large Corporation.*

### Mechanisms against abuse

ICANN needs to ensure that adequate mechanisms are in place prior to launching any new gTLDs to protect against abusive new registrations. There are in fact substantial domainers who could put out \$185,000 very easily, contrary to some discussion at the Sydney trademark protection meeting. *Hearst Communications, Inc.—Large Corporation.*

### More information needed in many areas

More details are needed regarding criteria for inclusion in the IP Clearinghouse database; cost information; operational details for the Watch Service, IP Claims Service; and URS; and operational details for the GPML. *Hearst Communications, Inc.—Large Corporation.*

### Dispute proceedings and fees

The requirement that both parties in a dispute must advance “estimated” fees to the DRSP with a refund to the prevailing party needs to be clarified. In addition to the evaluation fee, ICANN should require an escrow for any registrant to make sure there are funds available to collect in the event of such a dispute. Only one fee should be required in the case of a rights holder’s objection to multiple applications for the same gTLD. *Hearst Communications, Inc.—Large Corporation.*

### Objection process—appeals and other procedures

IP rights holders should have legal recourse and the right to appeal adverse rulings on an objection. DRSP panel decisions should not be subject to further review but rather to an appeal process by a third party dispute resolution provider and/or a court. Dispute resolution examiners must meet certain standards of trademark/IP qualifications. Hearst agrees with the IRT that for transparency, panel decisions should be published, and searchable through an open access, centralized database. The application procedure should include due diligence for past domain name abuse by an applicant, and this should be a factor if raised in any objection. *Hearst Communications, Inc.—Large Corporation.*

## London

### Transcript Summary

#### Representatives at London session

The representatives from the IRT at the London session, appearing in their individual capacities as experts on the subject matter, were: Jonathan Cohen, Managing Partner, Shapiro Cohen of Canada; Ellen Shankman, Principal, Ellen B. Shankman Associates for Israel; David Taylor, Partner, Lovells in Paris; Jeff Neuman, VP Law and Policy for NeuStar; Stacey King, Senior Internet Lawyer IP for Richemont; Fabricio Vayra, Senior Counsel, Intellectual Property, Time Warner. *N. Wood.*

#### Sources of IRT recommendations

The IRT recommendations are based on best practices across the Internet in a number of different areas. *N. Wood.*

#### Background on the IRT mission

On the table for the IRT was not whether new TLDs should go forward, but that assuming that they do, what would experts in the area of trademark protection and other issues propose to address these concerns? There was recognition that as successful as it has been, the UDRP is no longer sufficient. Solutions were designed with the intent that they be balanced, and a checklist of criteria for assessing each proposed solution was developed. *E. Shankman.* The IRT was composed of volunteers trying to help the Board and community to find balanced solutions; the recommendations are proposals that do not necessarily have to be accepted. *J. Cohen.*

#### Proposed solutions

Most of the identified problems are known, and very few of the IRT recommendations are new or unprecedented. *D. Taylor.*

## Background on demand media

Demand Media's best known brand eNOM is the second largest ICANN-accredited registrar with 12 million names managed. We support introduction of new TLDs and believe they will create improved prices, services and choice for consumers. *R. Tindal.*

## Perspective on IRT proposals

For Demand Media the focus of the debate is on finding workable compromises on proposals for additional rights protection mechanisms that create maximum benefit with minimum harm. The IRT report sets forth good principles for achieving that goal. In our view four of the solutions proposed by IRT meet those principles and Demand Media supports them (the IP Clearinghouse, Thick Whois, IP Claims Service and Sunrise, and the expanded algorithm for string comparison). We do not believe the URS and the post delegation dispute resolution mechanism are fully compliant with those IRT principles, and the globally protected marks list (GPML) fails to meet those principles. *R. Tindal.*

## Perspective on new gTLD trademark protection debate

The debate needs to be more balanced. So far the debate seems to assume that there are all great trademark claimants and all bad registrants. There are in fact bad trademark holders who seek to abuse the system. *P. Keating.*

## IRT—clarification on pricing suggestions

All of the numbers proposed by the IRT were intended as orders of magnitude for what the IRT members thought might work. The actual crunching of the numbers of how much will it really cost providers to provide this kind of service, how much each side should pay and what they should pay, etc., were mere suggestions. If the debate goes more to what's a good idea and who should be paying rather than the dollar amount, this might help direct the discussion better. *E. Shankman.*

## IRT recommendations—support

Dot Berlin supports many of the things the IRT did—especially the URS, the post-delegation dispute resolution, thick Whois and the algorithm procedures. *D. Poshinovsky.*

## Apply the additional rights protection mechanisms to existing gTLDs

The additional rights protection mechanisms proposed by the IRT will only be effective if they are applied to existing TLDs and in particular .com, .net and .org, which more than 90% of today's cybersquatting cases come from. *D. Poshinovsky.* Most brand owners would agree with that. *J. Neuman.*

## GPML concerns

The creation of the GPML for only 100 worldwide trademarks is not a reasonable investment. It will also be the beginning of a trademark powerhouse with catastrophic consequences (e.g., if Sun Microsystems is on the list, then the well known British newspaper Sun has no chance to get its .sun TLD without asking Sun Microsystems for permission). *D. Poshinovsky.* The IRT did not come up with criteria for how many marks would actually be included in the GPML. The intent behind the GPML is not to create monopolies. The proposal was that anybody who met the criteria—Sun the newspaper, Sun the computer, any other sun like Sun Raisins—could get on the list. It would not preclude anyone of those, or a third party who does not own a right in sun as a trademark but who may have a legitimate right to obtain sun. The applicant for sun, even if initially blocked at the GPML level, wouldn't go to the trademark owner—the applicant would go to an independent party. In the example, Sun the newspaper could easily obtain sun because they would have a legitimate right. By contrast to the GPML, the existing sunrise system creates a situation where brand owners have to defensively register a domain and hold it for a long time, before anyone in the general public who may have legitimate reasons has a right to

register it, and the registry ends up with dead space. With GPML the brand owner does not have to defensively register and maintain a domain that it probably does not want. An applicant in the general public has the ability to make a showing to get a domain, and the registry ends up with a viable space as opposed to defensive dead space. *F. Vayra.*

### **Distinction between the IP Clearinghouse and the GPML**

Inclusion of a trademark in the IP Clearinghouse does not bestow any particular rights—it is just a simple database of authenticated marks, and the registry gets to choose what it does with the data in the IP Clearinghouse. The GPML does bestow rights, and I share the concerns voiced about that. *R. Tindal.*

### **IDNs—concerns about the IRT process impact and lack of inclusion**

The IRT process did not include enough expertise to create enough counter debate regarding how the IRT recommendations would affect when gTLDs and IDNs or ccTLDs and IDNs are rolled out. How is the staff going to account for this concern if IDNs were never factored comprehensively into the IRT recommendations? This is a major challenge. The ICANN Board and staff pursuant to the Board resolution that created the IRT should reinstate the function of the IRT but after incorporating comprehensive expertise in IDNs on its membership and panelists to make it congruent not only with ASCII gTLDs, but also making it congruent with IDNs gTLDs and ccTLDs. For example, what the IRT considers “slam dunk” may not be so from an IDN perspective. In many parts of the world, one computer in an Internet café may be servicing 50 users (so by the time the poor citizen gets back to his computer to read his email that he has been sent notice...). So the notice timeframe is an example—not necessarily purely whether 15 days is enough or 21 days is enough; it’s making it congruent with the functionalities, with the way these people live in the local community. *K. Fattal.* I agree with this point about IDNs, and I stated up front that the IRT did not have the ability or the time to consider all the impacts of IDN. We identified that as something that needs much further and deeper study. *E. Shankman.* The next steps following the IRT are to take the IRT report and the comments on it and consultations input and determine how and in what form these solutions can be implemented. If they need to be implemented in a way to appropriately consider different community IDNs or different communities across the world, then that is really important and input should be submitted on that. *K. Pritz.*

### **IDNs—ICANN communications plan**

Has ICANN planned anything similar to the trademark/IP road shows to educate the community on IDNs in the IDN regions? *K. Fattal.* There is a communications plan for IDNs that is partially executed and can be re-publicized. *K. Pritz.*

### **Background on WIPO**

WIPO is an intergovernmental organization with 184 member states; almost all the countries in the world are WIPO members. WIPO is mandated to promote a balanced and accessible intellectual property system. As part of that mandate WIPO has been addressing IP questions raised by the domain name system since 1998.

Some of this WIPO work led to the adoption of the UDRP. WIPO has also developed recommendations adopted by its member states that have been taken into account in developing criteria for the legal rights objection procedures proposed in the first and second versions of the ICANN Draft Applicant Guidebook for new gTLDs. WIPO is not a member of ICANN’s IRT. WIPO does serve as an ICANN-accredited UDRP dispute resolution provider through its Arbitration and Mediation Center. In the last ten years, it has administered more than 15,000 UDRP cases. WIPO has also been involved in developing registry-specific policies and provides the dispute resolution services to 58 ccTLDs. *Eun-Joo Min.*

## WIPO new gTLD recommendations overview

Expanding gTLDs represents a watershed moment in the DNS and adequate safeguards have to be in place to protect trademarks. In this spirit WIPO made four key recommendations regarding the new gTLDs process: (1) the trademark-based pre-delegation dispute resolution procedure for new gTLD registries--i.e., the legal rights objection procedure currently included in ICANN's draft applicant guidebook; (2) the trademark-based post delegation dispute resolution procedure for new gTLD registries and registrars, intended as a form of standardized assistance to ICANN's own compliance oversight responsibilities that would provide an alternative to court litigation (not a proposal to shift the burden of contract compliance from ICANN to trademark owners--it is intended to outsource that function to experts; (3) a discussion draft of a trademark-based expedited domain name suspension mechanism intended to address trademark abuse at the second or third level; and (4) substantive comments provided to ICANN's IRT team's draft and final reports. *Eun-Joo Min.*

### Focus of the problem addressed by IRT

The IRT was focusing mostly on people who are pulling up domain names and slapping a pay per click (PPC) page on it. This is not protecting consumers, but is protecting the trademark itself. ICANN is not the policeman for instances of consumers being defrauded. We are talking here about a civil remedy that allows you to close down things. I disagree with the principle that trademark laws are there to protect the consumer. In most European countries it's viewed legally as protecting the investment and goodwill that the company has engaged in order to promote its brand. Consumer confusion is really a matter of jurisprudence for common law jurisdictions such as the U.S. and the U.K. **Male unidentified.** It is important to emphasize that IP laws including trademark are not just about protecting IP owners but everyone. E.g., trademark law is about not only protecting brand owners but also the general public. *Eun-Joo Min.*

### Trademark holder responsibility for costs and trademark policing

Every dollar that ICANN receives comes from a registrant. The community outside of trademark interests should not have to bear the costs of the activities of a very few people. The laws in every country require trademark holders to police their own marks. Costs imposed on registries will be pushed down to registrars, who will push them to registrants. These costs are solely to protect commercial entities who are benefiting from their own trademark. Trademark owners should not seek to have others act as a police officer for their protection. *P. Keating.* Brand owners are also registrants and have thousands of domains of which we use less than one hundred—all the rest are for protection. We spend a fortune to protect our brand. Consumers are bearing the costs when brand owners are having to pay for all the enforcement—it trickles down. **Female unidentified.** It is important to emphasize that trademark law is a consumer protection law. The ultimate benefactor of trademark policing is the user. The collateral to not protecting brands and helping brand owners to do that is that consumers get hurt. *F. Vayra.*

### Infringements—more in quantity and sophistication; rapid takedown and balancing interests

The trend in the marketplace, contrary to what some of the ICANN published materials say, is a steep rise in the number of infringements that are more elaborate and tedious to track down, forcing brand owners to focus on fewer and fewer. There should be a survey of brand owners to get input on what is actually happening, not what is registered as complaints. With the first complaint the offending websites should disappear, since the gross amount of money is made in the first fortnight and after that squatters don't care if they are terminated – they just leave and don't bother to cover any tracks. The IRT has only begun its work, only scratched the surface and there is no reason why it should think it's concluded. *S. Panpi.* I agree that the numbers of registrations versus UDRPs can be very misleading. There should be a fast process for taking down squatters. Input is needed on how to balance that against claims of

registrants and domainers that brand owners are too aggressive and that the system will be used to either reverse hijack or game. *F. Vayra*.

### **Concern that IRT recommendations implementation will delay all new gTLDs**

CORE fully supports the IRT recommendations but is concerned about the timeline. What can be done to prevent delay of projects that will not have the problems at issue in the IRT process? One option is to allow a process to go forward based on self-selected applicants who would have to stay back if there is an objection. *W. Staub*.

### **Cultural and linguistic TLDs**

There is an opportunity to develop best practices with the kinds of groups (e.g., some cultural and linguistic TLDs) that have a very low incident rate (e.g., four UDRPs in 36,000 domains); if these groups can communicate regularly with ICANN and others they could help develop a very positive approach to how new gTLDs will be implemented. *A. Jones*.

### **Centralizing data**

If data is centralized with a neutral provider, the system would be more efficient – i.e., the IP clearinghouse, the GPML and IP claims all housed in one public database. Why would the IP clearinghouse be considered confidential data? *W. Staub*.

### **Other noncommercial user constituency concerns about the IRT recommendations**

The GPML changes the face of trademark law, and there is no consensus as to which marks are worthy of global protection and even WIPO has refrained from providing such a list. The URS is a dangerous provision; instead the UDRP should be amended. We have strong objections to Thick Whois and the post delegation dispute resolution mechanism. Finally, the IRT recommendations would expand the rights of trademark owners. There are some good suggestions but the implementation falls short; we need to find a balance. *K. Komaitis*.

### **IRT recommendations—support**

MARQUES and Nestle support the IRT proposals. It is right to have new legal means and new rules linked to the expansion of TLDs. The URS proposal of the IRT to freeze the domain is good—i.e., some brand owners don't want to have the domain in their portfolio, but if some do then there is the UDRP. The URS will be lower cost for brand owners. Trademark lawyers do not abuse the system-- the point is for brand owners to protect their rights, not to "clean out the Internet." *C. Perrion*. The IRT proposals, especially the URS freeze, are sensible. The cost of the clearinghouse is going to have to be low so that for brand owners it doesn't become regarded as another type of de facto registration. *A. Mills*. The Danish law association supports the IRT report but does not think it goes far enough to protect trademark interests. *K. Christiansen*. MarkMonitor is an advocate of the IRT proposals which if well implemented could provide quick and cost-effective remedies for rights owners. *C. Jamieson*.

### **Implementation of IRT recommendations**

ICANN should announce a detailed schedule for the implementation of critical rights protection mechanisms (RPMs), especially the URS. ICANN should specify that the RPMs use automation and Web 2.0 technologies and process efficiencies, so that new gTLDs live up to their safety and security promise and are implemented in a cost effective way. Real costs to rights holders must be carefully considered. Smaller rights owners are most harmed by the current system because they lack the resources to defend their rights. *C. Jamieson*.

## More work needs to be done on IRT recommendations; impact on new gTLD timeline

We still do not have the criteria for the GPML, let alone whether there is a good cost and effect ratio. We do not know enough about avoiding abuser complaints. Many in the community still do not know what the criteria is for applications because the Applicant Guidebook is not in a final version and prospective applicants cannot properly budget and get their projects underway. ICANN should prioritize areas –look at the set of recommendations that are on the table at the moment and maybe leave those for a later stage that can't be completely answered and properly considered so that the application window for next year is not jeopardized. *T. Rickert*. If we put some things off because they're too hard to work on now there would have to be another draft version of the guidebook after that, and we would not want that. Our preference is let's debate all of these carefully and work out which ones work, and get them in a September and final version of the Applicant Guidebook. *R. Tindal*. It is important to note that more work is needed and that the IRT report does not really represent a "finished" tapestry. *M. McFadden*.

## IRT mandate

The IRT mandate was pretty much that we assume that new gTLDs are going forward—and what would we do not only for brand owners but also for the community at large to make them implementable and fair. It was not a choice of the IRT to serve as a buffer. *J. Cohen*. It was important for brand owners to come to the table in the IRT even with the mandate we were given and try to work with it. *S. King*.

## Burden on trademark owners

Most of the finance and resources needed to make the IRT recommendations work will be pushed back onto brand owners. There is nothing here that puts any kind of responsibility on to domainers to check that they're not infringing somebody's rights. *C. Walters*. It's a cost of business for domainers, especially those who create automated software, to build into their software something that either ensures they are not infringing or to employ people to review names before or just after they are registered so they are not misused. Unfortunately that is not a mandate that ICANN could propose. **Male unidentified**. The IP clearinghouse moves toward this kind of solution. *R. Tindal*. There has to be a balancing of interests regarding cost burdens. **Female unidentified**. WIPO believes that the cost burdens for the IP Clearinghouse should be shared by all interested parties and not be imposed solely on trademark owners. *Eun-Joo Min*. If registries and registrars are being forced to take certain actions, they should not be required to pay for them. A balance needs to be struck and the IRT found that balance. **Male unidentified**.

## Important but unaddressed issues

There were some issues that the IRT thought were important but did not address because of time – e.g., proxy services and IDNs. **Female not identified**.

## Feedback Form Summary

### Support with comments

See comments on IP Clearinghouse, i.e., cost, and also our detailed submissions on the IRT on ICANN's website. *S. Payne, BBC Worldwide—Large Corporation*. If they speed up the process and keep the NCUC away, yes please go ahead! *Domain marketing*. IRT recommendations seem very balanced. *Small Business*. Please refer to our public comments. *C. Jamieson, MarkMonitor*.

The CAC provided its written comments online. *Z. Loebel, Czech Arbitration Court—Noncommercial organization*. Addressing and propositions solving this issue are mandatory to the development of the Internet and its extension through the new gTLDs. *Nestle Group—Large Corporation*. The implementation of the IRT proposals is vital for the effective and valuable implementation of new gTLDs



so as to not stifle innovation and competition but also protect consumers and rights owners. *A. Mills, Experian Ltd.—Large Corporation.*

Caveat that my preferred approach would be an updating of the UDRP (I understand the issues with this) to deal with undefended complaints on a cheaper expedited basis and also introduce an appeal stage; the GPML has issues; overall the IRT has done a valuable and important piece of work. *Nick W-S, Nominet—Registry.*

Support, but dependent on associated costs to brand owners. *Large Corporation.* Support, but could go further—would like some mechanisms to discourage domainers from registering other people’s brands in first place. It is wrong that legitimate owners are facing additional costs despite huge amounts paid by domainers. *Large Corporation.*

(1) Many countries/trademark registries run a list of famous trademarks (e.g., Portugal) so why not run a GPML? Facebook has just run a similar pre-open date list. (2) Why not run a pre-delegation dispute opposition period for domain names—similar to a trademark application; (3) Will there be any jurisprudence for the trade mark protection provisions in the Applicant Guidebook. I need to advise on the meaning of these provisions; currently they are meaningless. (4) As a representative of a brand which is also a dictionary word, I would like to know which is the stronger right—a global trademark portfolio or a legitimate interest in a dictionary meaning of the relevant term (e.g., apple). *R. Pringle, Shell International Ltd.—Large Corporation.* Support but they need to create real deterrents to infringement—e.g., “slam dunk” infringers should incur considerable penalties. *Interest not specified.*

### **Implementation timeline**

The overall concern that remains is the implementation timeline. We need to make sure that TLD projects that do not require the IRT recommendations are not held up waiting for the finishing touches of the RPMs that are not necessary for them. *W. Staub, CORE-- Registry-Registrar-Professional association.*

Any decision against implementation would have serious consequences for all involved parties and ICANN as an organization. *Large Corporation.*

### **Apply to existing gTLDs**

While being broadly in support there are some issues which to be addressed as well. In particular, any new mechanism has to be applied to the existing gTLDs to have a real effect. *Registry.*

### **Trademark owner concerns**

Generally the mechanisms are too restricted and do not provide sufficient protection to trade mark owners. Seems as if ICANN doesn’t really believe that trade mark owners are under constant attack on the Internet. Trademark owners shouldn’t bear all the costs of the enforcement. Costs must be low. *Large Corporation.*

### **Board presence/consultations**

Why was no one from the ICANN Board present in London? Aren’t they supposed to hear the actual comments during the consultations? *Large Corporation.*

### **More work is needed**

Agree broadly but think much more work to be done the nuts and bolts. It’s such an important area and one that will potentially be used as a basis for whole gTLD system for many years. We need to get this right. Needs at least one more draft. *Large Corporation.* Further review is necessary before final approval or rejection can be done. Question whether the recommendations should be applied

universally to every new gTLD, and whether applicable to gTLDs serving communities which are not in a commercial realm or for local communities of different legal backgrounds. *R. McGary—Registry*. But strongly think the recommendations need more time and work spent on them. *Interest not specified*. IRT report and suggestions are greatly appreciated although it is cause for great concern that ICANN is rushing all time limits, not allowing proper discussions on e.g., the IDN issue in relation to protecting trademarks when introducing new gTLDs. *C. B. Christiansen, Danish Lawyers Association—Professional association*. We are broadly supportive but believe the IRT recommendations are a baseline—a floor not a ceiling and believe that costs on brand owners need to be minimized. *Large Corporation*.

### More work; process concerns

Nice work though only a start; should continue much further. One grave concern—the work within the IRT has been almost opaque, but what could be seen lead to the conclusion that part of the report has been omitted by ICANN (?). Why was Richard Tindal given such extended speaking time? That was a very odd and partial set of views aired—very unprofessional way of (mis) using our time. Besides, he was not able to substantiate anything. Why pursue methods proven noneffective and just apply patch-on-patch? Instead of “bad faith” use “good faith” that would force registrars to gather proof from the very beginning to be able to prove “good faith” instead of complaints trying to prove “bad faith.” Registrars should deposit a refundable fee per domain... **[comments missing—continued on other side of doc. which is not included in set of scanned docs.]** *LEGO—Large Corporation*.

### Opposition

The solutions that were proposed are mostly too “vanilla” based to actually work. The recommendations were hastily written and can work mostly in “Anglo Saxon” countries. ICANN may be acting outside its mandate. *O. Crepin-Leblond, Internet User*. Not finished; one-sided; needs more consultation; panel needs more experts and diversity. *A. Bennett—Reseller*. Report seems to omit protection for registrants/registrars. *A. Barnett—Registrar*. Concerns are increase in trademark holder rights; some proposals are likely to stifle new and innovative gTLD proposals; and the IP Clearinghouse works against fair use. *R. Wickham, 2020 Media—Registrar*.

### Make ICANN and issues more accessible to everyday users

This was clearly a valuable consultation—relatively well attended. Although perhaps it would have had even better response were it more publicized. One comment from the floor which was well-taken was a general lack of awareness of the significance of these issues by those who are the most affected. If brand owners themselves are relatively ill-informed then the problem is likely exponentially magnified among ordinary users of the Internet. ICANN must make itself and these issues more accessible, more mainstream, more connected to the world of everyday users so that the consultations on today’s and other subjects are not dominated by the “usual suspects” time and again, however valid and thoughtful their concerns and comments are. *Law Firm*.

## Unregistered Trademarks

### Sydney Feedback

#### Unregistered trademarks protection

The IRT presentation has lacked information about protection of unregistered trademarks, and this area needs to be addressed. It should be easy to find out whether or not a dot com was registered before some legal shark decides to spend money getting the trademark. *P. Foody*.

## IP Claims Service

### Sydney Feedback

#### Overview

The IP Claims Service notifies both potential applicants and trademark owners who have put their data in the IP Clearinghouse that, on the one hand, there is a mark in the IP Clearinghouse that identically matches what you are applying for, and, on the other hand, where the owners of the marks are concerned that something has been applied for that matches a mark, if the applicant chooses after notification to proceed with his or her registration, he or she will be asked to make some representations and warranties regarding legitimate use of the mark, accuracy of information provided, and so forth. *M. Wong*. The IP Claims Service is one pre-launch mechanism and is not a real-time service; it is not for every registration ever registered in a TLD, but is merely during the startup process and is an alternative to sunrise. *J.S. Evans*.

#### Impact of IP claims service—basic words already registered as marks

With the notifications involved in the process, aren't we going to be turning a lot of people away and chilling their use of domain names—they will not register because they feel they are walking into a problem? *K. Kleiman*. If you choose to do an IP Claims Service, you will get notified; you are free to proceed with the registration. It asks you to make a representation that to your knowledge you are not infringing the rights of another, the same thing that you would normally have in your domain name registration agreement. *J. Neuman*.

#### Support for IP claims service

The IP Claims Service and its sister RPM the sunrise are strong RPMs. It happens during the launch phase and it is important to understand that it is not something that would happen in perpetuity in the registry but just during the first month or two months. *R. Tindal*.

### New York

#### Transcript Summary

##### IP claims service

IP Claims Service is a prelaunch mechanism at the second level, intended to be the minimum rights protection mechanism adopted at the second level and is intended for any mark. In this service the registry provides notices to potential registrants for domain names that are identical matches to marks contained in the IP Clearinghouse that there may be claims and that the prospective registrant should therefore proceed at its own caution. If the prospective registrant decides to go forward, there are representations and warranties made by that prospective registrant. The IP Claims Service also notifies the trademark owner that someone has gone through with the registration. *J. Neuman*.

### London

#### Transcript Summary

##### IP claims service and sunrise

Both of these mechanisms have been tested and proven to work and there is solid consensus on them. The IRT proposal would improve the sunrise concept by enabling a registry to choose from the IP Clearinghouse database which marks it thinks are applicable to the sunrise. Previous sunrises were more generic in their application. *R. Tindal*.

## Pre-launch IP claims service

This service is for those who do not adopt sunrise processes and is modeled after a process introduced by .biz in 2001. It applies to all registered marks that do not necessarily qualify for the GPML and it provides notices at pre-launch to potential registrants for domain names in a new TLD if the TLD corresponds to a mark that has an intellectual property claim that's an identical match. The applicant can then decide if it believes it has a legitimate interest and whether to proceed with the application. It does not prevent an application but puts the applicant on notice of the mark that is out there. The notice to the applicant will state that if the applicant proceeds to registration then the applicant may be subject to one of the challenges envisioned by the IRT, such as the URS, and will ask the applicant to make representations and warranties that they will not use the domain name in an infringing manner toward those marks on the IP Claims list. If the applicant proceeds to a registration then the trademark owner will be notified. *J. Neuman.*

## IP Clearinghouse

### Sydney Feedback

#### Overview

The IP Clearinghouse will include and support data that relates not just to the GPML but also other forms of marks that do not qualify for the GPML. In effect, it will be, if it works, a large-scale repository of data relating to all kinds of rights that support new gTLD registries. Among its key features, data submitted by trademark owners has to be validated annually. The burden will largely be on trademark owners to provide and update accurate information. Trademark owners are the owners of the data they provide, and data will be used only for the sole and specific uses for which the IP Clearinghouse is set up. It is recommended that a licensing and sublicensing process be set up. The IP Clearinghouse will be run by a separate, outsourced entity selected through an open, competitive tender process (not any entity in an existing contractual relationship with ICANN) to which equal access will be required. Scalability should be included and costs should not be prohibitive, and there should be incentives for trademark owners to want to use the IP Clearinghouse. *M. Wong.*

#### Safeguards and oversight

WIPO believes that given the central role envisioned for the IP Clearinghouse, there should be very close oversight by ICANN, adequate safeguards in place, and, if a monopoly is granted, the roles should also be limited. One option is to grant roles to different entities—e.g., data collection and storage to one entity, and data validation to a different entity, and IP claims to a third entity. *E. Min.*

#### Financial considerations

It is unclear who will pay for the IP Clearinghouse. Fees should not be imposed entirely on trademark owners, but should be shared by all relevant actors in the DNS. *E. Min.* There is a tension between making the IP Clearinghouse robust—at least as fast and reliable as the registry infrastructure which already exists (which sounds expensive)—and making it cheap for mark holders. *J. Buchanan.* The IRT did not want to dictate funding models, and in a competitive process for selecting the entity to run the clearinghouse it is assumed that bidders would suggest some funding models. Funding models could also be proposed in the comments process. The IRT did envision that the costs would be shared. Other ideas were discussed, such as ICANN funding some of this, but there was no consensus position put into the IRT report. *J. Neuman.*

#### Rights included

I really do not see how there is any excuse for also putting designations of origin and quality into that category with registered trademarks. This is not about what is the international value of the different

types of things of national origin according to international law. It's the fact that they do exist and in different national regimes, and they should have at this level of preventing abusive registration the same level of protection. Because they have less mechanism frameworks and because we are only thinking about trademarks, by legal definition it doesn't have this tool. *A. Abril i Abril*. Regarding the point made by A. Abril i Abril, this may be a miscommunication in the report. The IRT did not mean to say that the clearinghouse had to collect all these elements, but had the concept of a tool in mind (i.e., if a registry wants to give some sort of preference to those marks based on designation of origin, that the clearinghouse could be a repository for that information). The IRT was not suggesting that the element be used in every single TLD launched, but to help future registries to have one source to go to if they choose to give a preference for that type of mark. *J. Neuman*. With regard to unregistered marks in the clearinghouse, the intent was to allow the database to get as much information as the registry needs for implementing its RPM. So if the registry wants to recognize unregistered marks, not that it has to, it could use the clearinghouse. *J. Neuman*.

### **Trademark registrations on an intent to use basis**

Many marks are registered on an intent to use basis. If they are registered trademarks and they fulfill the criterion, then that ought to qualify them for inclusion as trademarks if they satisfy the national registration criterion and they are marks of national effect and so on. That may or may not be the case in other countries. If you do not have a right to register based on an intent to use in your country, that does not make you a trademark rights holder in the eyes of the IP Clearinghouse. *M. Wong*.

### **IP Clearinghouse: concern about expansion of existing trademark law**

Are we giving a lot more rights and opportunities to people beyond existing law (expanding existing national trademark enforcement into international rights that trademark holders don't currently have)? This seems to be open to a lot of abuse, not only for existing trademark holders but for cybersquatters. *David. B.* The mechanisms were designed to minimize gaming problems. The clearinghouse's validation function with whichever national trademark registry you got your trademark registration from is one way to minimize that problem. *M. Wong*. With the clearinghouse, it is just an efficiency mechanism—it is not creating anything that has not been done before and it is a model that has been successful. All we are saying is let's aggregate it into one central location. *J.S. Evans*.

### **Support for IP Clearinghouse**

eNOM supports the IP Clearinghouse; it is a practical, efficiency measure and will save trademark holders money by stopping them from having to go to individual registries repeatedly. It is not setting policy in any respect—it is a database, and registries get to choose how they apply the data in that database. Protections can be put in place against misuse. *R. Tindal*.

### **IP Clearinghouse is problematic**

It is a one size fits all approach that ICANN is strongly encouraging that will not be appropriate for many TLDs (e.g., for an IDN TLD it may not be appropriate to be talking about global names). *David K.*

### **IP Clearinghouse—languages**

How many languages will the clearinghouse need to be in and what costs are involved? How will the operator of it accommodate dealing with a global Internet, especially working with IDN gTLDs in many different languages? People in the developing world would be concerned about costs being passed on to people running the IDN gTLDs and if that would amount to a regressive tax on non-English or non-Roman languages and be a damper on the entire purpose of IDN gTLDs to make the Internet as linguistically diverse as quickly as possible. *R. McKinnon*. These are all good points that need to be addressed. The intention was for the clearinghouse to be able to collect information in multiple

languages and to be able to be used for IDN registries. The intent was not to pass on the cost to the registry; we do not want to hamper competition in the registry space. *J. Neuman*.

### Existing watch services

Is the IP Clearinghouse recreating the wheel – i.e., aren't existing watch services and other information in various languages all over the world doing the job of notifying large trademark owners that their mark is being registered as domain names and informing them where to go to find those domain names? *K. Kleiman*. To my knowledge there is not an existing watch service that actually validates and verifies that you have the right you're claiming to have before getting the results. It was not intended that the IP Clearinghouse would replace existing watch services. *J. Neuman*.

## New York

### Transcript Summary

#### IP Clearinghouse

The IP Clearinghouse was proposed as a way to have a cost-effective and efficient database with two main functions—to be the centralized entity that all new gTLD registries and possibly the registrars would interact with in relation to implementation of the Globally Protected Marks List (GPML), the IP Claims Service, and the URS. Trademark owners would submit data to the clearinghouse (run by an outsourced entity not currently in a direct ICANN contractual relationship) either directly or potentially through the registry or registrar for a fee. The IP Clearinghouse would validate the data. Access to and use of the data would be restricted to the purposes for which it was submitted, and trademark owners would grant a non-exclusive license to the data to ICANN which would sublicense it to the IP Clearinghouse. Equal access to all ICANN registries and registrars would be required. The IP Clearinghouse would need to be robust (scalable and able to accommodate records of different types of rights), secure, flexible and fast, and operate at reasonable cost to trademark owners. *K. Rosette*.

#### IP Clearinghouse

The IP Clearinghouse makes ICANN a global IP rights protection manager, far beyond its mission as a technical manager of the DNS; there is a risk of many unintended consequences of the IP Clearinghouse. The market can provide this service and should be allowed to operate. *C. Climen*.

#### IP Clearinghouse-support

The clearinghouse will allow smaller registries to implement policies that are tailored to the area they are working in. *A. Van Covering*.

#### IP Clearinghouse—allow public access

The clearinghouse should be designed to allow public access to it. The restriction that only registries and registrars of ICANN can have access should be dropped, and ICANN should conduct outreach to make the public aware of access to the database. There could be a trade off where there is public access but some limitations on what could be done with the data and that sanctions would apply for violations. *T. Barrett*.

#### IP Clearinghouse provider

ICANN should drop the restriction that a currently contracted ICANN entity cannot be the IP Clearinghouse provider in order to solicit the most innovative range of solutions. If it turns out that an innovative solution comes from a well known registrar or registry, that issue can be addressed in the contract. *T. Barrett*.

## Feedback Form Summary

### Support with comments

Long overdue! Well-done! *Small Business*. Support, as modified by our filings on the record. *P. Flaherty & M. McKeehan, Verizon—Large Corporation*. A fine idea that will solve many here-to-fore intractable problems. *Registry*. Perfect and needed! *J. LeMan, Lord, Abbett & Co.—Small Business*. Support, but need to protect broad commercial base. Not just large corporations. *Professional association*.

### More details needed

More detail is needed about how the IPC will, or must, be used for new gTLD applications. Also, there should be an opportunity for additional public comment on the specifics of IPC implementation. *T. Blasey, ITT—Large Corporation*. More detail is needed regarding criteria for inclusion in the IP Clearinghouse database; cost information; operational details for the Watch Service, IP Claims Service. *Hearst Communications, Inc.—Large Corporation*.

The IP Clearinghouse is a good start, but the following points are noted: (1) It is highly questionable whether the launch and scaling up of the proposed IP Clearinghouse, and the collection and validation of the very substantial amount of data required can be completed within a timeframe compatible with the proposed launch of an initial round of new gTLDs for first quarter 2010. (2) The proposed “reasonable” fee structure should not burden owners of substantial numbers of trademark registrations. (3) The discussion of “annual” validation of data must take into account that the terms of trademark registrations may last for varying periods up to ten years or more. *Hearst Communications, Inc.—Large Corporation*.

### Use by UDRP Panelists

Important that it also frequently be updated and searchable by UDRP panelists. *D. Bernstein, Debevoise & Plimpton LLP—UDRP Panelist*.

## London

### Transcript Summary

#### IP Clearinghouse

Even absent ICANN creating it, Demand Media believes that the marketplace would create one or more such clearinghouses. Demand Media would support a solution with either one or multiple (regional) clearinghouses. *R. Tindal*.

#### IP Clearinghouse

WIPO feels that the ubiquitous role envisaged for the clearinghouse requires adequate safeguards and close ICANN oversight. In particular circumstances, differentiation of roles may be appropriate rather than granting the different roles to one entity. Trademark owners should not shoulder the whole burden of financing the clearinghouse but the burden should be shared among all interested parties, including registries and registrars who will benefit from any clearinghouse put in place. *Eun-Joo Min*.

#### The IP Clearinghouse

(Which has a precursor in .eu and .asia) is a database with two principal functions—a central entity with which all new gTLDs registries and possible registrars will interact in relation to the GPML, the Pre-launch Claims Service and the URS. The information is collected for validation and it has been suggested that it include registered and unregistered rights. Data is submitted by trademark owners either directly or through the registry for a fee which should be reasonable. The data needs to be validated initially and then annually. Data is owned by the trademark owners so they need to grant a license through. The

clearinghouse is to be an outsourced entity not in direct contractual relationship with ICANN and which is available 24/7 and scalable. It must operate with fast and secure delivery of accurate information in a standard format using a secure, robust, state of the art technological platform. Trademark owners should be able to put their entire trademark portfolio into it and the cost to them should be reasonable. *D. Taylor.*

### IP Clearinghouse—objection

The Noncommercial Users Constituency believes that the clearinghouse is beyond ICANN's mission and would give ICANN privileges enjoyed by national trademark offices. In future years this database could be abused and used against domain name registrants. The idea is valuable but its presentation so far is quite problematic. Having one massive database will raise issues of consistency and uniformity. There is no indication in the IRT report how ICANN is going to ensure that all trademark owners are listed, or how it will deal with trademark registrations in other countries that are not valid. These issues need to be addressed. The market should address the demand for this clearinghouse. *K. Komaitis.* The IRT focused on one provider as a way to make sure there was uniformity. Multiple clearinghouses that adhered to a standard protocol could alleviate concerns about uniformity. *F. Vayra* responding to *K. Komaitis.* Having to develop a standard to have multiple clearinghouses would delay the new gTLD program until the standard could get approved. If the program starts out with one clearinghouse, it could be figured out for future rounds if it is the desire of the community to have a competitive marketplace for clearinghouses. **Male unidentified.** It is nowhere mentioned in the IRT report that having one clearinghouse is an initial plan. *K. Komaitis.*

## Feedback Form Summary

### General Comments/Questions

#### Opposition

Must take into consideration local IP and trademark laws. Will prevent registration of 'legitimate' misspellings. *A. Barrow, Any-Web Ltd.--Registrar/ Domain Marketing.* If the IP Clearinghouse is one on which one can base enforcement of marks rights, it is not designed in a structured way that will avoid excuses and unfair practices. If the IP Clearinghouse is a list bearing no relation to enforcements (and is thus just "for informative purposes"), it is a waste of ICANN resources. This list might be undertaken by the market, but it is not up to ICANN to open yet another can of worms. *O. Crepin-Leblond—Internet User.*

This could exist in the marketplace so see no need for ICANN to run an additional database. *Registrar.* Data should come from national trademark registries, not trademarks themselves. The private nature of the list is a grave concern. Class of use is critical in trademark registration and use of a domain is critical from the UDRP point of view. The IP Clearinghouse idea does not answer these 'use/class' issues - an appeal is no use to the average registrant using a cheap registrar, who has no intent to infringe the trademark class. *R. Wickham, 2020 Media—Registrar.*

An expensive and costly powerhouse for only 100 famous trademarks? This does not work. *K. Krischenowski, .berlin TLD--Registry.*

#### Support with comments

Broadly in support of an effective mechanism which has to be implementable, preferably making use of existing list and directories. *Registry.* Full support offered for this. *Large Corporation.* Assuming that this information is advisory and not prohibitive whilst ensuring low/no barrier to entry for brand holders. *J. Robinson--Small Business/Registrar/Hoster.* Please think carefully about harsh penalties for trademark owners submitting data with minor errors, since it involves significant documentation; annual



verification is too frequent/onerous. Reasonable cost to ensure IP clearinghouse isn't expensive way of recording a right that owner has already paid to protect. *Large Corporation*.

Published databases of trademarks should be used instead of asking trademark owners to again register their trademarks with the IP Clearinghouse. *Interest not specified*. Please refer to our comments previously made. *C. Jamieson, MarkMonitor*. Needs to be more stringent. *Interest not specified*. Trademark search providers should be consulted. *S. Stolfi, CT Corsearch USA--Trademark Research Company*. Helps to avoid clashes. We are domainers but we own trademarks too. *Domain marketing*.

The process proposed seems to reject trademark application examination undertaken by national offices in many countries. Such examination is subjective and the applicant for a trademark has an opportunity to present arguments. Would this be the purpose of extended evaluation? Is ICANN concerned about setting precedents? As a member of your panel has commented today the issue of 'confusion' is not clear cut. On whom would the task of this analysis be placed? *J. Goodchild, W.P. Thompson & Co.--Law Firm*.

To what depth would trademark holder details be exposed via this database? If it is extensive and fully transparent, such a database would become a source of competitive intelligence, which in turn may discourage trademark holders publishing/submitting such details of all their rights. *D. Green—Large Corporation*. Must be undertaken by trademark professionals. *R. Bond, EMI Group—Large Corporation*.

1. Cost of recording details of trademarks needs to be low and with a reducing cost for filing multiple mark details. Remember cost of getting an EU-wide trademark in 27 countries is less than 1000 Euros, so more recordal of legal rights needs to be low so it does not become a quasi-legal necessity for brand owners.
2. The details recorded on the clearinghouse database would become a valuable trademark searching tool and commercially licensing this could offset the recording costs to TM owner. However, license from owners needs to be made and include this type of usage. *A. Mills, Experian Ltd.—Large Corporation*.

(1)The correct name is probably "Marks Clearinghouse" because it is not concerned with copyrights or patents; (2) Use the DNS for look-up of data, similar to .tel model; (3) This could be done with a ".trademark" functional TLD, or, slightly less user-friendly, with ".trademark.arpa" (similar to ".in-addr.arpa" or "e164.arpa."); (4) decentralized operation will probably lead to faster implementation. *W. Staub, CORE--Registry-Registrar-Professional association*.

### Cost/reasonable fees

Important that the fee is reasonable--why a fee at all? Can't ICANN sponsor this with the \$185,000 USD per Domain? *Large Corporation*. Dependent on associated costs to brand owners. *Large Corporation*. A good idea - but cost? *Nick W-S, Nominet--Registry*. But real concerns about cost. The cost to the brand owners probably will be substantial, not just the actual filing cost but the man-hours in pulling the information together and of course the enormous existing cost of maintaining a global trade mark portfolio. This cost should not rest on the brand owners alone. The IRT is a proposal to protect registries and registrars from facilitating widespread infringement of IP rights and they should contribute to the costs. *S. Payne, BBC Worldwide--Large Corporation*.

### IP claims service

Not sufficient if only "identical", must be broader to cover typos, mark and generic names etc. Not sufficient warning if only "identical". No notice to Chanelshop. If Chanel is the mark, doesn't make sense. It's not sufficient if this is just pre-launch. *Large Corporation*.

## More work needed

As outlined, generally a good idea, but still a lot of work/discussion to be done before it can reach a workable model. Though very odd why algorithm/model for string comparison is not put to public discussion/scrutiny? “Open source” comes to mind. I would personally be glad to contribute. *LEGO--Large Corporation.*

## IP Clearinghouse Provider

There should be one provider only. *EURODNS--Registry.*

## Globally Protected Marks List (GPML)

### Sydney Feedback

#### Overview

The criteria for the GPML are numerical and purely objective; eligibility requirements are to be set very high and very strict. With regard to the November 1, 2008, date, the IRT report contemplates that as registrations go on and as new application rounds are launched, that certain criteria requirements as well as these dates may well have to be revised. The GPLM operates at two levels: if anyone’s mark makes it past the strict criterion on the GPML, they will have for that mark a top level protection and a second level protection. With respect to the lack of numbers in the report, data that ICANN staff is compiling to assist in relation to the strict thresholds for the GPML have not yet been received. *M. Wong.*

#### Top-level protection

For the top level, what is analyzed when a new gTLD is applied for is either an identical match with the actual mark on the GPML, or confusing similarity. If after this evaluation the applied-for gTLD is an identical match or is found to be confusingly similar to the actual mark on the GPML, there is a reconsideration process. It is in the IRT report that all applicants who fail the initial evaluation should have a chance at reconsideration. *M. Wong.* At the top level, the entities that own marks on the GPML will merely be given the same opportunity that ICANN in DAG 1 and DAG 2 is reserving for itself and its contracted parties, the registries. In the current initial evaluation, string confusion will be done against existing TLDs and reserved names, so we are simply adding on to that. If folks have an objection to that idea, it should be across the board. *K. Rosette.* At the top level it seems like you have a really big hammer for a nonproblem; this is not \$6 cybersquatting—people have to front up \$185,000. *A. Schubert.* The IRT report says that the problem and issues are at the second level and not at the top level, because there are not that many cybersquatters with \$185,000 to go out and lose that money. *D. Taylor.* Once you have proven you have rights, unless you pony up the \$185,000 and make the initial investment to run your own TLD, it just goes back in the pool and becomes whack-a-mole, even on the top level. *J.S. Evans.*

#### Second level protection

For the second level, the main difference is that the match between the actual mark on the GPML and what is being applied for at the second level is limited only to an identical match. At that point a dispute resolution process can be initiated that includes an appeal, and if the applicant can show that he or she has legitimate rights or interests in the domain name, and that can include, e.g., generic uses or permissible product descriptions, that will go through the registration process. *M. Wong.*

#### Effect of being on GPML list

If you are on the GPML you are not automatically entitled to the respective domain name (response to A. Schubert inquiry). The GPML does not entitle the mark owner to priority or any other benefit under

sunrise. *M. Wong*. While the GPML would not grant people additional legal rights it would grant them administrative rights which will empower them and have a chilling effect on others. *A. Schubert*.

### Negotiations with trademark owner

Why cannot an applicant, like we do with geographic designations, go to the trademark owner and negotiate a letter of no rejection? It's a bit of overkill and the protection should at least allow for negotiations between parties and not automatic killing of the application. *A. Abril i Abril*.

### GPML should be dropped--costs outweigh benefits

eNOM opposes the GPML. It will be complex, controversial and politicized to actually come up with what the list is. The criteria for the list is subjective. We do not know how we are going to decide that threshold number, and who decides certain other matters. There will be political globalization in that there will be folks from less-developed countries with strong marks there who want to be on the list but don't meet the criteria. We will therefore see lobbying from some countries to lower the threshold for less developed countries versus western countries. It is not worth all this trouble because the GPML list does not add much value. At the top level the list adds no additional value to what the DAG legal objection process already provides. The list only adds a kind of marginal benefit at the second level. Being on the list does not give you a preference in sunrise. *R. Tindal*. The noncommercial users constituency strongly opposes the GPML; it is a massive extension of existing legal rights. *K. Kleiman*. GPML takes rights away from the rest of us. The costs outweigh the benefits that the very small group of big companies will get with the GPML, especially considering the introduction of the many other new RPLMs proposed. *P. Stahura*.

### Alternative: UDRP threshold issue-de facto GPML

A simpler alternative to adopting a new scheme to address the harm which is cybersquatting should be considered. There have been some 30,000 UDRP cases heard; this amounts to a sort of de facto GPML, because there would be none of the prospective entrants in the GPML that have not already been the subject of a finding in a UDRP case that they have trademark rights. The UDRP is a vastly superior alternative to litigation. Why can't the starting point be that before you can register any new TLD (and not just in a sunrise period), you must check whether the underlying mark or domain is the subject of an existing UDRP decision. If it is, the default is that you run the dispute in a UDRP proceeding before registration, not force it to happen afterwards, after some potential harm is done. *P. Argy*.

### Chinese, Japanese, Korean languages

It is important to look at how these languages will meet criteria set and what issues this raises. Also, instead of creating one centralized database or services for the GPML, maybe there's an alternative way of doing that by dividing the service into different languages. **[name missing from transcript—working for dot asia]**

### GPML—global consensus

How does the strict GPML criteria get global consensus? Countries have different jurisdictions, and different trademark laws with different protection. *G. Yuanyuan*. Regarding the point about different national laws and jurisdictions, the GPML was designed with some basic requirements. One is that you have a trademark registration of national effect. That will be validated by the IP Clearinghouse. There will be no question as to if it's a trademark from country x that's going to be more suspect than a trademark from country y. It's a question of adding it all up. If you have the required number of national registrations and they cut across all five global ICANN geographic regions, then that's the criterion. *M. Wong*.

## New York

### Transcript Summary

#### Globally protected marks list

The GPML is beyond ICANN's mission. There is no international consensus on globally famous marks. The GPML protects these trademarks not as marks for goods and services but as strings of characters protected across all new top-level domains, regardless of use or relevance. This list will remove from the domain name dictionary basic words such as apple, sun, time and people. *C. Climen*. We don't like the GPML, but would look at a list if produced by WIPO. *A. Van Couvering*.

#### Globally protected marks list

The GPML is not a famous marks list, but is a criteria-based list – e.g., very strict numbers for trademark registrations of national effect, across certain regions. All of the registrations at issue would have to have been issued prior to the date of launch. At any time that someone applied for a top level string, it would be compared to the marks on the GPML. If there was an identical match, the application would initially fail. Reconsideration would be possible; to prevail one would have to show that there is no confusion with the brand or that one has some sort of legitimate purpose. At the second level you also have an initial block, but the applicant also can go into reconsideration by a neutral third party and it was recommended that the same type of standards as used in the UDRP be employed. This process is designed to avoid having brand owners registering defensively every single mark they have and to also allow consumers to have access to some viable space. If the brand does not make it onto the GPML then you still have all the rights that are granted in the Draft Applicant Guidebook for the legal objection process. *F. Vayra*.

### Feedback Form Summary

#### General Comments/Questions

##### Region coverage requirement

Question: Please consider the issue of German companies that because of WW1 and the Treaty of Versailles (1919) cannot do business in the U.S. and Canada. Their house marks are registered in most other countries. Why should such companies not be allowed on the GPML with four out of five regions where their house marks are extensively registered? *Law Firm-Large Corporation*.

##### Additional sources of protection

We represent a not-for-profit sports and athletics association with globally protected trademarks. Although these marks are internationally well-known and protected, they may not be as extensively registered as commercial trademarks. Rather, we believe the GPML should consider additional sources of trademark protection, such as; - Special Statutory Protection (international) - Court Rulings (international) - Marketing Evidence of Global Recognition. We ask that additional flexible criteria be added. *Law Firm*.

##### Support with comments

This will remove a lot of wasted time and resources from the New gTLD application process. A welcome addition to the process. *Small Business*.

The criteria specifics (including threshold numbers) need to be defined, and there should be an opportunity for public comment on the specific criteria, once determined. No criteria should be finalized before public comment is considered. *T. Blasey, ITT--Large Corporation*.

Support, as modified by our filings on the record. *P. Flaherty & M. McKeegan, Verizon—Large Corporation.*

This is a very important protection so that owners of unique, well known and oft-used marks need not seek gTLDs solely for abusive reasons. *D. Bernstein, Debevoise & Plimpton LLP—UDRP Panelist.*

### **GPML requirements need clarification**

The threshold for inclusion on the GPML should be 100 trademark registrations. However, requiring certain numbers of them to be “spread” across each of the five ICANN regions may be problematic (a mark may be well known throughout the world, but certain regions may not have many trademark registered for various reasons—e.g., difficulty of doing business in certain countries). ICANN should also consider including in the IP Clearinghouse a “Regionally Protected Marks List”; criteria for this list will also have to be developed. *Hearst Communications, Inc.—Large Corporation.*

### **GPML criteria**

Regarding criteria for inclusion of a mark on the list or registrability of a proposed gTLD in the Pre-Launch Claims Service, ICANN should take into account the fact that sometimes a trademark owner will permit a third party to register a competing mark. There may be third party owned “competing” trademarks which would be viewed under ICANN’s criteria to be “competing” against the trademark owner’s marks. However, such marks are registered because the trademark owner permits them to be registered, under strict limitations. The existence of those marks should not be considered as “competing” marks in determining: (1) whether a trademark owner’s marks should be added to the GPML; or (2) in connection with URS proceedings; or (3) in connection with reconsiderations of initial evaluation proceedings. ICANN also needs to specify the projected costs for initial registration/continued validation of marks on the GPML. *Hearst Communications, Inc.—Large Corporation.*

### **Objection process and GPML**

If a trademark owner successfully opposes a gTLD application, then it should be moved onto the GPML to prevent any future applicant from attempting to register it or a close variation of it, since it would be stopped at the examination stage by the presence of it on the “reserved” list. This would prevent a trademark owner from having to submit and prosecute objections to the same or similar gTLDs multiple times. *Hearst Communications, Inc.—Large Corporation.*

### **Opposition**

The list does not exist and even within the trademark community there is substantial disagreement. When and if such a list is developed by WIPO and/or others, I could look at this as something possible. *Registry.* GPML should be broad enough not (limited to famous marks) to protect international commerce by protecting a broadly representative group of trademark holders engaged in international commerce (not just groups who have registered many URL’s but are not actually involved in commerce). *Professional association.* It’s like boiling the ocean. Too big of a problem, with few remedies that are not already in place. Just too complex as indicated by eNom. *J. LeMan, Lord, Abbett & Co.—Small Business.*

### **Revise second-level dispute process**

ICANN needs to revise the second level dispute process to mandate a standard sunrise process and incorporate the “globally protected marks” protection procedure for second level domains also. *Hearst Communications, Inc.—Large Corporation.*

## Appeals--location

ICANN needs to reconsider the IRT final report position regarding the filing of appeals in a court located in the country of the registrant or the registrar with authority to decide a case of cybersquatting or trademark infringement. This is a recipe for chaos and gaming of the system by domain registrants. *Hearst Communications, Inc.—Large Corporation.*

## London

### Transcript Summary

#### Globally protected marks list (GPML)

Demand Media fully opposes the GPML and urges its elimination and believes that other RPMs will better satisfy the objective of the GPML. The GPML will be very difficult to create because the criteria and threshold for getting on the list is inherently subjective. It will be very politicized and controversial among trademark holders and countries about who gets on the list and who doesn't. In addition, the GPML doesn't add a lot of value to the process—the GPML gives you no more real benefits at the top level than you have in the existing draft Applicant Guidebook. At the second level, inclusion on the GPML only gives quite marginal limited benefits. If the list truly has extremely well-known brands, each of them will only get one exact match protection at the second level in a TLD. Further, the GPML probably breaches the IRT guideline that an RPM not expand existing legal rights. *R. Tindal.*

#### Globally protected marks list

The GPML resembles a reserve list and is not a famous marks list. It is strictly built on criteria: a brand owner would have to have a certain number of regions for trademarks of national effect; those registrations have to have occurred before a certain date; we put in the concept of having your mark as a principal online presence – e.g., Delta would need delta.com to match its trademarks. The GPML would not replace any legal rights objections that a brand owner already has in the Draft Applicant Guidebook. If an entity does not have marks included in the GPML it can raise objection through that other process. The GPML has top level protection –no different from what is currently proposed in the DAG for certain ICANN terms. During the application process whatever is applied for would be compared with strings in the GPML and it is for exact matches only. If there is a match there would be an initial refusal which can be subject to a reconsideration process. Reconsideration is not an opportunity to submit new information but to clarify that you have a legitimate interest and your term is not likely to confuse regarding what it has been compared against. At the second level, again for exact matches only there would be an initial block but there would be an opportunity for reconsideration to show legitimate interest (using standards currently applied in the UDPR under 4C). *F. Vayra.*

#### GPML and WIPO

WIPO's understanding of the IRT's GPML recommendation is that it is intended to be a totally different type of list with criteria based on contract and therefore would have very little to do with WIPO's work regarding well-known marks. *Eun-Joo Min.*

### Feedback Form Summary

#### General Comments/Questions

##### Support with comments

The criteria should be revised. Whilst not wishing to expand the list to an unmanageable length, currently it's far too restrictive. *Large Corporation.* Please refer to our public comments. *C. Jamieson, MarkMonitor.*

In principle good but as it stands is very vague and so difficult to see if in practice will be satisfactory. *N. Leroy, CSC—Registrar*. Please consider for the GPML infractions where brand owners are excluded in jurisdictions for legal reason to hold trademark rights. *Large Corporation*. Great idea so long as multiple marks can be added and doesn't prevent genuine applicants registering from a non-competitive market. *Registrar*.

It is known that trademark with a reputation are the ones mostly infringed. The GPML offers brand owners a paper tool to recognize the worldwide existence of their brands and the investment related to their brands. *Nestle-SA—Large Corporation*.

Doesn't provide sufficient protection to GPM owner due to "identical" criteria. Must protect more than "identical" especially on second level. Protection of mark and typos and generic words such as chanelshop, chanel, chanle, etc. Marks that do not qualify for the list should be protected if they can prove they've been systematically abused in the past. Known cybersquatters should not be allowed to overcome a block just by opting in. *Large corporation*.

Establishment and especially use ought to be elaborated more before implemented. Miss some clarification re. "policing" and ongoing maintenance. Would love to help out. *LEGO--Large Corporation*. This would make protection a lot easier but consideration needs to be given to the small company with trademarks. Costs must be small. *Interest not specified*.

1. Costs of recordal should be appropriate - see my comments about the IP Clearinghouse.
2. What about the maintenance of list or for new brands to get on it? E.g. roll forward 5 years. A new brand gets registration in most countries of the world. If cut-off for GPML is November 2008, how can it get benefit? *A. Mills, Experian Ltd.—Large Corporation*.

It should be clarified that trade mark law is not a uniform international law. It is therefore imperative for trade marks to be protected globally from anti-competitive behavior and trademark infringement. However to have a list is incredibly difficult to do. As ICANN is aware, clear guidelines should be provided and it should provide for trademark owners who may not be in the top 250 brands list, for example. Common law rights should also be considered as well as those trademarks which have been registered due to acquired distinctiveness. I look forward to knowing (a) the criteria to be on the list and (b) the number (this has to be fixed) of those of the GPML. *R. Bond, EMI Group--Large Corporation*.

More certainty is required as to whether "globally protected" means famous. The two are not synonymous yet this seems to be the general feeling. Brand owners may have marks protected in dozens of countries, yet still not be owners of "famous" marks. While the debate over what is or is not a famous mark in any given jurisdiction will likely continue throughout eternity - the question of the magnitude of an owners' investment in protecting its mark "globally" however is not so vague a concept. Nor is the issue of the magnitude of its enforcement burden which is directly related. If the focus is taken away from the concept of fame, which is so subjective and likely not susceptible to being defined sufficiently to put together a viable "list" and put more on simply quantifying the "global protection", the constructing of such a list may actually be doable - the question then becomes simply how many registrations must one have to be "globally protected". *-Law Firm*.

## Opposition

Totally impractical. Unnecessary. *Registrar*. The GPML cannot be created without a clear rule set- which will be impossible to define. Better proposals have been made by Richard Tindal and Mr. Keating today. *Registry*. This may start out as a small and exclusive list of Trademarks and brands, but will soon

mushroom because of political and national pressures. *A. Barrow, Any-web Ltd. –Registrar/Domain marketing.* No company should have monopoly prior rights to a dictionary word. *A. Bennett—Reseller.*

This is a recipe for failure. Since 95+% of the English dictionary is somehow trademarked in specific fields of activity, a list with no country classification and no trade classification is impossible. It is a can of worms which could bring ICANN down because ICANN will end up in the heart of any and all trademark disputes. *O. Crepin-Leblond, Internet User.* Unsure what the additional protections this offers above IP Clearinghouse, apart from offering additional rights to large brands. *Interest not specified.*

I agree with the use of a GPML in respect of gTLD applications but NOT in respect of second level registrations. *R. Wickham, 2020 Media—Registrar.*

There are many examples of major brands also being “bad actors”. The GPML protects those, who arguably, need the least assistance given the nature of a global brand. Moreover, the additional new gTLDs with more secure/rigorous controls specific to certain special interest groups “should” reduce this need. *J. Robinson, Small Business.*

1. The beneficiaries of GPML are those who already can look after themselves: the victims as I see it are those for whom resources are much tighter and the fees for UDRP etc are beyond reach. 2. The cut off for protection is arbitrary. 3. This is a real attack on first come first serve (FCFS) domain registration. Once a block list is established then religious groups, governments, politicians etc. will seek to expand the list e.g., for expletives. Ultimately it will make domain name registration slower, more expensive etc. which is not in anyone’s interest. *Nick W-S, Nominet--Registry.*

Why should only globally protected marks be entitled to protection? My trademark registrations entitle me to protection so I should not have to incur additional costs. Identical matches should be extended to cover combinations e.g., applecomputer, nikeshoes, etc. The GPML should include all trademarks registered anywhere in the world and therefore doesn’t require a new list. The onus should be on the registrant to ensure his application does not infringe prior rights. *Small Business.*

### **GPML eligibility**

Do not agree with setting limit on number of globally protected marks (e.g., 100, 1000). Anyone who meets criteria should be entitled to achieve status of GPM. Further study on requirements need to be fully consulted upon. *Large Corporation.* Our German clients particularly are concerned (and they are major brand owners) that they will not meet the numerical requirement for trademarks in North America because of the narrow definition of “goods and services” in the USA. We heard you have commissioned a survey to define criteria. Please consider European companies in your consideration. *Registrar.*

The threshold for getting GPML status is too high. Further, an exclusively quantitative documentation requirement for GPML should be changed to encompass also qualitative criteria as is the fact for national and regional famous/well known/reputation trademarks. *C.B. Christiansen, Danish Lawyers Assoc.—Professional association.*

### **More details needed**

Very difficult to comment given the criteria are not specified. If the GPML is available to a sufficient number of trademarks and acts as a block, then yes. Details are needed. *S. Payne, BBC Worldwide—Large Corporation.*



### Near term feasibility concern

Whilst I am in favor of the list, I doubt that it is feasible as proposed in the near term; in the long term it can be linked in with the IP Clearinghouse as a way to invert the burden of proof for a selection of often-infringed trademark strings. *W. Staub, CORE--Noncommercial organization.*

### Size of list

It depends how big the list is. If under 1,000 it could be okay; indeed, it could be very helpful to us as domain marketing specialists. *Domain marketing.* Support, but am concerned if number(s) of marks is too great—e.g., over 1,000. *Small Business.*

## Uniform Dispute Resolution Procedure (UDRP)

### Sydney Feedback

#### Cybersquatting and number of UDRP cases

The issue of whether the number of UDRP cases filed with WIPO is actually going down proportionate to the number of domain name registrations needs to be assessed. Also, how do you know if a rise in UDRP actions is a rise in cybersquatting instead of a rise in trademark owners seeking more protection from the UDRP than it was originally drafted for? *K. Kleiman.* An offered correction to that point is that total UDRP cases have had declines year over year on an absolute basis (total cases filed across all providers in the UDRP has gone down on an absolute basis); the total cases under WIPO (the percentage, WIPO's market share) have gone up. *E. Noss.*

#### UDRP scope

From large brand owner perspective, the UDRP only deals with a very small number of gTLDs; there are other dispute mechanisms that brand owners file in. Based on having to file one of these a day, the numbers have gone up, based on personal experience. *J.S. Evans.*

#### System abuse: use of UDRP as alternative domain acquisition procedure

We have seen a significant increase in the use of the UDRP as an alternative domain acquisition procedure for rights owners and other trademark holders. It is a way to go after a domain name at a cost of \$5,000 that might cost \$50,000 or \$100,000 to go and acquire if it was available at all. The discussion must be balanced by recognizing that there are good actors and bad actors on both sides of this issue. What needs to be part of the dialog is that there is abuse of the process. *E. Noss.*

#### Support for IRT results; electronic UDRP pilot

The Czech Arbitration Court supports the results of the IRT team as work in the right, forward-looking direction, and notes that ICANN approved its pilot for electronic UDRP on 21<sup>st</sup> of May, and the Court is now receiving new, only online cases. *Z. Loebel.*

### New York

#### Transcript Summary

##### UDRP reform

While ICA does not object to the standard sunrise and the IP clearinghouse with some modifications, the URS denigrates due process rights. Instead, there should be an expedited policy development process for those who are concerned about the UDRP. This would solve a lot of concerns and an improved system would be put in place at .com and at other incumbents where most of the major infringement concerns are. By doing this through ICANN's policy process, ICANN will insulate itself from a lot of potential litigation if it follows its own rules. *P. Corwin.*

## London

### Transcript Summary

#### Problems with the UDRP

There is a lack of judicial oversight of UDRP decisions in many jurisdictions in the world, as well as a failure to apply traditional trademark laws. The UDRP system is unbalanced and it is largely unmanaged by ICANN. If you measure the number of UDRP claims today based on the number of registered domain names you would find a precipitous decrease in the actual number of UDRP cases when compared to the number of registrations. While many cases default, many cases are defended and in many cases the cost of defense is much higher than the cost of actually filing the complaint.

There is no importation of local laws of the applicable jurisdictions into the UDRP process with respect to looking at the rights of the respondent, whereas those local law concepts have been imported with respect to the claimant having trademark rights.

A complainant can win even when the trademark did not exist when the domain name was registered. Complainants can claim a trademark right even when the term has been expressly disclaimed in the trademark registration in which they're actually asserting the claim. There are many instances in which UDRP panels are reaching conclusions that contradict the actual intent expressed in the documentation that created the UDRP process. *P. Keating.*

#### Remedy—URS or UDRP but not both

There should not be a “free do-over”—that is unfair to the defendant. If you choose the URS, then that should be your process and that should mean you have waived your right to use the UDRP.

#### Proposal to amend the UDRP instead

Instead of a separate URS process, an amendment should be made to the UDRP process—specifically that a respondent at day 14 can pay a small fee and elect to defend the domain name, the domain name stays up and alive, and the UDRP process continues as normal, with a response due in six more days. If the respondent elects to surrender the name, then the UDRP process halts and the domain name is transferred. If the respondent does nothing, then the domain name is immediately suspended and the UDRP process returns to its normal course, with the exception that the web page no longer resolves (it could go to a controlled blank white web page). This proposal does involve amending the UDRP process and there is a clear desire to modify the UDRP. The new gTLD context provides an opportunity to test this proposal and see if it works; if it does, then it could be applied to existing gTLDs (.com, .net, .info, etc.). *P. Keating.*

## Uniform Rapid Response System (URS)

### Sydney

#### Overview

The URS is designed to go after bad actor cybersquatters, not for the more fringe scenarios where there may be some alternative generic meaning to a trademark or in some jurisdictions a free speech or other fair use scenario. How the URS works: ICANN would select a neutral dispute resolution provider. It would involve a complaint, notice to the registrant, an answer, case evaluation, a decision by a qualified legal expert to be chosen by the dispute resolution service provider and then means for appeal. Once the complaint is lodged with the third party dispute resolution service provider, the web site will immediately be “frozen” (not shut down but cannot be transferred). If the complaint is successful, the site will remain frozen, and the content will come down and instead will redirect to a standard URS

process page. If the complainant wins and there is an appeal, the web site goes back up during that appeal process. There are also provisions to deal with abuses by aggressive trademark holders. If there has been an abuse of the system three times, that particular complainant will be locked out of the system for one year. It is important to note that there is no transfer of the domain name happening; we are not looking to replace the existing UDRP but are solely looking for the removal of the abusive content. *R. Pangborn*. Both the URS and the UDRP are intended to be alternative dispute resolution procedures that complement existing national legal procedures. In the IRT report discussion of the URS, it was made clear that the court option would always remain available. *E. Min*.

### **What constitutes “abuse” of the process is unclear**

Whether the balance of the process is tilted too much in favor of complainants centers around what the threshold is for determining whether it’s a clear-cut case as well as what abuse looks like. *J. Buchanan*.

### **URS –agreement modification for changing domain name settings**

Responding to J.C. Vigne inquiry, the new TLD agreements will establish the ability for registrars to change the settings of the domain names in the context of the URS where the domain name is “frozen.” *J. Neuman*.

### **URS should go through the normal ICANN policy process**

The “URSP” is a major new policy which should go through the normal ICANN policy process. *P. Corwin*. *J. Buchanan*.

### **Opposition to URS; it will replace the UDRP**

The statement on page 25 of the final IRT report that the URS is intended to supplement and not replace the UDRP is completely erroneous. In an April letter WIPO has stated that in analyzing 400 UDRP cases, an expedited suspension mechanism (ESM) limited solely to identical matches would capture a significant majority of UDRP disputed domain names. Is it not reasonable to assume that an ESM which extends to confusingly similar names would capture the vast majority of UDRP cases and would in fact be the new UDRP at all new gTLDs? *P. Corwin*. URS will replace the UDRP. *K. Kleiman*. WIPO shares the IRT’s view for the need of a rights protection mechanism that would narrowly complement the UDRP, not replace it. It is not the case that the ESM would cover the vast majority of disputed names if we limited it to identical. The April WIPO letter says that the vast majority would be covered if we include the category of disputed domain names that include identical and also domain names that incorporate the trademark in its entirety. *E. Min*.

### **URS would be an inefficient and unfair process**

The harm could be addressed more fairly and efficiently by, e.g., putting the registration on hold until a UDRP hearing has been conducted. That is better than the risk of the applicant investing in the web site only to lose it summarily. URS should be reserved for cases with identical marks or marks already the subject of a finding of rights. *P. Argy*.

### **URS process is unclear**

Much clearer instructions are needed for URS; so far as described the URS process seems a bit like “I know it when I see it” and does not appear to be clear cut. *D. Yee*.

### **WIPO comments on IRT final report URS proposal**

There are some significant differences between the WIPO ESM proposal and the final IRT report URS proposal. The final IRT report is a shift from the draft IRT report in that it requires a full examination by a panelist also in cases of default. WIPO believes it would be more efficient to filter out these default cases but without a full examination by a panelist. There should be a process for a domain name

registrant that did not respond within the time period to put up a claim and assert legitimate interests and if those interests are proven to retrieve that domain name. Also, the WIPO proposal recommended that the suspended domain name be put on some sort of reserve list so that it cannot be registered immediately thereafter. The IRT is recommending that the domain name be suspended for the duration of the life of that domain name registration. In practice it will probably mean a suspension for a few months, maximum, and then it will go back to the pool and be subject to cybersquatting again. Providing a remedy of such limited effectiveness would force trademark owners into engaging repeated serial URS proceedings in lieu of defensive registrations. *E. Min.*

### Technical and email privacy concerns

How will the URS deal with the 65,534 other ports allowed by the TCP/P protocol; how will incoming email be dealt with for the suspended domain, a crucial privacy issue which could lead to interception of e-mail? *P. Vande Walle.* The name servers will be redirected to the name servers of the service provider who will display that page, so all of those applications will be shut down, including email. *J. Neuman.* Some controls are needed on where it gets redelegated to and what that other party is allowed to do. That other provider could actually intercept email if it set up MX records. *B. Tonkin.*

### Notification—14 days is unworkable

The 14 days response period is unworkable. There should be a possibility to extend it given how long certified mail can take and problems with email reliability and spam. *P. Vande Walle.* This point is valid and it is actually one of the reasons why the IRT differed from WIPO and required an evaluation in the case of a default, because of scenarios where notice is not effectively delivered in a timely way. *J. Neuman.* The default answer that is built into the process anticipates the scenario where you are on vacation during the registry of your domain and did not receive the notice in time. *R. Pangborn.* The 14 day notice period is unfair and inadequate and will lead to gaming of the system. *K. Kleiman.*

### URS modifications suggested

- (1) There should be a competitive service provider process.
- (2) There should be a separation between the business processes and adjudication process in the URS. Complainants would have the ability to select the supplier of their choice who would provide those business processes. The adjudicator would be assigned, as opposed to the current UDRP system which allows complainants to shop for adjudicators.
- (3) Fundamental fairness needs to be at the core of the process. An adjudicator must qualify for the post; they could be a panelist in the existing UDRP but they would then forgo the ability to appear before the panel, such that practitioners would have a choice. They could be on either side as complainants or respondents. They could either be panelists in the process or they could choose to be advocates in the process. The UDRP lacks that fundamental principle of administrative fairness. *E. Noss.*

### Criteria

Regarding terms – registered and used in bad faith, will there be an “and” or an “or” word used in the criteria used by the examiner? Also, page 35 is confusing and may need to be revised. *Victoria B.* The intention is not to create new criteria and to use the same criteria as the UDRP. *B. Tonkin.*

### Deterring URS abuse

While the URS is sound, as established eNOM believes it will be abused. To reduce abuse, the URS should be made more expensive to use, and the threshold under which you can be deemed abusive should be lowered. *R. Tindal.*

## Effort should go to fixing the UDRP

The URS seems like a Band-Aid for the UDRP. If the URS is a supplement, why isn't it more of a feeder into the UDRP process? *Ed. J. Buchanan.*

## New York

### Transcript Summary

#### URS

The URS is designed to address in a faster and less expensive process for brand holders the substantial number of UDRP cases that go unanswered (we understand it is 70% of the UDRP cases are clear cut and there's never an answer). The URS remedy does not require transfer or acquisition of the domain name, unlike the UDRP. The URS remedy is for slam-dunk cases where you just want to take down the name. Upon URS initiation the domain name would be frozen for transfers, and there would be notice, via email, registered letter and another email, of the URS complaint. Fax notice is being examined. The standard of proof for the URS complainant would be clear and convincing evidence that there is no contestable issue. Every complaint will go to an examiner who will look at the merits of the case regardless of whether an answer is filed or not. If the examiner finds in favor of the complainant, then the domain name is frozen at the registry and the DNS record associated with the domain name is updated to redirect web traffic to a website with a standard URS process page. That means that the website would resolve to a standard error message that is hosted by the third party provider. Complainants must agree to indemnify third parties based on the representations in the complaints. Complainants are subject to a ban if they abuse the system by filing three abusive complaints, and there are rights of appeal. **[Male not identified]**

#### URS-opposition

The URS will replace the UDRP with a faster, cheaper and fundamentally unfair process. Domain name registrants will lose their domain names and website speech before they even know a challenge has been filed. What is needed is UDRP reform, not its replacement. *C. Climen.*

#### URS—improvement suggestions

The URS is very important to trademark owners but it only allows for domain names to be frozen, which isn't adequate protection for trademark owners. Domain names should also be available for transfer to the trademark owner. Further, the URS is not "rapid" enough. *P. Flaherty.* What is the basis for claiming that the URS will open up a lot of abuse by trademark owners? No model should be based on the fringe cases. It should be based on the 95% of cases that are legitimate. *B. McMurtrey.* If 5% of the URS cases are abusive in some way, we should find a way to minimize that, and the notion of a bond or something of that nature is worth considering. *R. Tindal.*

#### URS—qualification to use it

If there is a minimum number of domain names that must be registered by a registrant in order to qualify for using the URS, that seems to allow hackers to know how to game the system and avoid enforcement by registering N minus one domain names. *M. Trachtenberg.* The URS is trying to get at bad actors who really have a lot of domain names. *R. Tindal.* The concept of aggregating domain names and looking at the number is in the proposal. *J. Neuman.*

## Feedback Form Summary

### General Comments/Questions

#### Support

Finally rapid take down! Good job! *Small Business*. Support, with higher penalties for wrong claims. *Interest not specified*. URS - like regimes work well in the ccTLD space. If this is worked out properly, this could work well. *Registry*.

Support, as modified by our filings on the record. *P. Flaherty & M. McKeehan, Verizon—Large Corporation*.

I think this is essential to prevent abusive cybersquatting. Just the existence of the URS will have a prophylactic deterrent effect. I do think all cases should be reviewed by a panelist and not granted if default - it will force complainants to bring only appropriate cases because they will know someone will give the file a substantive review even in default cases. I have ruled for defaulting Respondents and have even awarded RDNA in such cases. *D. Bernstein, Debevoise & Plimpton LLP—UDRP Panelist*.

#### Fees

Fees should be shifted, and/or bond or escrow amount established, to pay for successful brand owner's URS action. *T. Blasey, ITT--Large Corporation*.

#### Needs more work

Needs more work, as indicated by WIPO and eNom. Two issues: -No default judgment. -Names are not transferred, just suspended. *J. LeMan, Lord, Abbett & Co.—Small Business*. More details are needed about URS operations: how the examiner panels will be constituted; qualifications for individual examiners; and the mechanism for enforcement by the registrars of the panel's decisions. *Hearst Communications, Inc.—Large Corporation*.

#### London:

### Transcript Summary

#### URS

URS is potentially the most powerful RPM in the IRT report but it should be modified. Demand Media is concerned that the URS will be abused by some overreaching trademark holders, malicious parties and competitors. Demand Media would like to see more discussion on possibly increasing the URS claim fees or compressing tiers so that there is less potential for abuse (e.g., the National Arbitration Forum is on record saying that \$200 is not an amount that any capable adjudicator is going to be able make judgment upon) Also, if the intent is to go after serial cybersquatters, then the minimum threshold of names subject to a claim should be raised. *R. Tindal*.

#### Timing and other requirements

The URS is not very rapid—we have to wait until after an examiner who is paid \$100 gives an opinion. It has a poor notification system. Facts should be included in the process and exhibits should be transmitted electronically.

#### Trademark law interpretations

Despite the requirement that the trademarks have to be registered in a jurisdiction with a substantive review process, there are limitations—e.g., the U.S. has a substantive review process but you can also submit a declaration under Section 2F and claim acquired distinctiveness which is viewed only on an ex parte basis and only on a prima facie case basis. So you get registered trademarks for the likes of “Cheap

Auto Insurance” used to sell insurance; it is doubtful that those are the types of trademarks that the IRT had in mind but those are the trademarks that nevertheless can fulfill the rules. There are also figurative marks issues; e.g., in the UDRP context and presumably the URS the owner of a figurative mark “cars” could claim all rights to the word “cars” and challenge the domain of a registrant who is using it in pay per click (PPC) to sell automobiles.

### **Burden of proof**

The burden of proof standard—a well-developed U.S. standard being imposed on the rest of the world—provides no absolute rules for the panelist and the rest of the world will not be able to appreciate that standard. There is no concept of legitimate interest. Bad faith is all-inclusive.

### **Suspension; abusive complaints**

The suspension concept creates difficulty. Trademark holders, as part of their obligation to police their marks, should keep the names. For example, Verizon claims publicly to have recovered nine million new users, new customers, based upon the domain names that they have recovered through the dispute process. In that context the suspension concept is hard to understand. The whole concept of abusive complaints is far too tolerant.

### **Expedited domain name suspension mechanism**

This would apply to the second or third levels, and while akin to the URS has these significant differences: (1) in case of a respondent default, there will be an automatic suspension, but at the same time there would be adequate safeguards to protect rights of registrants who for a legitimate reason were unable to respond in time. There would be a very low burden on the registrant for responding to the complaint; (2) the remedy provided would be of a more lengthy duration—at least a few years, not just through the life of the domain registration itself—so that trademark owners would not be perpetually engaged in these URS proceedings and the system would be more cost-efficient. *Eun-Joo Min*.

### **Uniform Rapid Suspension System (URS)**

URS is meant to supplement UDRP not to supplant it, by creating for brand owners a faster, less costly process for slam-dunk cases to get these domain names down. A neutral provider would be appointed through ICANN. There would be two ways for a brand owner to file a complaint. Pre-registering through the IP Clearinghouse would be cheaper because you would not have to provide evidence with each filing—it would already be on file. There would be need to be submitted by the complainant a form complaint and screenshot of the website filed with the URS provider. Following an initial examination confirming requirements are met, within 24 hours the domain name would be frozen and could not be transferred. At that point the site is still resolving. The registrant is given notice of the complaint by email and certified mail, and we are looking at fax also, and has 14 days to respond via a form. There is an opportunity for the registrant to claim that the complaint is abusive. If no response is filed, then there is a default. The examiner considers the complaint, whether there is an answer or not, and the examiner gives a response. If the examiner finds that it is a clear cut case they will keep the name frozen until it is up for renewal and the domain name will no longer resolve to the active web page; it will go to a page that says it has been taken down, and there will be a notation on the Whois record that it has been taken down. This will give notice to people who may be trying to buy the name from the registrant who may be trying to transfer it, and also gives notice to people who may want to register the name when it is up for renewal. If brand owners want the name transferred, then they can use the UDRP or courts for that, not the URS process. At the end of the registration the name would be up for renewal—brand owners could try to get it or there may be someone else with a legitimate right to the name. The domain name registrant can appeal the decision subject to certain time periods. In the case of an appeal

to the URS ombudsman, if it is determined that the examiner overstepped the bounds then the amount of the appeal will be refunded to the appellant. Complainants have to indemnify third parties based on representations in the complaints. Complainants are subject to a one year ban from the URS system for filing 3 abusive complaints. *S. King*.

### URS appeal process

There are two types of appeals—a default situation type and a substantive decision by the panel. If there's a substantive decision by the panel, an appeal to the ombudsman would not unfreeze the name. The only time the freeze is lifted is if it's a default and the domain name holder wants to appeal to a court. **Male unidentified** responding to *A. Mills*.

### Feedback Form Summary

#### Support with comments

Both implementable and justifiable; full support. *Large Corporation*. Urgently need something cost effective as we have for .uk. *Small Business*.

Support, however, I do not agree with some of the suggestions. Freezing should be long-term. There should not be a minimum number of domains against which a complaint can be made. I am broadly in favor of WIPO's amendments. *R. Bond, EMI Group—Large Corporation*. Suspension should also include taking down the website so that it deters infringement and counterfeiting. *Interest not specified*.

Support, except do not want to put my clients through 2 processes—i.e., URS and UDRP. URS must be quick and inexpensive. *A. Wong--Trademark attorneys*. If the cost is greater than defensive registration then what is the point? *Nick W-S, Nominet-Registry*. Support, but we need a mechanism for repeating offenders and typosquatters. Maybe a slight modification to UDRP would work better than reinventing the wheel? *Interest not specified*.

But should be by default when complaint raised, unless there exists previous decision, thereby cutting the window of cybersquatters down to a minimum, and cutting the time window a cybersquatter can profit. For trademark owners a slight delay of usage of a new domain is preferred to let squatter run "wild." *LEGO—Large Corporation*. What about non-English/non-ASCII domains/registrar? *R. Wickham, 2020 Media—Registrar*. Improve the system. *Registrar*. Please refer to our public comments. *C. Jamieson, MarkMonitor*.

#### Analysis and process questions

Will cases of non-exact match infringements, for example, typo or exact match and affix be considered clear-cut cases? My question is will there be a checklist where all criteria have to be met in order to bring a site down or will it be reviewed on a case by case basis? *N. Leroy, CSC-Registrar*. URS examiners have to have a certain amount of training. As well as deciding on "slam dunk" cases, they also are asked to decide on whether complainants acting in bad faith/being anti-competitive. In this case quite a high level of examination is required. Is appeal to UDRP of right? Perhaps consider if being on standard legal basis—errors of law or errors of fact—to ensure not duplicating actions. *Large Corporation*.

#### Recommendations

We need a loser-pays mechanism. Obvious types should be covered by URS. Fee must be low. No need for substantial examination if default decision. Domain must be frozen for at least 5 years after the decision, and should not go back into circulation after less than 1 year. Not quite clear which cases are slam dunk—please give examples. *Large Corporation*.



### Abuse concerns

Concerned about unlocking of a domain on appeal—could be abused by a “bad actor” registrant to move domain or create other disruption problem. I am strongly against the commercial necessity to obtain a domain name by threats/UDRP/litigation when it is never a domain name that the business would have bought. The ongoing cost of maintenance is an unnecessary burden. *A. Mills, Experian Ltd.—Large Corporation*. Support, but need to ensure it is not used by trademark holders to harm competitors and should only be used to protect from strong infringement. *R. Coghill, Group NBT PLC—Registrar*.

### Notice

Support inclusion of fax for notice. *A. Mills, Experian Ltd.—Large Corporation*.

### Cost/Timing

Must be very low cost to brand owners and quick resolution. *S. Payne, BBC Worldwide—Large Corporation*.

### Recommendations

(1) URS should be integrated with UDRP; (2) Add faster option; (3) Add opt-out of registrant of URS in exchange for vetted contact data. *W. Staub, CORE-- Registry-Registrar-Professional association interest*.

### Relationship to UDRP

Could it be combined into the UDRP as a first step? We give names back already if we sweep them up by mistake. Free mediation like with Nominet would be good. *Domain marketing*. How does this relate to UDRP, i.e., once a site is frozen, can you then apply to URS for a transfer? *Interest not specified*.

### Opposition

Concerned about abuse and creep.

*A. Barnett-Registrar*. I agree with all of the points made by Paul Ketting from Law.es. *A. Bennett, Reseller*. This proposal favors trademark owners, irrespective of whether trademarks are coined words, famous marks, or common words. The URSS could be abused by holders of common words trademarks. *O. Crepin-Leblond, Internet User*. URS needs to be revised. Do not agree with bringing one complaint against multiple domain names and multiple registrants. Each domain has different nuances which must be considered. *A. Barrow, Any-Web Ltd.-Registrar/Domain Marketing*.

### Opposed to URS; improve UDRP instead

The UDRP process should be improved. If someone is found to be malicious they should be charged “costs” or some kind of fee and until paid, all domains in their ownership placed on hold. *Interest not specified*.

## Post-Delegation Dispute Mechanism (PDDM)

### Sydney Feedback

#### PDDM focus

PDDM is for systematic cybersquatting that occurs on the second level. It does not impose on registries a monitoring requirement about registrations. It has to be systematic cybersquatting where there is a bad-faith intent to profit by the registry itself. *J. Neuman*.

### **PDDM is unnecessary**

It is better to leave enforcement in the hands of ICANN rather than have a third party involved. The trend of third party involvement in enforcement is a concern. If the problem is ICANN enforcement, let's do something in ICANN to get contracts enforced, and not hand things to third parties. *R. Tindal*. WIPO believes in the preventive effect of the PDDM and believes it is needed. *E. Min*.

### **ICANN enforcement of contracts**

To be clear, ICANN has stepped up enforcement efforts and there is no interest in having contracts that are not enforced. *P. Dengate Thrush*. With regard to ICANN staff and the enforcement process, for technical questions such as if there is trademark abuse, it may be more efficient to ask a neutral panelist who has expertise in the field to make that determination and make a recommendation to ICANN for its consideration. *E. Min*. AIM supports the PDDM. The history of ICANN enforcement is not good. *P. Sheppard*. ICANN should be given the tool of graduated sanctions to bolster its enforcement capabilities. The work done here should feed into a policy development process that could apply to all the existing contracted parties which would presumably have a much broader and useful effect. *J. Buchanan*. The recommendation was that graduated sanctions are not supposed to apply only in this situation, but that ICANN should in its contracts have graduated sanctions. The recommendation was silent on when those sanctions could be exercised. *J. Neuman*. There is a graduated sanctions program for registrars in the registrar accreditation agreement the ICANN Board has approved. WIPO is recommending a similar graduated sanctions procedure for registrars as well.

## **New York**

### **Transcript Summary**

#### **Post delegation dispute resolution mechanism**

The PDDR is intended to address bad actor registry operators who act inconsistently with representations they have in the registry agreement or if they act in bad faith with intent to profit from systemic cybersquatting. Third parties submit a claim to ICANN which then is required to investigate it and will take enforcement action if there is a breach of the registry contract. If the claim is unresolved, then the third party can initiate the PDDR process which will entail a comprehensive arbitration-type process with an investigation by a neutral third party and a panel decision. Standing is given to the party that is actually harmed by the activity. *J. Neuman*.

#### **Post delegation dispute resolution**

This raises concern--ICANN should police its own contracts. *A. Van Couvering*. We have strong objection to the post delegation dispute resolution mechanism as drafted. *C. Climen*.

### **Feedback Summary**

#### **General Comments/Questions**

##### **Apply to all TLDs**

Make this retroactive to all current and future TLDs. See comments posted by Danny Younger in response to travel request to offer 1 -x 2 - character domain names. Perfect example of where post -delegation should be used. *Small Business*.

Again, this is important to provide deterrent effect on misconduct by registrars. To have the effect, the panel needs to have the ability to award remedies with real teeth. *D. Bernstein, Debevoise & Plimpton LLP—UDRP Panelist*.

### Support with comments

Need to protect against abusive practices of registries and cybersquatters and not overburden trademark owners' ability to protect their marks. Registrants should share more of the monetary burden. *Professional association.*

Support, as modified by our filings on the record. *P. Flaherty & M. McKeegan, Verizon—Large Corporation.*

### Needs more work

Needs more work on the business case analysis to determine costs/fees for resolution. *J. LeMan, Lord, Abbett & Co.—Small Business.*

### Opposition

This is a complete usurpation of ICANN's authority to administer its own contracts. *Registry.*

## London

### Transcript Summary

#### Post delegation dispute resolution mechanism (PDDR)

Demand Media supports the concepts in this RPM that a registry must perform consistently with its contractual obligations and with its proposal undertaking. Demand Media objects to the portion that provides third party beneficiary rights and uses words like "intent to profit" and "bad faith" and "manner of operation." These terms are inherently hard to quantify. Demand Media would like this area dropped—third parties should not be injected, and ICANN should be the one performing the compliance. We disagree with the view of some that ICANN is not doing a great job of making its contracted parties comply. If there is a problem the solution is for ICANN to increase its resources and its focus on compliance activities. *R. Tindal.*

#### Background on the post delegation dispute resolution mechanism

It is intended to apply to situations where TLD registries are causing or materially contributing to trademark abuse —e.g., the registry is using the TLD for a purpose inconsistent with relevant representations made in the application phase such that trademarks are infringed; or when a TLD operator turns a blind eye to systemic cybersquatting in its domain instead of adopting appropriate mechanisms to counter such abuse. We are recommending that ICANN consider adopting this mechanism not only for registries but also an analogous procedure for registrars. We believe that having such a mechanism in place will have a deterrent effect that will guide all relevant actors toward more responsible conduct, to make registries and registrars mindful of their involvement in any trademark abuse occurring in their space. *Eun-Joo Min.*

#### Post-delegation dispute resolution mechanism (PDDR)

The PDDR is intended to provide a way for complaints to be submitted to ICANN in situations where there are bad actor registry operators who act inconsistently with the representations made in their agreement or have bad faith intent to profit from systemic cybersquatting. Per the IRT proposal, ICANN would be required to investigate those complaints and determine if there has been a breach of the registry agreement. If there is a breach then there would be enforcement similar to the remedies included in the Registrar Accreditation Agreement which the ICANN Board signed off on (e.g., monetary sanctions, suspension or termination of the registry agreement). If the issue is left unresolved or ICANN does not act on the complaint, then the third party can formally initiate the PDDR, which will require a more comprehensive arbitration process. It has to cause confusion with the complainant's mark—it's

not intended to give a cause of action to any person or entity. The first applicable dispute is where the manner of operation or use of a TLD is inconsistent with the representations in a TLD application and such operation is likely to cause confusion with the complainant's mark. A second applicable dispute is for breach of the rights protection mechanisms that causes confusion to the complainant's mark. The third applicable dispute is that the manner of operation or use of the TLD exhibits on the part of the registry a bad faith intent to profit from the systemic registration of domain names which are identical or confusingly similar to the complainant's mark. This is not intended to obligate registries to do any monitoring, but it is intended to address the case where a registry may have a bad faith intent to profit from domain name registrations. In the PDDR a complaint is filed with a neutral provider which will then issue a decision and make a recommendation to ICANN on the remedy. There are also sanctions possible against the complainant if it is a case where the complaint was filed to harass the registry operator. A complainant would be barred from further filings if there are three separate occasions where a complaint is found to be without merit. There would be pretty extensive costs for filing this type of action. *J. Neuman*.

## Feedback Form Summary

### General Comments/Questions

#### Registry agreement

This issue really should be covered in the ICANN registry agreement. *A. Barnett—Registrar*.

#### Support

Please refer to our public comments. *C. Jamieson, MarkMonitor*. Total support is offered. *Large Corporation*. Bad registries get the business a bad name. We are impacted too as registrars. *Domain marketing*. Cannot really understand why ICANN does not undertake its own compliance, but support anyway. *Small Business*.

#### Opposition

ICANN has in place mechanisms through its contracts with registries. This proposal will discourage applications from small and innovative new gTLDs. *R. Wickham, 2020Media—Registrar*. Not sure I understand how PDR works with regard to existing procedures and what the PDR mechanism adds to the process. Why not improve registry compliance by ICANN? *R. McGary—Registry*.

#### Competition for provider

ICANN should invite interested dispute resolution providers to compete to become the post-delegation dispute resolution provider. The Czech Arbitration Court is interested in participating in such a competition. *Z. Loebel, Czech Arbitration Court—Noncommercial organization*.

#### Pre-delegation suggestion

Similar concerns might be used for a pre-delegation objection process to address excessive external costs. *W. Staub, CORE—Registry/Registrar/Professional association*.

#### Clarify PDR

Does this only cover the .apple example? Would it also cover a registry selling second level domain names containing famous trademarks to non-trademark owners for commercial use (e.g., PPC)? If such sales are systematic...registries should be forced to monitor. *Large Corporation*.

### Time limit concerns; prove effectiveness by using mechanisms first with existing TLDs

Freeze and deace should not be time-limited. Built-in time limits of this sort will be to the benefit of squatters and other criminals, but just an added cost and nuisance for trade mark owners. Why not prove the suggested processes to the existing TLDs, then after a test period before pushing on to implement gTLD? *LEGO—Large Corporation*. [question—is this more of a URS comment?]

### Process

Once resolved the brand owner should not have to maintain the infringing domain. It should go into “dead space” being blocked but for no fee. *Interest not specified*. [question—is this more of a URS comment?]

## Thick Whois

### Sydney

#### Feedback Form Summary

##### The thick Whois approach is narrow-minded

It seems that it is acceptable to introduce a GPML which basically creates a tiered trademark holder type scenario where a small trademark holder doesn't get to be on the list and a few big brands do, which is controversial. At the same time, the position is that the status quo regarding Whois and what is and isn't displayed should be maintained, while ignoring that ICANN has given dot tel the opportunity to grant private individuals the opportunity to opt out of Whois display. [name missing from transcript]

### New York

#### Transcript Summary

##### Thick Whois

The Draft Applicant Guidebook has recommended a thick Whois for all new gTLDs. It is notable that every single gTLD with the exception of .com, .net, and .jobs has a thick registry. In jurisdictions where it is not an issue (e.g., privacy laws don't create an issue), then registries are to not only collect all of the thick Whois information but they should also display it. The IRT also recommended that ICANN work to establish a centralized Whois system so that IP owners, consumers and others could go to this centralized source to find information on all the gTLDs as opposed to going to, e.g., 500 registries to get the information. *J. Neuman*.

##### Thick Whois

Thick Whois is a great idea. *A. Van Covering*. We have strong objections to Thick Whois as drafted. *C. Climen*.

#### Feedback Form Summary

#### General Comments/Questions

##### Support with comments

Thick Whois should be applicable to all registries - current and future. *Small Business*. This is a good idea. The original idea for “thin” Whois was just a ploy by NSI for commercial purposes. A thick Whois makes much more sense. *Registry*. Ensures accountability if a claim needs to be made. *J. LeMan, Lord, Abbett & Co.—Small Business*. Support, as modified by our filings on the record. *P. Flaherty & M. McKeehan, Verizon—Large Corporation*.

As a UDRP panelist, I have been very frustrated by the thin WHOIS data that sometimes is available, which makes it difficult for us to ensure a fair result. *D. Bernstein, Debevoise & Plimpton LLP—UDRP Panelist.*

## London

### Transcript Summary

#### Thick Whois

Mandatory Thick Whois is a significant improvement (as there is no thick Whois in .com and .net which constitute 84% of all gTLD registrations). Demand Media supports the thick Whois proposal and recognizes that ICANN has in place a policy mechanism to deal with scenarios where a registry is in a jurisdiction where privacy laws could prevent the publishing of a Thick Whois. *R. Tindal.*

#### Thick Whois

The IRT recommended Thick Whois for all the new gTLDs. Thick Whois is a central registry level of Whois information for all the domain names registered in that registry. It ensures consistent data and faster lookups. If a registrar goes under all the information is maintained. IRT recommended that ICANN consider the option of a centralized Whois registry where all of this data could be deposited. *S. King.*

### Feedback Form Summary

#### General Comments/Questions

##### Do not make it commercially available

Do not agree with it being made commercially available. *A. Barrow—Any-Web Ltd.—Registry/Registrar/Domain Marketing.*

##### Source of registrant confusion

Whois data has a history of abuse, in particular by “bad actor” registrars/resellers, which has already resulted in massive confusion for registrants. Such confusion by 500 namespaces [and] registrars and I fear registrants will not know whois who! *J. Robinson—Registrar/Hoster.*

##### Support with comments

Easier to have an industry-wide standard. Will ease abuse of Whois and its accuracy. *R. Coghill, Group NBT PLC—Registrar.* Support Whois with cheap and easy access. *Interest not specified.* This is essential to ensure transparency and accountability in the system. *Large Corporation.* Please refer to our public comments. *C. Jamieson, MarkMonitor.* Agree to thick Whois; should be applied to all TLDs. *Interest not specified.* Definitely a good idea—essential. *N. W-S., Nominet—Registry.* Agree would be very useful for current gTLDs. *Large Corporation.*

Centralized Whois with ICANN (with information database maintained in the U.S. where less relevant issues as to privacy) is to be introduced. Ban or specified limitation on Whois privacy/shields to be considered. *Law Firm.* A must-have. *D. Krischenowski. .berlin—Registry.* It is a serious barrier and problem to brand owners tackling cybersquatting (particularly in obvious infringement cases) where it is not possible to identify the owner or registrant. *A. Mills, Experian Ltd.—Large Corporation.*

Support, but concerned that there is no creep into data compliance within the registry, and/or that accuracy or not of data is used to prejudice registration. *A. Barnett-Registrar.* Accurate data in one place is essential. *Small Business.*

### Private registration

Support, but what about whois privacy services? Private registration products are big business for registrars. *A. Bennett-Reseller*. Support but there must be means to protect privacy, allow use of proxy registration. *Interest not specified*. In support but what are the implications for proxy/privacy services? *Interest not specified*. Slightly concerned about the privacy aspects of who controls the data of the registrants. E.g., are the safeguards sufficient? Safeguards in jurisdictions outside EEA or U.S. safe harbor. *Interest not specified*.

### Opposition based on privacy concerns

Privacy concerns make me point to saying no thank you. These were not addressed satisfactorily in the IRT recommendations. Modifications to this section, to include exceptions or some kind of solution for those individual users wishing to maintain their privacy, might be enough for me to say “yes.” *O. Crepin-Leblond, Internet User*. How will thick Whois deal with data protection legislation in the EU, Canada and Australia? *Interest not specified*.

### Support, but opposition to proxy services

Work also needs to be done on proxy registrations. I am in agreement with the comment from the floor—if a proxy service is shielding an abusive registrant then they should be responsible too. By preference, proxy services should not be allowed. *S. Payne, BBC Worldwide—Large Corporation*. Thick Whois is definitely needed; no proxy registrations should be allowed. *Large Corporation*. Privacy settings implemented by some companies such as proxy domains should not be permitted. Nominet’s privacy is acceptable as long as address details are provided in case of dispute. *R. Bond, EMI Group—Large Corporation*.

### Resolve thick Whois issues before new gTLD implementation

A very long list of yet unresolved and undiscussed issues still lingers regarding the specifics of operation of Thick Whois. As Thick Whois is going to be a key tool, gTLD should not be implemented until these issues are fully resolved. *LEGO—Large Corporation*.

### Legacy thin registries

Universal Whois should be considered for the legacy thin registries. *W. Staub, CORE-- Registry-Registrar-Professional association interest*.

### Support for Proxy services.

Okay but we want to keep proxy registrations. *Domain marketing*.

## Expansion of String Comparison

### New York

### Transcript Summary

#### Expansion of tests for string comparison during initial evaluation

The IRT recommended that in the initial evaluation strings that are visually similar would be identified and that once whatever threshold that ICANN intends to use is met, then at that point similarity in sound and meaning would also be considered. IRT also recommended that all applications that would fail the string confusion portion of the initial evaluation be given a reconsideration opportunity, to make the process fairer. *K. Rosette*.

## Feedback Form Summary

### General Comments/Questions

#### Also define TLD

ICANN also needs to define what a “TLD” is. It must be the apex of “a well-defined human activity, community or sector”. One TLD should not be able to cannibalize another, e.g., after .NYC is awarded to allow “.Bronx” or “. Brooklyn” (2 New York City boroughs). *Small Business*.

#### Support with comments

Support, as modified by our filings on the record. P. Flaherty & M. McKeenan, Verizon—Large Corporation.

A robust string comparison process will help avoid some cybersquatting and malicious activities before they can start. D. Bernstein, Debevoise & Plimpton LLP—UDRP Panelist.

## London

### Transcript Summary

#### String comparison algorithm

The IRT has recommended that if the algorithm finds that there is visual similarity, then at that point in time you would look to other things like sound and meaning to weed out false positives with the algorithm. It would not only apply to things on the GPML but also to the other things in the Guidebook (existing gTLD strings, existing ccTLD strings). *J. Neuman*.

#### Evaluation of strings

The Guidebook makes clear that the algorithm is advisory to the people who are doing the actual string similarity comparison. *M. McFadden*. The IRT has recommended that in cases of failure on string confusion that there be a reconsideration process that looks at other things or allows an applicant that failed to go into more extended evaluation. **Male unidentified**.

## Feedback Form Summary

### General Comments/Questions

#### Support with comments

Support in principle for this to be part of the decision-making process. *Large Corporation*. Just seems sensible. *R. Coghill, Group NBT PLC –Registrar*.

Example: .tel should NOT block .hotel. *Registrar*. Needs review and monitoring. *Interest not specified*. Normal trademark evaluation is needed. *Large Corporation*.

Yes. Should be substantially augmented both in scope (also to be used on 2<sup>nd</sup> and 3<sup>rd</sup> level domains) and in algorithms used. At the very least the specifics should be put under public discussion and involvement to devise a workable set of methods. Next that the service should be in a process of ongoing improvement. Last, that the code should be open so that all parties can use and contribute. Would like to contribute. *LEGO—Large Corporation*.

Please refer to our public comments. *C. Jamieson, MarkMonitor*.

Should also cover conceptually similar TLDs, e.g., .auto, .car/.computer, .pcs. Should cover plurals, hyphens, translations, as trademarks do. *Interest not specified*.



Comparison of visual, conceptual and aural properties should be made; .car and .auto should not be allowed. *R. Bond, EMI Group—Large Corporation.*

Concern about practical implementation. The courts and trademark registries have enough difficulty identifying a “rule” and applying it consistently to issues of identity. However, string-based is just not enough and could end up with ridiculous conclusions--if we mean “conceptual similarity” by “commercial impression” we should say so clearly. *A. Mills, Experian Ltd.—Large Corporation.*

Confusing similarity must always be considered in the specific context. This means that the strings alone are insufficient for analysis; the use of the strings must be part of the considerations. *W. Staub, CORE--Registry-Registrar-Professional association interest.*

It will help get applications through quickly. *Domain marketing. Why not? Small Business.*

### **Use as advisory tool**

Again, as per comments with IP Clearinghouse, I think this should be advisory/warning, and that the risk is taken by the registrant whilst preserving the FCFS [first come, first served] model – in conjunction with any new gTLD specific space rules. *J. Robinson – Hoster. See this as an advisory tool only. Registrar.*

### **Undecided**

Unsure as to saying “yes” or “no”, prior to finding out how extensive these string comparisons will be. *O. Crepin-Leblond--Internet user.*

### **Opposition**

Only humans can be trusted to make a judgment on initial interest confusion. *A. Bennett –Reseller.*

## **WIPO-Related**

### **New York**

#### **Transcript Summary**

#### **Support**

Good input. *T. Blasey, ITT--Large Corporation. Good. J. LeMan, Lord, Abbett & Co.—Small Business.*

Verizon supports WIPO’s positions to the extent they are consistent with our filings on the record. *P. Flaherty & M. McKeenan, Verizon—Large Corporation.*

#### **WIPO caseload**

WIPO would be far more credible if they didn’t twist statistics. For instance, while WIPO’s caseload has gone up, it is at the expense of other resolution providers - in fact as a whole the caseload has gone down, and there is at least a reasonable case that WIPO’s increase is due to forum shopping. *Registry.*

### **London**

#### **Feedback Form Summary**

#### **General Comments/Questions**

#### **Clarity requested about WIPO proposals**

Which measures exactly does WIPO propose to put in place so that cybersquatting on new TLDs is prevented or at least limited? It is not recommended that registries monitor registrations for infringements as this would be too lengthy and time-consuming a process. What then is recommended?

*N. Leroy, CSC—Registrar.* ESM—does it cover typos? Why such a low burden on the registrant? Again the burden is put on the trademark owner. Good with suspension for a longer period of time. *Large Corporation.*

### Reconcile IRT and WIPO approaches

The differences between the WIPO approach and the IRT recommendations need to be reconciled. *Large Corporation.*

### Enforcement costs

Completely disagree with WIPO's comment that trademark enforcement and defense costs should be shared between trademark holders and other parties. *O. Crepin-Leblond, Internet User.* Disagree that registries and registrars should share the burden of protecting trademark owners in the IP Clearinghouse. *Interest not specified.*

### Cost sharing

I have not previously read the WIPO proposals and so am not across the detail, but they seem sensible. Particularly suggestion the costs should be shared also by registrars and registries. *S. Payne, BBC Worldwide—Large Corporation.*

I agree that financial burden of the IP Clearinghouse should be shared between brand owners, registrars and registries. *Nestle SA—Large Corporation.*

### Prefer all the IRT suggestions

WIPO are too biased in favor of trademark owners. IRT is fairer. *Domain marketing.* Prefer IRT to WIPO. *Small Business.*

### Support

Broadly in favor of WIPO's amendments.

*R. Bond, EMI Group—Large Corporation.* Good presentation. Good points. Reasonable set of conclusions. Apparently much further down the road to devise workable solutions than ICANN. Weird that ICANN did not engage into much closer joint work very early in the process. *Large Corporation.* Clear presentation. *Interest not specified.* Excellent and informative. *R. Bond, EMI Group—Large Corporation.* WIPO's comments are highly valuable and carry support of virtually every country in the world and so carry great weight. WIPO also has great experience and it would be mad to ignore their views in the light of that experience. *A. Mills, Experian Ltd.—Large Corporation.*

### Criticism; questions

Tamiflu was a bad example to use. *A. Bennett—Reseller.* WIPO seems to have done very little; they could be proposing revision of the UDRP. *R. Wickham, 2020Media—Registrar.* Tamiflu infringements in .com— is this systemic abuse by .com? *Law firm.*

### WIPO suspension mechanism

The suspension mechanism is an excellent proposal especially as to extent that it provides for a longer period in which the contested domain name stays frozen after the decision and provides for an easy way for respondent to avoid default cases, but in case of default better solution than the one of IRT is envisaged. *Law firm.*

## Demand Media Proposal

### New York Feedback

#### Support

I broadly agree. Interest not specified.

#### Criticism

Poorly conceived ideas, based on misleading and incomplete data. *T. Blasey, ITT--Large Corporation.*

#### Panel process

Why did ICANN put Demand Media on this program? This is tantamount to ICANN's endorsement of Demand Media! Why? *Small Business.* Excellent to hear from other non-ICANN experts. *J. LeMan, Lord, Abbett & Co.—Small Business.*

#### Partial support

Support IP Clearinghouse, Thick Whois, Pre-launch/sunrise and expand string analysis. Other points, to the extent they are consistent with our filing on the record, we strongly disagree with. *P. Flaherty & M. McKeehan, Verizon—Large Corporation.*

Able to oppose even 1, no minimum. *Interest not specified.*

## Malicious Conduct

### Sydney Feedback

#### e-Crime management

e-Crime is not a fully solvable problem, it's more a matter of management. Collaboration and data sharing and education are extremely important. There needs to be more global cooperation. Criminals migrate from TLD to TLD over time. We can assume that criminals will register names in new TLDs. Challenges to dealing with e-crime problems include legal ones —e.g., privacy laws, government regulation and controls; technical challenges; and costs. *G. Aaron.* We have to get beyond just looking at this in terms of trademark infringement because it goes beyond that. *B. Brendler.*

#### Marketplace role

While we talk about government regulation, in reality the marketplace can often dictate how bad behavior gets dealt with and registries/registrars respond to that because it is the market force pushing them. Some of this may be solved by technology and self-identifying about having high levels of security. *R. Rasmussen.* There seem to be good opportunities for market-based solutions with the new TLDs—e.g., creation of a set of good TLDs that have exceptionally high security practices, with 100% guaranteed Whois, and with consumers educated to take advantage of these opportunities. There could even be a dot anon and people and ISPs could make decisions how to interact with it or not, but at least it would be there for people to participate in meaningful speech. *J. Buchanan.* Consumer education is difficult to do and it will take some work. It will be hard to get consumers past the original mindset of dot gov, dot mil, dot edu. *B. Brendler.* Regarding R. Lowe inquiry if there is a business case for security done by registries, there have been encouraging results for the .info registry from the investment and effort it has put into security. *G. Aaron.*

#### Codes of conduct for new registries

It is important to have codes of conduct, "kits" that we can offer the new registries, showing elements to them of what they should do, rapid suspension being one of them. *A. Abril i Abril.*

### Recommended action by ICANN in new gTLD process

In the new gTLD process applicants should specifically state what they intend to do regarding abuse policies and handling (e.g., best practices should be followed). Applications that fail to include provisions for abuse handling or abuse policies should be referred to the extended evaluation process for a closer look. ICANN compliance staff needs to be ready for the new TLD round; they have a central role in responding to Whois complaints. They should be reviewing regularly all registrars' compliance with Whois, port 43 and web-based Whois, in accordance with existing policies. *G. Aaron.*

### Registry eligibility and security processes and levels; financial sector

In general, one of the first decisions is who is eligible to be a registry and issues to be considered include good standing, how we manage endorsements and objections, and whether we do background checks (criminal and financial). Potential requirements for high-risk or high-security domain names are levels of encryption and authentication, and certificate management. There might be browser certification; we might require not just DNSSEC but also specific requirements about key management within DNSSEC. Ultimately we have to decide on the right level of security in operating all of those registries. Financial sector domains probably need a higher level of security than you would set as a floor. These requirements could be put into the applicant guidebook and what is applicable generally and to certain categories could be differentiated within the guidebook. Setting the rules up front in the guidebook makes sense rather than looking at applications after the fact. Responding to P. Stahura inquiry, one possibility is to have a high bar technically in the DAG for high security domains in the DAG (e.g., dot good bank, dot security), or it could be that we decide collectively that that security applies across the domain space. *L. Williams.* We have to link the meaning of the words to the bar level—someone has to make a judgment, i.e., this one means something really secure so we have to have a high bar. *P. Stahura.* One option is not to carve out financial, but to try to establish a definition for high risk or high security (i.e., anything that claims to have or implies it has high security or is of higher risk). *L. Williams.*

### Range of threats and challenges

Threats include domains purchased for criminal activities with no proper validation and verification in place; bogus Whois data; unauthorized modification of the NS reports; domain squatting; and malicious DNS fast flux—the single flux which involves manipulating the error reports, and the double flux involving the manipulation of the NS reports. There are challenges related to the repetition of these activities—attacks on the same providers and use of the same services—as well as delays from bogus Whois situations and cross-border issues, where a domain quickly moves on to another I.P. address and the process for removal of the domain may be very time-consuming. Flagging for “bank” names may be helpful but not all banks have the term “bank” in the domain so many can be missed. For criminal cases the UDRP process is too long. *A. Othman.*

### Solution approaches

It is important to have some measurable mechanisms (security controls, policy or technology) in place and we need to ensure they are scalable (e.g., domain lockdown where alerts go out to registrants). It should be asked—is security integrated into the business process? We need to focus on preventive measures. When things go online to make an application go faster, are we lessening or losing on controls on security requirements? Audits for registrars' online application process should be employed. We also need to ask if voluntary best practices work and how to measure compliance, as well as the responsiveness of registrar, registries and implicated parties. The way forward includes ensuring that input validation is there, that recording the owner of the subdomain is actually done in practice, and having proactive scanning and detection. Responsive action would be to reduce the time taken for takedowns and flagging or acting upon a customer registering for malicious domains with further investigation to further weed out bad actors. *A. Othman.*

## Whois role

Whois is the issue to which we need to pay the most attention. Doing business in an atmosphere of complete anonymity leads to e-crime problems. *B. Brendler.*

## Registrar liability risks; false positive takedowns

In response to M. Rodenbaugh inquiry, there have been cases of risk of liability for false takedowns. *G. Aaron.* We should not be thinking of contracts as loose regarding end user registrants—i.e., the suggestion that registrants have no rights or immunize and indemnify everyone above them in the chain raises concern. *W. Seltzer.* Regarding the risk of liability to registries for false positive takedowns, why don't we agree that collectively the Anti-Phishing Working Group can find very cheap insurance for these cases to guarantee that registries and registrars can take these actions without needing legal expenses and doing research on legal regimes and costs, etc? *A. Abril i Abril.* It's up to business to have that insurance. If not required in the ICANN contract then it is a good best practice to have a general comprehensive liability policy that could cover you for that kind of rare risk. Also, a false positive is incredibly easy to fix--simply turn it back on and damage is cut off pretty quickly. *M. Rodenbaugh.* Perhaps a "safe harbor" approach could be developed for registrars. *Andrew K.* Responding to comments and inquiry by Andrew K. and Marilyn Cade, the issue of registrar responsiveness in cases where registrar action is needed can be challenging due to the different sizes and structures of registrars, some of which are very small and which don't pay attention. *G. Aaron.*

## Identity assurance mechanism

Is it time to require registries, registrars and possibly even registrants to have digital certificates with an independent high level of identity assurance behind them so you can stop some of the spoofing, substituted DNS records and other problems, and is that technically feasible? *P. Argy.* The financial/elevated domain space sector would likely support that. That could be considered for any elevated risk or elevated domain ranges, and it could be not just certificate issuance but management and monitoring of the certificates, and other kinds of authentication requirements, and could facilitate trading of secure email in and out of that domain. *L. Williams.*

## Multiple governments and differences

What about the issue of people concerned about malicious governments? Also, is it a problem that different governments have different goals and put pressures on you to comply with different rules for things like content? *D. Yee.* There is some evidence that state actors are behind some of the kinds of attacks we are seeing, which makes it far more difficult to deal with them. Different regulatory schemes and laws in various countries for mitigation of various content on the Internet present challenges. Some coalescing is occurring through the Council of Europe's Cybercrime Convention—this is providing good tools for law enforcement and others to normalize how they do things. *R. Rasmussen.*

## New York

### Transcript Summary

#### ICANN efforts to date

ICANN's efforts to date regarding the overarching issue of malicious conduct include working with many experts, including the anti-phishing working group. ICANN intends to leverage outside expertise rather than ICANN growing into a place where its staff become security specialists and have the ability to do audits and fine-grain security practice checking. There is also a constant theme in the comments that we need to standardize remediation approaches, to the extent possible. *G. Rattray.*

### **Banking and financial issues**

The term “security implicated new gTLDs” generally refers to banking and finance, recognizing however that there are other communities that have a requirement for higher levels of security given what they do (e.g., medical). *G. Rattray.*

### **Effective security practices**

Effective security practices in all new gTLD operations would include DNSSEC implementation and prohibiting wildcarding. There is also the need to remove “glue records” from expired domain names—this is an example of a good practice that will make the new gTLD domain space easier to secure. *G. Rattray.*

### **Responding to malicious conduct**

Ensuring the ability to react to malicious conduct is also being analyzed in the ongoing consultation – e.g., Whois requirements, enhanced compliance on the part of ICANN’s compliance team, consideration of registrar-level requirements, points of contact at the registrar level and other recommendations from the SSAC. There is also the inclusion, as a requirement for an applicant, of an anti-malicious conduct and anti-abuse approach so that as part of the evaluation there is an understanding of what new gTLDs are doing in terms of being able to deal with situations of abuse and malicious conduct. *G. Rattray.*

### **Background on the Anti-Phishing Working Group (APWG)**

APWG currently has more than 3,300 members, from 1,800 different companies, law enforcement agencies, government ministries and international treaty organizations. APWG tracks and reports on electronic crime events worldwide and feeds it back to industry. The most consumed data are the URL black lists given to toolbar developers, browser developers, and AV companies that use it to help inform the products and advise consumers about bad sites. It is also used primarily by security companies to chase bad sites and counterfeit sites. APWG members are also advisors to government treaty associations, law enforcement agencies, industry, governance groups and the press. APWG has a peer review electronic crime research conference every year done in partnership with the IEEE, and also does original research. *P. Cassidy.*

### **Registry control and ownership**

Registry control and ownership is a difficult area that will get worse and is very much an issue in the banking community. A criminal group could control a registry – e.g., banks, supermarkets regularly bought by criminals or put into control of criminals through arms-length associations. You have to be aware that you are being watched and the opportunities are being hunted for in this space. *P. Cassidy.*

### **Ownership of and access to registration data**

Ownership of and access to registration data is key for the responder community, including the extent to which data is dispersed and how that affects response times and the number of consumers who are actually exposed to fraud. *P. Cassidy.*

### **Impact of varying registrars’ anti-abuse policies and procedures**

Registrars’ policies and procedures against abuse are not all equal, and malevolent opportunists will always go after the weakest link. This raises concerns about whether the registrars with the weakest policies will chase out the best intentions of registrars that want to do the hard work of security in their spaces. *P. Cassidy.*

### Changes to registrant qualifications

Issues to be considered include: will a registrant qualification come with certain guarantees that could slow down response to an electronic crime event? Will the string give the attacker more opportunity by telling them more about either the company who owns that string or the customers of that string? Would the new TLDs' names actually create new kinds of attacks based on the TLD name itself, and is there something we should do about that before the name is registered? *P. Cassidy.*

### Scaling issues

For responders, when there are more TLDs and more registrars, responders get more data that must be consulted and that slows down the response time and imposes costs on third parties if they have to organize a contract for access to the zone file. There seems to be positive progress on some issues like DNSSEC. Prevalence of fraudulent registrations will go up with the number of new TLDs. Issues like Malicious Fast Flux and other DNS attacks are threats, especially with new TLDs. *P. Cassidy.*

### APWG project--standards for domain suspension

APWG is working on a project to codify what is done all too casually in this area. The project is basically a security channel communications system that will allow signed affidavits to go from various accredited intervenors (e.g., brand holder security teams and security companies) to make secure communications to registries to accelerate suspension of abusive domains that are probably only used for criminal enterprise. *P. Cassidy.*

### Registry Internet Safety Group—background

The group is about 1 ½ years old and was formed by registries to facilitate data exchange and create best practices for dealing with e-crime like phishing and malware distribution. It includes both ccTLD and gTLD registry operators, security vendors, registrars and observers from national law enforcement bodies around the world. *G. Aaron.*

### Criminal activity on the Internet—trends and impact of more TLDs

We cannot necessarily say there will be more or less crime if there are more TLDs, but the location of where that crime is occurring in the DNS may change because criminals tend to migrate in their use of TLDs and registrars. Vulnerable web servers are how criminals conduct most of their business—they break into those machines and rope them into bot nets and that is how most phishing takes place. *G. Aaron.*

### Challenges in responding to e-crime

When responding to e-crime, registries and registrars can have legal issues to deal with – e.g., EU privacy laws that may bar the sharing of Whois information to the same extent that it is shared elsewhere. Government regulations and control are important (e.g., some ccTLDs are controlled by governments and many of them have direct obligations imposed by their governments). The issue of website suspensions for bad activity also presents risks; there is the need to exercise care so that an innocent party's website or email is not shut down accidentally. Verification and identification of criminal behavior are key issues and can be difficult. Technical challenges to getting good data to rely upon, examine and trade also exist. Registries and registrars have to budget for the costs of this mitigation work. *G. Aaron.*

### Cooperation in mitigating problems using the DNS

Cooperation is already global (e.g., ShadowServer, APWG) and we need to see more of that. Threats to the DNS at the top level are where ICANN has its obligation; ICANN cannot be and is not responsible for everything that happens on the Internet. *G. Aaron.*

## Recommendations for ICANN in the new TLD process

First, in the new TLD application evaluation process, ICANN should look to see if potential registry operators are stating in their applications if they will have abuse policies and procedures. Awareness of the operators is half the battle. If applicants do not have anything in their applications, then ICANN should put them into the extended evaluation process for a closer look. Second, ICANN should continue to think about its compliance methods and how that works with more TLDs. Registries and registrars need to be very careful about providing their Whois within contracts and ensuring that the information is available to responders. *G. Aaron.*

## Examples of gTLDs with intrinsic potential for abuse

gTLDs with intrinsic potential for abuse include financial, medical and critical infrastructure industries (the U.S. has a list of 18 critical infrastructure industries). **[Male unidentified in transcript]** Response to *chat room* query.

### Financial gTLDs

A cooperative global effort among financial and banking entities led by BITS has been underway, working to ensure that financial gTLDs are as secure as would be expected if they were being operated within bricks and mortar institutions—i.e., meeting all the expectations that customers have about how strong a bank or an insurer is, and the expectations of regulators. This group intends to provide to ICANN staff ideas regarding what would be required for the responsible launch of a financial TLD (fTLD). The fTLDs will be targets for e-crime and abuse. The group of TLDs with elevated security requirements could be fTLDs or just highly secure (“security implicated domains”). The ICANN community as a whole will ultimately decide whether fTLDs are treated slightly differently or if instead the high-risk or highly secure TLDs have this separate category. It is important to sort out what entities should be participating in the process regarding fTLDs, what the roles are, and how to handle enforcement. The financial industry would like to have clear rules in place about what is required to be “highly secure” before applications start flowing in and are adjudicated. This approach could be cheaper and simpler than dealing with problems after the fact. *L. Williams.* While having high security will depend on action of the registries and registrars, the predicate for high security can be laid by up-front requirements at the application level that only the registry operators who are prepared to take on that responsibility will be the ones running financial gTLDs. **[Male unidentified in transcript]** Response to *chat room* query.

### Financial gTLDs—proposed processes

The financial industry is working to develop ways to plug specific requirements and policies into the existing proposed process for new gTLDs. These ideas are on the table and in flux and community input on them is welcomed (PowerPoint addressing parts of this area is to be posted on the wiki):

- (1) **Application “first cut” opt-in stage:** regarding applications, one proposal is for applicants to “self identify” as being fTLDs, or that they identify that they intend to be highly secure and are willing to satisfy whatever the elevated requirements are;
- (2) **Evaluation stage:** ICANN might, with or without the contribution of the financial sector, establish an IT security standard that would be applied in the initial evaluation process, and the process would have to ensure that anyone needing to operate at a higher level of security actually has an audit in place that they provide those high levels of security and meet measureable requirements;
- (3) **Objection and dispute resolution stage:** ICANN might do less here and the community, industry, regulators and civil society might weigh in on the issues of the right participants applying for applications, with a registration process involving the right registrars, etc. It might turn out that a form of validated registration process makes sense for other industries or groups as well;



- (4) **Pre and post delegation testing and monitoring stage:** Once people have contracts in place and have this delegation, they must satisfy their promises; it may be a bit more than contract compliance (e.g., a combination of activity by ICANN, industry and auditors and registries to ensure that obligations are satisfied). *L. Williams*.

#### Impact of new TLDs on perception of financial security

It is time to sharpen up security, and there is a responsibility to do that in the context of the new TLD process if it can be done in a way that is better than .com or other existing TLDs. There is also a high likelihood that people will have higher security expectations about a TLD such as .bank or .vault than they do about .com. *L. Williams* responding to *A. Van Covering* query.

#### APWG rapid takedown proposal

The IRT and APWG rapid takedown proposals are different and have different purposes. The phishing proposal is to deal with a subset of domain names used for phishing. In that process time is of the essence. By contrast the IRT is basically going through an arbitration-type process, more a judgment call about whether the domain is owned by a bad actor and what to do after that. *G. Aaron* responding to *D. Younger* query. APWG is working on a standard and reasonable takedown notice process. **[Male unidentified in transcript]** Response to *chat room* query.

#### Rapid updates/rapid mods

The APWG hasn't yet commented on and discussed the issues of whether rapid updates/rapid Mods should be mandatory in the new gTLD applicants and how criminals take advantage of rapid updates in certain ways. *G. Aaron* responding to *E. Brunner-Williams* query.

#### Financial gTLDs—global approach

It is not the objective of the financial community to create two regimes developing a .bank – one U.S. centered and the other European centered-- but rather the set of rules that are appropriate for, and developed and managed by, the global financial services community. It would not serve anyone's needs if it turned out to be a U.S. based or U.S. centric effort. *L. Williams* responding to *E. Brunner-Williams*.

#### Financial gTLDs—enhancing security if institution is also the ISP (upstream control of transmission pipe)

Every institution is getting more involved in how communications are provided. The financial industry engages the communications industry and individual institutions engage ISPs. Whether they would actually trade equity is a little beyond scope here. *G. Aaron* responding to *P. Fudey* query.

#### Financial gTLDs standards—effect on existing .com financial sites

If a good precedent is set on standards for new financial gTLDs, then the hope is that the precedent would spread back to .com and other existing domains, in an operationally reasonable and politically reasonable way. It might not happen instantly, but if there are some good practices developed, they should be employed very broadly. Seal programs may also help create consumer demand for a higher level of security. *L. Williams et al.* responding to *P. Corwin*.

#### Timing of specific malicious conduct recommendations

It is fair to say that the process for dealing with the overarching issue of malicious conduct is at a more preliminary stage with respect to specific recommendations than the IRT process for the overarching issue of trademark protection, but the goal is to get specific recommendations out on malicious conduct issues in the near term. **[Male unidentified in transcript]** Response to *M. Bohannon*. It is unclear that specific recommendations will be released before the next ICANN meeting in Korea. **[Male unidentified in transcript]** Response to *chat room* query.

### Use of public communities for security solutions

Security companies and some registries and registrars are taking advantage of community resources to come up with security solutions (e.g., stopbadware.org), but it is unclear that there are discussions about incorporating those resources in a formal way. The notion of a “seal” made known to consumers that a certain operation has met a set of security standards has been part of the discussion. **[Male unidentified in transcript]** Response to *J. MacFie*.

### Whether to have .XXX site

The broader issues about the appropriateness of .XXX are outside the scope here. *G. Rattray* responding to *P. Fudey* query.

### ICANN responsibility for Internet safety

The Internet is not a fit place to attract young people, older people, people that aren’t that net savvy. ICANN exists to make the Internet the safest place it can possibly be and it is falling very short on that responsibility. *P. Fudey*.

### Fostering information exchange about malicious conduct is vital

While ICANN is not ultimately responsible for all things that go bad on the Internet, it is vital that ICANN fulfill its role regarding the malicious and abusive use of the DNS and the unique identifiers. The information exchange that is beginning to come out of ICANN to the community about issues and implications of malicious conduct is very important. *M. Cade*. Progress has been made on information sharing but input and suggestions from the community would be welcome about additional things ICANN could do to raise awareness. *G. Rattray* responding to *M. Cade*.

### Up-front safeguards against exploitation opportunities with new TLDs

With more TLDs there will be more exploitation opportunities, making it critical to have safeguards built from the start instead of trying to retrofit them or add them after the fact. *M. Cade*. ICANN is in the building it in (rather than bolting it on) stage regarding preventive measures to lock out bad actors through rules that kick in before applications ever show up. *G. Rattray et al.* responding to *M. Cade*.

### Timing of new gTLD rollout and impact on minimizing malicious behavior

The issue of timing for new gTLDs is a matter that is in the mix in terms of recommendations to ICANN about how to minimize the potential for malicious behavior (i.e., don’t open up the process until the whole process is ready, don’t accept an application until the applicant has shown they are ready by whatever criteria is ultimately decided upon). *G. Aaron et al.* responding to *S. Metalitz* query.

### Next steps

Implementation recommendations on malicious conduct will probably be inserted in the next version of the Applicant Guidebook and feedback will be taken through that process. *K. Pritz et al.* responding to *K. Rosette* query.

## London

### Transcript Summary

#### Status and background

ICANN has been working with a number of groups, including the Anti-Phishing Working Group (APWG), and major banking and financial groups, among others. A final report is expected from the APWG. There is some overlap between the issues of malicious conduct and trademark protection. Malicious conduct generally refers to when criminal activity occurs – e.g., phishing to conduct financial fraud, identity theft,

the spread of malware and establishment of botnets. ICANN has received extensive comment on this issue and is continuing to receive input. The ICANN Security and Stability Advisory Committee has issued reports and recommendations in this area, which are being considered to the extent that they are applicable to new gTLDs. In Sydney the Board passed a resolution that ICANN will not allow new gTLDs to conduct DNS redirection in synthesized responses. A number of effective practices might be required of all new gTLDs' operations – e.g., the strong effort in the DNS community to get DNSSEC signed at the root and implemented at all levels of the DNS, prohibiting wildcarding. Another effective practice is removal of glue records, one of the records in your domain file, for expired domains so that hackers cannot take advantage of that in order to redirect DNS resolution. Whois requirements are important for ensuring the ability to react when malicious conduct occurs. Implementation recommendations will be part of Version 3 of the guidebook as well as an explanatory memorandum. *G. Rattray.*

### **New gTLD registries—qualifications and protections**

The process will require a high degree of vetting, not only at the outset but continually after that, especially where there will be TLDs that have a meaning of security and confidence to customers (.bank). It is important that new and appropriate policies are set up front against abuse. Vulnerabilities need to be considered also. Scaling up is a big concern. There is a need for consistency and easy access to the right contact information when there is an incident (e.g., Whois). It would be good to have standards adopted by new and existing registries so that we have straightforward and consistent mechanisms for fast and effective takedown activities. Awareness is also needed regarding bad actors that either own registries or are linked into those registries and are able to acquire many domain names themselves. A lot of work can be done on preventing fraud. *M. Sutton.*

### **Anti-abuse programs**

NeuStar, operator of .biz and .us, started an anti-abuse program to deal with abuses that were going on in .biz (pharming, phishing and other malicious activity). NeuStar investigates complaints and verifies them, and sends a report to the sponsoring registrar and gives the registrar 12 hours to take down the name. If there is no response, then NeuStar takes the name out of the zone. About 95% of the registrars take the names down on their own after NeuStar notifies them. More than 100,000 names have been taken down at .biz with no complaints. NeuStar also participates in security forums and integrates law enforcement into its processes. NeuStar is a founding member of the Registry Internet Safety Group. Registries cannot solve all problems alone—collaboration is needed with other organizations. *J. Neuman.* As a public company NeuStar does not report on the type of financial cost accounting such as the percentage of overhead spent on investigation, reporting and takedown. Not every registry can do this in-house and it may be more economical and efficient for some to outsource it. *J. Neuman* responding to *chat room* query. The impact of costs put on registrars in the compliance process needs to be factored in so that there is balance in the mechanism. *P. Keating.*

### **Anti-abuse policy recommendations for registries**

Applications that fail to mention anti-abuse policies that are based on current best practices defined by industry leaders should be referred to an extended evaluation. New registries once approved should codify their anti-abuse policies in their registry and registrar agreements and require that such policies be passed through to registrants. These restrictions need to be enforceable through contracts. Registries or their backend operators should join industry groups like the RASG and APWG. They should have a process to receive complaints, including those about malicious abuses. Registries, backend providers or their outsource partners should publicize that information on their website and have ways such as email for registrants and users to contact them, and attempt to verify complaints (e.g., either independently or with the help of an accredited third party). Registries should take action against domain names that are objectively proven to be involved in domain name abuse, and subject to legal restrictions should

share data with other registries, ICANN and other industry players that may be impacted by such abuse, and seek out law enforcement agencies for collaboration. *J. Neuman.*

### Anti-abuse tools for registries

Registries can provide a lock on domains used for phishing which immediately removes the domain from the zone file and prevents a move to a different registrar or its deletion and re-registration. Many of the issues can usually be dealt with at the registrar level. The sanction for breaches of contract (e.g., registering a name for illegal uses) is to cancel the registration. For new gTLD registries, it will be important to be prepared to react to instances of abuse, and to have good relationships with law enforcement and registrars. Registrars are usually in a good position to address the problem with the people who have registered and abused the domains and it is in everyone's interest to get quick resolution of problems. If things can be addressed in minutes, then people won't end up visiting those sites and they don't get incorporated into the DNS or cached in local ISPs. It is important to be vigilant and to educate the communities you deal with as a registry. The key to long-term success is a very competitive environment where registries live and die by their reputations. Prevention is better than a cure. It is not an option to not do these things. *N.W. Smith.* There is a lot of up-front work that can be done by registries – such as verifying postal addresses for legitimacy, and preventing people from putting bogus data into Whois. **Male unidentified.**

### ICANN compliance process

Would it make sense to have a more visible internal process for compliance as ICANN is developing agreements –i.e., for each paragraph, how is ICANN going to ensure that the contracting parties do what they have promised and ensure that there are reasonable sanctions. For example, one of the main problems with the Registrar Agreement was that the only sanction was to “kill” them, which was excessive for a lot of the peccadilloes. **Male unidentified.**

### Malicious Conduct Panel Feedback

**Do you think the panel adequately addressed the potential range of concerns in this area? What is your opinion on what concerns are highest priority?**

*New York:* They've done a good job with known threats. What scares us are new, emerging threats. *P. Flaherty & M. McKeenan, Verizon—Large Corporation.*

*London:* Yes. *A. Barrow, Any-Web Ltd.--Registrar.*

Further thinking on how to set in place the required panels, so that the implementation timeframe isn't jeopardized further. *Large Corporation.*

Yes. Phishing. *Large Corporation.*

There is not enough talk on people using stolen credit card information to register domains. This is where nearly all fraud starts yet nobody is interested! Invest in chasing and catching these people! *Registrar.*

No. *EURODNS-Registrar.*

No, it was just a brief “run through” of headlines. But main message that there are indeed non-addressed concerns was of great interest. Please release further in-depth information through the website. *Large Corporation.*

What was the point of the sales pitch from Neustar? Not relevant to this panel session. We want to hear what ICANN will do to minimize the malicious conduct, not what Neustar does or does not. *Large Corporation.*

Yes. *A. Bennett-Reseller.*

The outline of economic impact was appalling! The ICANN guy was a joke! *Interest not specified.*

Not adequate. More examples needed. Nominet good. *Small business.*

No, they overlapped. *Domain marketing.*

**Do you think the panel adequately addressed the potential range of remediation approaches in this area? What is your opinion on what concerns are highest priority?**

*New York:* IPv6 and DNSSEC are lower priority for U.S. companies. *P. Flaherty & M. McKeegan, Verizon—Large Corporation.*

*London:* Yes. *A. Barrow, Any-Web Ltd.--Registrar.*

Approaches were not covered in detail, but this did not reduce the overall value of the session. *Large Corporation*

No—how do you stop the same third party repeatedly targeting your company? *Large Corporation.*

Nothing should be a higher priority than actually catching and prosecuting (and thus scaring others away) pranksters using stolen card information. *Registrar.*

Every registry should have as good measures as Nominet or Neustar have. *Nestle SA—Large Corporation.*

Typosquatting. *EURODNS—Registrar.*

No, but there were some good recommendations, but oddly of which very few (almost none) has found its way into the Guidebook. *Large Corporation.*

There was no real presentation of the work done within ICANN so it's impossible to answer these questions. *Large Corporation.*

Yes. *A. Bennett-Reseller.*

Rapid takedown most important. *Small business.*

Spam not mentioned. Rapid takedown important. *Domain marketing.*

**Do you think the ICANN approach to understanding community concerns in this area is adequate? What other concerns do you believe should be considered?**

*New York:* Vigilance, eternal vigilance. This area is just as important to Verizon as the trademark issue. *P. Flaherty & M. McKeegan, Verizon—Large Corporation.*

*London:* Yes. *A. Barrow, Any-Web Ltd.--Registrar.*

Yes, adequate enough for the ICANN Board to make a decision on the way forward. Further delay is unacceptable. *Large Corporation.*

Not sure. *Large Corporation.*

ICANN should impose the same conditions to all registries and make sure all of them comply. *Nestle SA—Large Corporation.*

Yes, usually. *EUROWWS—Registrar.*

No, not adequate: too sporadic, too little dialog, substantial concerns played down. ICANN refusal of policing the contract to come (in contrast to a normal contract management) strikes as being a mechanism for harvest benefit, not concerns for problems. *Large Corporation.*

Yes. *A. Bennett-Reseller.*

No, especially regarding .com. *Interest not specified.*

Yes, but also use of domains in spam. *Small business.*

Spam. *Domain marketing.*

**Do you think ICANN is considering an appropriate set of remediation approaches in this area? Do you have other suggestions?**

*New York:* International Law Enforcement cooperation and education is key to success.

*London:* Yes. *A. Barrow, Any-Web Ltd.--Registrar.*

Yes, proposals and approach have facilitated adequate consultation. *Large Corporation.*

Will any registries ever have to check for IP infringement by sites, i.e., a P2P file sharing platform site. Or is this resource dependent? *Abuse Issues.*

Three strikes you are out for repeat offenders. *Large Corporation.*

Set up a group for all registries/registrar/affected groups to pool information on fraudulent users. Invest in catching them. *Registrar.*

No. In the presentation done so far none has been mentioned, just outlined as areas to look further into. [comments missing—continued on reverse side of form] *Large Corporation.*

Yes. *A. Bennett-Reseller.*

No. More protection for the consumer. *Interest not specified.*

From past experience I'm aware that ISPs/registrar/hosters have routinely blocked the IP address range for entire countries. Whilst this has been an operational necessity, it should be acknowledged by ICANN/IGF that this is not in the broader interests of affected countries, i.e., "a few bad apples." *J. Robinson.*

## ROOT SCALING STUDY

### New York

#### Transcript Summary

##### Scope of the study and status

The ICANN Board requested that the Security Stability Advisory Committee and the Root Server System Advisory Committee conduct a study which goes under the label of Root Scaling. It explicitly covers both the implications of increased numbers of names at the root level as well as the potential for a number of other complexities to be added at the same time, such as implementation of DNSSEC, IDNs, new address records and “glue” in IPv6. Some of these things are going to happen at the same time so it is crucial to study their intersection in addition to simply the number of names that might be added. A study team lead by Liman Chapin [**check name spelling**] has been formed. A draft report from the study group to the two committees is expected at the end of August, and those committees will issue findings to the Board that will inform our moving forward on the new gTLD process. Rather than a focus on at what point specifically a number of new gTLDs will cause a fracture in the root zone, the Liman Chapin approach will be to have a model-based analysis about what sorts of issues are likely to pose stresses and to be able to understand when we will be able to see stress points coming and how to deal with them once they are identified. The study is looking at issues around provisioning and publishing the root zone. *G. Rattray.*

##### Engagement with ISPs and other key affected entities

It should be ensured that the root scaling study team engages in a timely way with all the key affected entities—such as the infrastructure providers who run the Internet. *G. Rattray* responding to *M. Cade.*

##### Next steps

The root scaling study will not be recommended to the Board by SSAC and RSAC until after the next version of the planned timeframe for the Applicant Guidebook—it will be a separate process. It is assumed it will be made public as soon as the Board receives it from the committees and hopefully it will have pointed recommendations about anything that would need to be done to the handbook or any other process so that the Board can consider those as they move toward the next ICANN meeting in Seoul. *G. Rattray* responding to *K. Rosette.*

### London

#### Transcript Summary

##### Scope of the study and status

The ICANN Board requested that the Security Stability Advisory Committee and the Root Server System Advisory Committee conduct a study which goes under the label of Root Scaling. It explicitly covers both the implications of increased numbers of names at the root level and as well as the potential for a number of other complexities to be added at the same time, such as implementation of DNSSEC, IDNs, new address records and “glue” in IPv6. Some of these things are going to happen at the same time so it is crucial to study their intersection in addition to simply the number of names that might be added. A study team lead by Liman Chapin has been formed. A draft report from the study group to the two committees is expected at the end of August, and those committees will issue findings to the Board that will inform our moving forward on the new gTLD process. Rather than a focus on at what point specifically a number of new gTLDs will cause a fracture in the root zone, the Liman approach will be to have a model-based analysis about what sorts of issues are likely to pose stresses and to be able to understand when we will be able to see stress points coming and how to deal with them once they are

identified. The study is looking at issues around provisioning and publishing the root zone. The RSSAC and SSAC will make their findings and recommendations in September, with those being dealt with as part of the process of bringing the overall new gTLD project to the Board at the Seoul meeting. *G. Rattray*.

### Public outreach communications plan and next steps

Given the possibility that a lot of unintended consequences will be discovered as a result of the root zone scaling study that may apply beyond the root zone and affect large scale operators, enterprise scale DNS, tier one ISPs, etc., it is recommended that the study report have a communications plan wrapped around it so that the technical community has visibility of the report. It is not good enough to have the report go back to RSSAC and SSAC. The impact of the report and studies that ICANN may commission afterwards has to go to the DNS operations committee. *M. McFadden*. It is assumed that the model used in the study will be published. *G. Rattray* responding to *J. Levine*.

### Methodology for studies

The study is going to build a model and will look at the ability of each element of the system to be able to handle increases in numbers and will also be considering if IPv6, DNSSEC, and IDN pose issues. Terms of reference have been published. *G. Rattray* responding to *chat room* query.

## ECONOMIC STUDIES

### New York

#### Transcript Summary

##### Scope of studies and status

The economic reports from Dennis Carlton focus on three things: (1) potential costs associated with TLDs and that they should be mitigated; (2) potential benefits of introducing new TLDs; and (3) price caps and whether there should be price controls in new TLDs. The report discusses mitigation of the potential costs of new TLDs to stakeholders (e.g., users, trademark holders, registrants, etc.) and the anticipated benefits of new TLDs (e.g., lower prices, competition, innovation, increases in participation through community-based TLDs and IDNs, and enhanced protection for brand holders). The report also concludes that price caps are not necessary and may inhibit marketplace development and innovation; that trademark holders can be protected by additional mechanisms; and that TLDs that attempt to act opportunistically will be punished by the marketplace. *K. Pritz*.

##### Cost-benefit analysis

A cost-benefit analysis about new TLDs is somewhat speculative but continues to be discussed. A metric must be established for this purpose, and ongoing economic analysis to measure the impact of new TLDs is required. *K. Pritz*.

##### Next steps

The immediate next steps will be to continue mitigation of costs in the new TLD program. This will include completing the New York and London consultations, making proposed changes to the Guidebook which will be put out for public comment, completing the root zone scaling study and holding additional discussions about the economic studies and the effect of introduction of new TLDs in the marketplace. *K. Pritz*. Given the comments of some participants (*M. Cade*, *S. Metalitz* and *M. Bohannon*) there will be some discussion on how to move forward on the issue of economic studies, what *Mark Bohannon's* version of an economic study would look like in order to have understanding of that and do some comparison. *K. Pritz* responding to *K. Rosette* query.



### **Expert discussion on economic analysis**

ICANN would support a discussion among experts – not just academic economists but also domain name marketplace experts regarding economic analysis (e.g., how to approach the scope and pace of the new gTLD rollout in order to maximize the benefits while minimizing the costs). *K. Pritz* responding to *S. Metalitz* query.

### **Scope of the Carlton economic study**

The current economic study by Carlton answers many but not all of the questions posed by the Board in 2006. One of the results of the economic study was that all those questions didn't have to be answered in order to launch new gTLDs. However, the Board certainly requested that study and so all those questions should be completely answered. That study was about the existing gTLD marketplace, not new gTLDs, so having said all of that, those questions certainly need to be answered and they will be. *K. Pritz*.

### **Carlton economic study is unresponsive to concerns raised**

The Carlton economic study is not meeting the expectations of the community, which has been made clear in the comments. The responses in the second version are not responsive to the questions that were raised. A robust dialog would be welcome, so that we can come to a better understanding of why it is so important for ICANN to understand the environment that it is trying to govern. *M. Cade*.

### **Registry/Registrar Separation**

Registry and registrar separation is also an important issue which the Board has asked the staff to hold consultations about. Study of that issue will go forward and those consultations will be set up. *G. Ratray* responding to *J. Neuman*.

### **Price controls**

There will not be fixed prices within a TLD. The way the current proposed registry agreement is written now, there are no price controls in the agreement. *K. Pritz* responding to *chat room* query.

### **Protecting existing gTLD registrants from large, unexpected price increases**

If there are price controls in an existing gTLD, they will remain. If it's a new gTLD the conclusion of the study was that acting opportunistically would harm the business model of the new gTLD and new gTLDs would be dissuaded from doing that for their own protection, and that in fact while switching costs still exist, they will be reduced with the introduction of new gTLDs. *K. Pritz* responding to *chat room* query.

### **Whether to limit the number of new gTLDs**

The GNSO discussed this issue at great length and recognized that it is difficult to limit them in a way that is fair and not gameable. The fair way to implement the process is to leave it open, following the GNSO policy recommendation and our best implementation advice. *K. Pritz* responding to *chat room query*.

### **Economic value of adding IDNs**

An alternative way to ask what is the economic value of adding IDNs is to ask what is the cash value of RFC2826, the IAD advice on the global, unique, DNS root. *E. Brunner-Williams*.

## London

### Transcript Summary

#### Status of economic studies and summary of key points

The final Carlton report focused on three things—the potential costs or downside associated with introduction of new TLDs and what should be done in mitigation; the benefits associated with introduction of new TLDs; and a discussion about whether price controls should be part of the introduction of new TLDs. The report strongly recommends that additional rights mechanisms be included, and that we remove artificial restrictions on the marketplace as 21 gTLDs is probably not the optimal number. The report stated that price controls were not necessary; that trademark protection could be accomplished through protection mechanisms, and that TLDs acting opportunistically, that charge high prices in a marketplace with many TLDs, would be punished for it and constrained in their actions by the marketplace. With more TLDs come lower switching costs that would enhance the effects of the market to constrain TLD behavior to be non-opportunistic. The report found that if ICANN were to impose price caps then this could inhibit some forms of innovation. **Male unidentified.**

#### Next steps

The best way forward is that suggestions based on the input from all the various sources will be put into the Guidebook, which is itself a proposal for discussion. **Male unidentified.**

#### Cost-benefit measurement

Attempting to measure the benefit accruing from new TLDs and attaching a value is difficult. Input on how to do that cost-benefit analysis would be appreciated. It is important that metrics are established to measure the performance of new TLDs, the effectiveness of rights protection mechanisms and either the increase or decrease in malicious conduct that occurs in this process. **Male unidentified.** There is an inherent unpredictability regarding what entrepreneurs and the market will create—it is very hard to quantify it. *R. Tindal.* We should let the marketplace decide whether the TLDs work or not. *P. Keating.*

#### Background on the economic study requested by the Board

Regarding the Board resolution asking for the economic study, there was not a demand aspect to it; it was really an analysis of the gTLD marketplace at that time, whether gTLDs were substitutable, what the switching costs and the market aspects were. As the new gTLD process gained momentum, the expectation in the minds of many participants in the ICANN community grew as to what the aspects of that study were—that it was also a study to ascertain demand at the top level and second level. The study to date has said that further assessment of that would be very speculative with a large margin of error. We don't need to cut off the discussion of what should be studied about the market, and we should talk about where ICANN should invest and where that investment can really pay off. *N. Wood* responding to *E. Shankman.*

#### Phased implementation of TLDs

Discussion of the scope of introducing new TLDs is still open and ongoing (e.g., there has been a proposal to fast track certain TLDs that committed to meeting all technical, security and trademark protection requirements). The GNSO discussions addressed the issue and the value that community-based TLDs bring to the environment and whether introduction should be limited to community TLDs, and decided that introduction of new TLDs should be more open. We should, however, continue the discussion of proposals and ways that could constrain the rollout of new TLDs. *N. Wood* responding to *E. Shankman.*

### **Registry/Registrar separation**

Further discussions are needed on the issue of cross ownership of registries and registrars—this issue directly affects consumers. Continuing the status quo won't work in the market as it exists today. *D. Maher.*

### **Consultation with U.S. government**

ICANN will collaborate in some way with the U.S. Department of Commerce on the launch of the new TLDs; ICANN is in communication with them. *N. Wood* responding to *S. Payne*. The question of how antitrust considerations are addressed is best directed to the U.S. Department of Justice. *K. Pritz* responding to *chat room* query.

### **Switching costs**

The economic study did take into account switching costs but there are aspects to switching costs and how we rely on the DNS that have not been fully explored. *K. Pritz* responding to *chat room* query.

### **Unified roots**

The reason we need new TLDs is as a way to defend unified roots. If the domain name space does not evolve, then people will go somewhere else and that would be much more difficult to police. *L. Stout.*

### **Economic study**

ICANN should study, understand and communicate the economic impact of gTLDs on consumers, companies and contracted parties before allowing expansion of the name space. *C. Jamieson.*