|  |  |
| --- | --- |
| **GAC Advice** | **Response/Discussion** |
| **All Strings - General Overview**  The GAC has advised ICANN to require all new gTLDs would require new gTLD registry operators to include specific terms and conditions in the registry-registrar agreement related to WHOIS accuracy and end-user conduct. Traditionally, these obligations have been contained in the Registrar Accreditation Agreement between ICANN and its accredited registrars. Presumably, the GAC would like to see greater registrar accountability, and is seeking to expand ICANN’s compliance resources by “deputizing” registry operators. Some niche and community-oriented applicants have proposed this kind of authority over registrar and end-user conduct. Other applicants, particularly those in the more generic space, have not. | **Changing the Registry-Registrar Relationship**. Whether one considers the GAC’s generally applicable advice to be “new policy” or merely “implementation” of existing policy, its adoption would fundamentally alter the relationship between registries and registrars in the ICANN structure, particularly with respect to truly “generic” TLDs. In 1999, in order to facilitate the creation of a competitive market for registrar services and to lessen ICANN’s dependence on the largest registries, ICANN expressly rejected a registrar-as-registry’s-sales-rep model and affirmatively placed itself between registries and registrars. Whether or not this was the GAC’s intent, significant elements of the Advice would reverse that structure by making registries directly responsible for enforcing registrar compliance with ICANN policy.  This would have important consequences that require careful consideration. If registry operators are expected to enforce ICANN policies – and even national law – across their distribution channel – and to be accountable for registrar conduct, then registries will require much greater authority and autonomy with respect to managing that channel. While some niche and community-oriented applications do contemplate greater registry control of domain name registration, applications for more generic TLDs generally do not. In cases where registry operators intend to play a more hands-on role, the applicants intend to operate in an environment that will facilitate this level of involvement, and they have had the opportunity to structure their business model accordingly. For others, this change is likely to have significant policy and business implications. Any such fundamental change in the relationship between contracted parties requires thorough consideration by those with appropriate business and legal expertise to evaluate all of the costs and benefits of any such change.  **Use of Objection Process to Create New, Conflicting, Changed Policy and Impose Unanticipated Costs**. The New gTLD Policy, developed by the ICANN community in a bottom up process over several years, was significantly shaped by GAC input – which included more than twenty (20) separate written documents beginning with the GAC Principles for New gTLDs in March of 2007. As the various “scorecards” and documents reflect, the community and Board worked extremely hard to accommodate GAC requests, suggestions, and recommendations throughout this process. It is most unfortunate that the GAC has used the opportunity provided by the New gTLD Policy to object to *specific strings* to call for material, *across the board* policy changes that: (a) been previously considered and rejected; (b) never previously contemplated; or (c) in some cases, internally inconsistent and irreconcilable. The introduction of material changes in registry requirements at this point in the New gTLD program is inconsistent with the New gTLD Policy itself, inconsistent with the GAC’s Operating Principles, which call for the provision of findings and recommendations in a timely manner, and fundamentally unfair to applicants who reasonably relied on the New gTLD Policy as described in the Applicant Guidebook. |
| **All Strings - WHOIS verification and checks**  Registry operators will conduct checks on a statistically significant basis to identify registrations in its gTLD with deliberately false, inaccurate or incomplete WHOIS data at least twice a year. Registry operators will weight the sample towards registrars with the highest percentages of deliberately false, inaccurate or incomplete records in the previous checks. Registry operators will notify the relevant registrar of any inaccurate or incomplete records identified during the checks, triggering the registrar’s obligation to solicit accurate and complete information from the registrant. | The New gTLD Policy contains a variety of new, mandatory rights protection mechanisms for trademark owners. The goal of improved WHOIS accuracy in the new gTLD context has been the subject of intensive discussions and negotiations among registrars, the GAC, law enforcement, and the community for several years. Inspired, in part, by GAC demands and threats, registrars have spent countless hours over the last 18 + months working with ICANN and law enforcement to craft a Registrar Accreditation Agreement (RAA) for the New gTLD program. The draft agreement, which is now posted for public comment, addresses a long list of LEA and GAC requests and saddles registrars with significant new obligations related to verification and validation of WHOIS data. In addition, the new RAA already requires registrars to create audit trails so that ICANN can evaluate and hold registrars accountable for any failure to act on reports of missing, inaccurate, or incomplete WHOIS data.  In addition, in December of 2012 ICANN created an Expert Working Group on gTLD Directory Services. The objectives of the working group are to 1) define the purpose of collecting and maintaining gTLD registration data, and consider how to safeguard the data, and 2) provide a proposed model for managing gTLD directory services that addresses related data accuracy and access issues, while taking into account safeguards for protecting data. This output will feed into a Board-initiated GNSO policy development process to serve as a foundation for the GNSO's creation of new consensus policy, and requisite contract changes, as appropriate.  Notwithstanding clearly relevant policy and process development, the GAC is now calling for a prescriptive, one-size-fits-all, registry led approach to a complex problem. While some niche and community-oriented applications do contemplate greater registry involvement in ensuring accurate WHOIS data, in those cases, the applicants intend to operate in an environment that will facilitate this level of involvement, and they have had the opportunity to structure their business model accordingly. To our knowledge, however, there are no automated tools available for conducting the kind of reviews called for in the GAC Advice. To the extent that it is possible to review WHOIS data address formats, existence of data, etc., that is already specifically required by the RAA itself. Moreover, registrars are now required to undertake verification of WHOIS information whenever they become aware of possible inaccuracy. ICANN operates a complaint referral process that, under the 2013 RAA, will trigger the registrar’s obligations to solicit accurate and complete information from the registrant. The GAC Advice would require registry operators to undertake costly labor-intensive manual reviews of WHOIS data samples and duplicate ICANN’s existing WHOIS complaint referral process. The cost of these requirements is unknown, and any impact they might have on WHOIS accuracy is entirely speculative. |
| **All Strings - Mitigating abusive activity**  Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law. | An obligation to comply with applicable law is generally an imputed term in all agreements. Presumably, the GAC has made this recommendation because it intends to obligate registries to play a role in enforcing the terms and conditions of an agreement (the registrar-registrant agreement) to which it is not even a party. But participants in the RAA negotiations – including law enforcement – have acknowledged that registrars themselves will often lack both the facts and the legal expertise required to determine (a) what law applies to a particular registrant’s conduct and (b) whether specific conduct is prohibited under the law that does apply. That is precisely why ICANN has adopted Consensus Policies such as the UDRP, Rapid Suspension, etc., which create expert bodies to evaluate registrant conduct in relationship to those policies (as opposed to the law of a particular sovereign). That is also why the rights protections mechanisms in the New gTLD Policy, as reflected in the Applicant Guidebook, do not impose this kind of operational responsibility on new gTLD registry operators. Indeed, the new RAA, which is extremely responsive to law enforcement recommendations, takes a different approach that reflects the appropriate role of registrars in supporting law enforcement activities by requiring dedicated points of contact, mandating specific data collection and retention practices, etc. But even that document - which has been the object of community discussion for nearly two years now - does not propose to deputize contracted parties to serve as extensions of law enforcement or the judicial system.  Problems associated with malware, botnets, phishing, and similar abuse are complex and require a cross-sector response, driven by subject matter experts. That is why many registry services providers (including Neustar) participate in voluntary industry coalitions such as the Anti-Phishing Working Group. Best practices emerging from expert organizations such as the APWG and the Copyright Information Center are more appropriate venues to tackle these problems, and far more likely to produce effective strategies to combat them. |
| **All Strings - Security checks**  While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved. | This Advice appears to be encompassed in the GAC’s Advice regarding abuse mitigation, above. It is addressed in the 2013 RAA through the new obligation that registrars provide 24/7 abuse contact information for use by relevant law enforcement, consumer protection authorities, etc., to report potentially illegal activities, and the requirement that such reports are reviewed and responded to within a specific time period. ICANN has the authority to audit registrar compliance with this obligation, and has a variety of enhanced enforcement tools to address non-compliance. Despite the clear focus on this issue in the context of the 2013 RAA, the GAC’s Advice creates a completely new, unanticipated cost – and associated legal liability to registrars and registrants – on new gTLD applicants. It is inappropriate to use the String Objection procedures in the New gTLD Applicant Guidebook to create significant new policy applicable to all TLDs. |
| **All Strings - Documentation**  Registry operators will maintain statistical reports that provide the number of inaccurate WHOIS records or security threats identified and actions taken as a result of its periodic WHOIS and security checks. Registry operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request in connection with contractual obligations. | ICANN has a web-based process for complaints about non-responsive registrars. ICANN and registrars continue to attempt to resolve significant issues related to frivolous and harassing complaints, and it makes little sense to create two different systems. To the extent any registry involvement is necessary, it should be sufficient to provide a link to the ICANN page at: <http://reports.internic.net/cgi/registrars/problem-report.cgi> |
| **All Strings - Making and Handling Complaints**  Registry operators will ensure that there is a mechanism for making complaints to the registry operator that the WHOIS information is inaccurate or that the domain name registration is being used to facilitate or promote malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law. | ICANN has a web-based process for complaints about non-responsive registrars. ICANN and registrars continue to attempt to resolve significant issues related to frivolous and harassing complaints, and it makes little sense to create two different systems. To the extent any registry involvement is necessary, it should be sufficient to provide a link to the ICANN page at: <http://reports.internic.net/cgi/registrars/problem-report.cgi> |
| **All Strings - Consequences**  Consistent with applicable law and any related procedures, registry operators shall ensure that there are real and immediate consequences for the demonstrated provision of false WHOIS information and violations of the requirement that the domain name should not be used in breach of applicable law; these consequences should include suspension of the domain name. The following safeguards are intended to apply to particular categories of new gTLDs as detailed below. | The WHOIS issues are addressed directly in the new 2013 RAA, which requires registrars to verify WHOIS information in response to reports of inaccuracy and, if they unable to do so, to suspend such registrations. It does not make sense to create potentially conflicting enforcement models. Moreover, this approach creates potentially significant liability to registrants – with whom registries do not have direct relationships in most cases.  Likewise, the new RAA requires registrars to provide Abuse Contact information and imposes a duty to investigate reports of registrant abuse. Registrars must provide monitored points of contact to receive reports of illegal activity by law enforcement, consumer protection, quasi-governmental or other similar authorities.  ICANN has a web-based process for complaints about non-responsive registrars. ICANN and registrars continue to attempt to resolve significant issues related to frivolous and harassing complaints, and it makes little sense to create two different systems. To the extent any registry involvement is necessary, it should be sufficient to provide a link to the ICANN page at: <http://reports.internic.net/cgi/registrars/problem-report.cgi> |
| **Advice: No Consideration Beyond Initial Review** |  |
| ICANN should not proceed beyond Initial Evaluation  .shenzhen (IDN in Chinese), .persiangulf, .guangzhou (IDN in Chinese), .amazon (and IDNs in Japanese and Chinese), .patagonia, .date, .spa, . yun, .thai, .zulu, .wine, .vin | The issue of geographic names has been the subject of extensive discussion and policy development as part of the new gTLD process. The GAC has contributed to and participated in these discussions, and GAC concerns have been addressed in the New gTLD Applicant Guidebook. The GAC Principles contained a broad statement regarding the use of country, territory, or place names and names that describe language or people. In addition, it its letter of 4 August 2010, the GAC indicated that it sought procedures to identify “strings that could raise “national, cultural, geographic, religious and/or linguistic sensitivities or objections.” Noting the work undertaken by the Recommendation 6 Working Group, the GAC commented that it remained concerned about proposed strings that are *“contrary to national law, policy or regulation … and/or refer to religions ethnicity, languages or other cultural identifiers that might raise national sensitivities.”* (Interim GAC comments dated 22 November 2010) On 26 May 2011, the GAC formally accepted the definition of geographic names in the Applicant Guidebook, saying:  *“Given ICANN's clarifications on "Early Warning" and "GAC Advice" that allow the GAC to require governmental support/non-objection for strings it considers to be geographical names,* ***the GAC accepts ICANN's interpretation with regard to the definition of geographic names****. The GAC appreciates the language that has been added to the Applicant Guidebook augmenting the definition of geographic names such that: “A string shall be considered to be a country or territory name if: … it is a name by which a country is commonly known, as demonstrated by evidence that the country is recognized by that name by an intergovernmental or treaty organization.”* GAC Comments on New gTLDs 26 May 2011.  As a result of GAC concerns related to geographic strings, country and territory names are not permitted in this new gTLD round. In addition, the Applicant Guidebook requires specified levels of governmental support for applications for strings that correspond to (1) capital city names; (2) city names used for purposes associated with the city; (3) an exact match for a country province or state listed in the ISO 3166-2 standard; (4) a string listed as a UNESCO region or appearing on the UN’s list of macro geographical, sub regions, and selected economic and other groupings list. The GAC has included several strings in this category that fall outside of the definition of geographic names, and that do not appear to raise cultural, or religious sensitivities. To the extent that these concerns arise from vague and undefined “national sensitivities” about strings that are not encompassed in (1) – (4) above, the objections raise significant questions about fundamental fairness, transparency, and predictability. At a minimum, complaining governments have a duty to explain why a specific use of a string create such national sensitivities, particularly where the governments themselves permit – and even grant trademark protection for non-confusing commercial use of identical strings.  Moreover, the commercial use of place names has been and continues to be a hotly debated topic in the context of international trade law. These discussions should be resolved in appropriate international treaty organizations, and ICANN should not permit itself to be used to short-circuit those processes. |
| **Category 1: Consumer Protection, Sensitive Strings, and Regulated Markets**  Category 1:strings “likely to invoke a level of implied trust from consumers, and carry higher levels of risk associated with consumer harm. “ The GAC Advice identifies a “non exhaustive” list of several hundred strings, including: | **Implementation Issues**. The GAC Advice asserts that the strings are “likely to involve a level of implied trust” and simultaneously create a relatively higher risk of consumer harm. This sweeping statement is overbroad and ignores entirely the important issue of context. In addition, even a quick review of the strings that have been included and excluded demonstrates the degree to which the GAC Advice lacks consistency and fails to reflect the kind of objective, principled basis that is fundamental to equitable implementation. The GAC Advice provides no principled basis for understanding why some strings are included and others are not. For example:   * The “Children” category includes:   + .*school* BUT NOT .*camp* * The “IP” List includes:   + .*fashion* BUT NOT .*style* or .*clothin*g   + .*author* BUT NOT .*actor*   + .*rip* BUT NOT .*bio*   + .*pictures* BUT NOT .*pics* and .*gallery*   + .*tunes, .music,* and .*song,* BUT NOT *.country*   + .*tour*  and *.tours,* BUT NOT *.voyages, .vacations, .booking*   + .*discount* BUT NOT .*cheap* or .*bargain*   + .*entertainment* BUT NOT .*booking, .tickets*, or .*ticketing*   + .*show* BUT NOT .*production* or .*event*   + .*hiphop* BUT NOT .*dance* * The “Education” list includes:   + *.degree, .mba*, and .*university*, BUT NOT .*college, .education, .phd, .training*, or .*science* * The “Health and Fitness” category includes   + .*care*, BUT NOT .*help*   + .fit BUT NOT .*yoga* or .*coach*   + .clinic BUT NOT .*salon* * The “Financial” category includes:   + .*lease* BUT NOT .*rent*   + *.exchange* and *.trading* BUT NOT *.trade*   + *.investments* BUT NOT *.gold*   + .*retirement* BUT NOT .*rich*   + *.financialaid* BUT NOT *.scholarships* * The “Charity” category includes:   + .*charity* BUT NOT .*foundation* * The “Professional Services” category includes:   + .*accountant* and .*associates* BUT NOT .c*onsulting* or .*marketing*   + And what about all of those other professions with licensing requirements such as .*realty, .plumbing, .builders, .contractors* and many, many others?   **Category Selection**. The “categories” identified by the GAC are broad and undefined. There is no principled basis for distinguishing between lawyers and plumbers, both of which are subject to licensing requirements. |
| **Category 1 Advice**   1. Registry operators will include in its acceptable use policy that registrants comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures. 2. Registry operators will require registrars at the time of registration to notify registrants of this requirement. 3. Registry operators will require that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law and recognized industry standards. 4. Establish a working relationship with the relevant regulatory, or industry self--‐regulatory, bodies, including developing a strategy to mitigate as much as possible the risks of fraudulent, and other illegal, activities. 5. Registrants must be required by the registry operators to notify to them a single point of contact which must be kept up--‐to--‐date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self--‐regulatory, bodies in their main place of business. | As discussed above, registrant is inherently obligated to comply with applicable laws relating to privacy, data collection, consumer protection, fair lending, debt collection, etc. The proposition that registrants are liable for their conduct under applicable law is not contested. The GAC Advice, however, would impose liability on registry operators with respect to registrant conduct, and require registry operators to identify the law applicable to any particular registrant, and to evaluate the conduct of a registrant against such law. Registry operators lack the factual background and requisite legal expertise needed to serve in a law enforcement capacity. While registries and registrars are obligated to cooperate with and assist appropriate law enforcement agencies in accordance with applicable due process requirements, “outsourcing” law enforcement to the private sector, particularly in a multi-jurisdictional global environment raises significant policy, due process, and business concerns that must be addressed.  This raises the same issues discussed in the general overview and in response to Item #1 above.  Privacy and data security requirements are established by national and local law, and vary dramatically from country to country. It is entirely reasonable to expect registry operators to handle data they collect and maintain to comply with applicable data privacy and security laws. It is reasonable to require registrants to be transparent about their data collection and processing practices, but in most situations it is unreasonable to expect registry operators to pass judgment on what law applies to a registrant’s conduct and whether or not that conduct is consistent with applicable law.  We think that this is generally a good idea, but raises questions from a contract enforcement perspective. Who, for example, would determine what industry self-regulatory organizations are “relevant” to a particular string? This seems like something that could be dealt with as part of an applicant’s Public Interest Commitments statement.  The substantive requirements of this GAC request has been fully incorporated into the 2013 RAA, which requires registrars to maintain a 24/7 monitored, single point of contact to receive abuse reports from designated law enforcement, consumer protection, and quasi-governmental or similar authorities, to publish their complaint processing policies and procedures, and to maintain auditable records of their responses to such complaints. The text of the RAA follows:  *3.18.2 Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the Registrar is established or maintains a physical office. Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report. In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law.*  *3.18.3 Registrar shall publish on its website a description of its procedures for the receipt, handling, and tracking of abuse reports. Registrar shall document its receipt of and response to all such reports. Registrar shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, shall provide such records to ICANN upon reasonable notice.* |
| **Category 1: Bullying/Harassment**  applicants should develop clear policies and processes to minimise the risk of cyber bullying/harassment | This Advice may be appropriate with respect to certain applications, but seems irrelevant to others. The applications for .*sucks*, for example, contemplate operating the TLD as a venue for product and service reviews. |
| **Category 1 “Further” Advice**  “strings are associated with market sectors which have clear and/or regulated entry requirements “ including: | To the extent that an applicant has indicated that second level-domains in a particular TLD will be limited to licensed providers of product or services, it would be appropriate to expect an applicant to propose policies designed to enforce such limitations. In this case, however, the GAC is not giving advice related to applicant accountability. Instead it is creating general policy based on the overly broad and simplistic assertion that all of these strings relate to market sectors that have clear and/or regulated entry requirements. For example, while many countries regulate claims that a product is “green” or “organic,” few actually impose credentialing/licensing obligations on market participants. And none, to our knowledge, require providers of “earth” related content to be licensed. Similarly while a country may license gyms and workout facilities, fitness magazines are not subject to licensing requirements. Likewise, as noted above, whole categories of licensed service providers (e.g., .*plumbing*, .*contractors*, .*builders, beauty salons*, etc.). |
| **Specific “Further Advice”** |  |
| 1. At the time of registration, the registry operator must verify and validate the registrants’ authorisations, charters, licenses and/or other related credentials for participation in that sector. 2. In case of doubt with regard to the authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents. 3. The registry operator must conduct periodic post--‐registration checks to ensure registrants’ validity and compliance with the above requirements in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve. | This Advice may be appropriate with respect to specific applications, but that will depend in each case on the particulars of an application.  This Advice may be appropriate with respect to specific applications, but that will depend in each case on the particulars of an application.  This Advice may be appropriate with respect to specific applications, but that will depend in each case on the particulars of an application. |
| **Category 2: Restricted Access** |  |
| As an exception to the general rule that the gTLD domain name space is operated in an open manner registration may be restricted, in particular for strings mentioned under category 1  In these cases, the registration restrictions should be appropriate for the types of risks associated with the TLD. The registry operator should administer access in these kinds of registries in a transparent way that does not give an undue preference to any registrars or registrants, including itself, and shall not subject registrars or registrants to an undue disadvantage. | The GAC’s assertion of “general rule” to the effect that the gTLD domain name space should facilitate open registration is entirely new and wholly unanticipated policy that is in conflict with the New gTLD policy itself. The ICANN community spent many years developing the policy to govern the allocation of new top-level domains. That policy clearly permits applications for closed use of generic strings. In fact, participants in the new gTLD policy development process deliberately avoided prescriptive rules on gTLD types, choosing instead to promote innovation and to let market forces determine the variety of new TLDs. The policy includes a “Community Preference” procedure to address the kinds of public policy concerns related to regulated and or otherwise cohesive community, and to address concerns related, for example, to piracy and intellectual property rights abuses. The policy also contained built-in competitive safeguards, including the right for competitors to object to applications on a variety of grounds. There is no justification for reversing the conclusions reached during ICANN’s policy development process and introducing an entirely new policy based on general and speculative concerns about competition that are not backed by competition theory or economics. |
| **Category 2: Exclusive Access** |  |
| Exclusive registry access should serve a public interest goal | This represents entirely new and unanticipated policy. Moreover, in many cases it is in direct tension with the Advice on to Category 1 strings, where the GAC has called for specific limits on registration at the second level. The Community Preference policy was intended to address public interest issues arising in connection with certain generic strings, and it should be implemented in a manner that protects such interests.  The ICANN community spent many years developing the policy to govern the allocation of new top-level domains. That policy clearly permits applications for closed use of generic strings. In fact, participants in the new gTLD policy development process deliberately avoided prescriptive rules on gTLD types, choosing instead to promote innovation and to let market forces determine the variety of new TLDs. The policy includes a “Community Preference” procedure to address the kinds of public policy concerns related to regulated and or otherwise cohesive community, and to address concerns related, for example, to piracy and intellectual property rights abuses. The policy also contained built-in competitive safeguards, including the right for competitors to object to applications on a variety of grounds. There is no justification for reversing the conclusions reached during ICANN’s policy development process and introducing an entirely new policy based on general and speculative concerns about competition that are not backed by competition theory or economics. As the US Justice Department has noted, new gTLDs are unlikely to possess market power and concerns about anti-competitive exclusionary conduct only arise where (1) a company possesses substantial market power, (2) that market power causes the exclusionary conduct, and (3) the behavior is motivated by a desire to eliminate or damage a competitor, prevent entry of a competitor into the market, and/or constrain competitive activities in the market. |