

To the members of the ICANN Expert Working Group:

This purpose of this letter is to submit comments and suggestions regarding the report entitled “Initial Report from the Expert Working Group on gTLD Directory Services: A Next Generation Registration Directory Service” published by the Expert Working Group on 24 June 2013. LegitScript appreciates the opportunity to submit these comments.

This letter contains two primary sections:

- 1. Objections to the EWG report and proposed WHOIS replacement.**
- 2. Alternate suggestions about how to achieve the EWG’s mission.**

The Expert Working Group (EWG) proposes to replace the current “open by default” system for domain name registration WHOIS records, in which anyone can retrieve and analyze a WHOIS record, with a “closed by default” system, in which one global organization, the Aggregated Registration Data Services (ARDS), would house and control access to all WHOIS records. Giving one organization such far-reaching and unfettered power over public and private entities’ ability to access and freely use WHOIS records raises serious concerns that cannot be resolved by relying on the development of additional policies in future stakeholder dialogues.

As an anti-cybercrime organization, LegitScript is keenly aware of the problem of WHOIS inaccuracy — an important problem to solve, but one that we believe can be addressed without threatening the free and open Internet. In considering whether measures designed to improve WHOIS data accuracy requires restricting access to WHOIS data, it is important to note that WHOIS data is not separate and distinct from the Internet; rather, WHOIS data undergirds the structure of the World Wide Web and is part of the Internet itself. Put another way, restricting access to WHOIS data means restricting Internet users’ access to a part of the Internet. Internet users currently have the *de facto* right to review WHOIS data if they choose, and a substantial number of Internet users avail themselves of that opportunity (even if many only do so occasionally), and in doing so, may utilize all of the fields that exist in most WHOIS records.

Internet users as a whole also benefit indirectly from organizations that utilize WHOIS information and redistribute it in combination with value-added services. Walling off a section of Internet-related data and creating “classes” of Internet users who could access that information would have serious consequences for Internet users as a whole.

Accordingly and as discussed in detail herein, LegitScript objects to the current proposal as it:

1. Shifts from an “open by default” to a “closed by default” system whereby only certain Internet users would be granted private access to gTLD domain name registration information;
2. Empowers one organization to determine what constitutes legitimate use of WHOIS data, and to track, monitor and audit requests and use of such records;
3. Grants monopoly power of all WHOIS data to the ARDS, including the attendant power to determine prices and restrict or prohibit access;
4. Stifles future innovation and competition involving existing and potential future uses of gTLD registration data;
5. Prohibits lay Internet users from accessing and using WHOIS information, in many instances activity which may improve the security and stability of the Internet for the benefit of all;
6. Limits cybersecurity and other organizations’ ability to investigate Internet crime and pursue legitimate business interests;
7. Violates the 2009 ICANN Affirmation Of Commitments and exceeds the scope of the EWG’s mandate as directed by the ICANN CEO and Board of Directors.

The objections below are both substantive and procedural, and are followed by concrete suggestions for alternative approaches. Moreover, as noted herein, the 2013 Registrar

Accreditation Agreement (RAA) contains numerous provisions regarding proxy and privacy services, as well as WHOIS. In light of those provisions, LegitScript believes that the EWG's proposed solution is unnecessary and may even conflict with the spirit of the new RAA.

LegitScript appreciates the opportunity to submit these comments and stands ready to assist the Expert Working Group however possible.

1.0 **Objections to Expert Working Group Proposal**

The following objections to the EWG proposal are both substantive and procedural.

1.1 **Shift From “Open by Default” to “Closed by Default” WHOIS Structure**

First, it is important to understand that the EWG proposes that WHOIS move from a system that is currently “open” by default to one that is “closed” by default.

Currently, WHOIS records are, by default, openly available on the Internet, either by a website-based query or via a Port 43 query. There are exceptions to this, of course, but situations in which WHOIS records are unavailable are accurately seen as the exception to the rule. In short, if an Internet user wishes to review a domain name’s registration record, they typically have the opportunity and *de facto* right to do so, without supervision, subsequent scrutiny or financial obligation.

The proposed new system, described as involving “gated access,” is properly understood as being “closed by default.” This is because, in contrast to a system in which all of the fields of a WHOIS record are publicly available via a normal query, as proposed:

- The full WHOIS record, as currently defined, would be unavailable. The default status for normal Internet users will be that only a restricted portion of the WHOIS record will be available, at most. Although not directly stated, the context of the proposal suggests that only a small portion of the WHOIS record (e.g., the registrant’s name) would be publicly accessible to the general public, with the remainder of information inaccessible.
- Remaining portions of the WHOIS record would be unavailable as a rule; exceptions would be made for select companies, government agencies and individuals who meet criteria determined by ARDS.

- Currently, there is – as a practical matter, with exceptions that EWG members are likely aware of – no or few limits to the number of WHOIS records that an Internet user can query. The EWG proposal indicates that there would be limitations placed on the number of queries that requestors – presumably including typical Internet users — could run.

In other words, the existing nature of WHOIS record availability is exactly reversed: currently, the default nature of WHOIS records is to be openly available, and instances in which WHOIS records are closed or restricted are correctly viewed as exceptions. Under the new system, the default nature of public access to gTLD registration data would be restricted, with privileges granted to certain requestors.

At least one member of the EWG has argued to LegitScript that the new system would be “both open and involving gated access” (because some minimal number of fields in existing WHOIS records could be publicly queried) thus implying that the fundamentally open nature of WHOIS records would continue in parallel with a gated access system. A plain reading of the proposal evidences this is not an accurate representation of the EWG’s proposed structure. Even if a single field or limited number of fields in WHOIS records remain openly available to all Internet users, the creation of a new structure to regulate who can see which fields, when, why, how much and for what cost, reverses the “open by default” nature of WHOIS and makes it “closed by default.” In this way, unrestricted access becomes the *exception*, not the rule. The current system in which any Internet user has the right to view, in most cases, a registrant’s name, address, city, state, email address, phone number, country, and more would no longer exist, and any such opportunity would exist only in the discretion of a global organization.

Moreover, the creation of such a gated structure does nothing to ensure Internet will continue to have even this, albeit restricted, level of access to WHOIS records. In short, the rules could change in the future, leading to further restrictions on what a typical

Internet user could access. Accordingly, the fundamental nature of the new system cannot be described as open. Rather, it would become closed by default, with some exceptions that the ARDS would grant to classes of Internet users who would enjoy access to certain information on the Internet that other Internet users would not be privy to.

For these reasons, simply expanding the use cases in Annex B of the EWG’s report will not address the concerns raised in this letter. LegitScript believes that there can be no compromise to the principle that a closed, gated-access “members-only” WHOIS system must be vigorously opposed as antithetical to the open and free nature of the Internet.

1.2 ARDS Data Collection and Punitive Powers

LegitScript also objects to the wide-ranging powers that will be granted to the ARDS. Irrespective of whether or not those powers are immediately and fully utilized, it is too much power and authority for any single organization to have.

As preface to this section, LegitScript understands that the EWG’s response to the concerns detailed in this section may be, in essence, “The future policy processes will address these concerns.” That response unfortunately misses the point. Even if the existing members of the EWG ensured that the short-term policy process addressed these concerns, a “closed-by-default” WHOIS system leaves no assurance that in five, ten or twenty-five years the “goal posts would not shift,” so to speak.

1.2.1 Centralized Data: Technical Risks

The Internet’s strength lies in decentralization. No one organization controls the Internet. By way of analogy, structurally and technically, there are numerous root servers and 13 named authorities in the root zone delegation data. There is no longer just one registrar (in contrast to Network Solutions’ near-monopoly in the 1990s). There are several reasons for all of this, but one benefit is that a centralized repository of data becomes a target for hackers and miscreants.

Centralizing all gTLD registration data in one place becomes a potential point of massive failure — a significant structural vulnerability. Indeed, it can be guaranteed that the ARDS would be a fat target.

One member of the EWG has argued to LegitScript that WHOIS data is already centralized, at registries, and the ARDS would be no different. However, that is not accurate: the registry only has its own data, and in a significant number of cases, the registrar also has thick WHOIS data. Even if a single registry's data were to be compromised, WHOIS records would still be available for other registry's data. (Depending on the size of the registry, of course, the effect would be different: losing access to all .COM data is different than losing access to all .AQ domain name information.)

To drive this point home, consider that in early 2013, rogue Internet pharmacy and spam content was found on an .ARPA website. The simple fact is that corruption and threats go hand-in-hand with criminal activity on the Internet, and the decentralized nature of the Internet is, in part, a protection of the Internet infrastructure as a whole.

1.2.2 Power to Determine “Permissible Purpose” and Audit Actual Use

The EWG and/or ARDS would be charged with determining what constitutes a permissible purpose for accessing each WHOIS field. Just as it is not ICANN's or the EWG's place to tell Internet users which websites they may and may not visit, it is not the EWG's or ARDS' place to dictate to Internet users which reasons for wanting to see who operates a domain name are legitimate, other than clear cut scenarios already determined by stakeholder consensus (e.g., those noted in the WHOIS Marketing Restriction consensus policy).

Even more troubling, the ARDS would then have the power to monitor how that information was used and — if it was used in a way that the ARDS disagreed with — impose penalties on the user.

By way of specific examples, consider the following. All of these fall squarely within the power of the ARDS as described in the report.

- A journalist is writing an investigative article and wishes to review currently-available WHOIS information. The ARDS would have the power to require the journalist to register and disclose the reason for wanting the information, and to determine if the journalist's reason was legitimate. It would also have the ability to monitor the journalist's use of the domain name registration data.

Note that bloggers increasingly play a journalistic role, so — for example — attempting to resolve this situation by requiring journalist credentials would simply chill bloggers' ability to freely write research-oriented or investigative blogs.

- A political activist may wish to expose corruption by an elected politician that requires access to WHOIS data, e.g., to show that the politician is operating a particular website. (This is not a far-fetched example; LegitScript is aware of at least one case in which a rogue Internet pharmacy was registered to an address that ended up being for an elected politician.) The ARDS would require the political activist to disclose his or her reasons for wanting the information, possibly leading to a chilling effect on the activist's desire to follow through in obtaining the information.

- The report explicitly states that the EWG or ARDS will determine what constitutes a legitimate law enforcement purpose. This is inappropriate on multiple levels. First, although there is an important need for citizen oversight of the police, the ARDS is emphatically not the correct organization to assume this role, and it is completely inappropriate for the ARDS to begin taking positions on what constitutes legitimate or illegitimate law enforcement requests. It is likewise wholly inappropriate for the ARDS to monitor how law enforcement agencies utilize the data, as this could compromise investigations. Second, the report suggests that the ARDS would also keep a log of all requests, presumably including law enforcement requests. Third, this raises questions, such as: Would individuals or companies engaged in illegal activity who worry about being targeted by law enforcement have the right to demand that ARDS tell them about law enforcement requests touching on their domain names, thus compromising law enforcement investigations?
- An academic researcher would be required to disclose the nature of their research; the ARDS would be empowered to determine whether it constituted legitimate research or not.
- An Internet startup has what it believes to be a great new idea for how to organize and analyze websites based in part on WHOIS data, or provide other value-added information or services. The ARDS would have the power to determine whether or not the idea was sufficiently worthy to warrant allowing the startup access to WHOIS data. Additionally, the startup might wish to keep its idea and strategy confidential as a trade secret, but the ARDS would have the power to require (potentially public) disclosure.

There are many more examples of the power that the ARDS would have to chill current Internet activities and free speech. Additionally, in all of the cases above, it seems probable that the ARDS would, as part of the decision-making processes, also have to determine who constituted a *bona fide* member of each profession or class: whether the individual should really be treated as a journalist, political activist, academic, OpSec specialist, and so forth, resulting in the creation of different classes or tiers of Internet users.

Given the current makeup of the EWG — professionals who are committed to openness and would never knowingly support any of the negative outcomes illustrated above — it may be tempting to see the sample scenarios above as far-fetched. It may also be tempting to respond that the multi-stakeholder governance process will assure that these negative scenarios do not come to pass. LegitScript believes that those responses are insufficient: who the stakeholders are in any ICANN process changes over time, and if a closed-by-default, centralized gTLD domain name registration system is implemented, there are no protections in the long-term from the ARDS’ power being misused as described above. By contrast, the current open-by-default system makes that sort of misuse of power impossible.

1.3 **Creation of a “Super Monopoly”**

The proposal functionally grants the ARDS a “super-monopoly” over WHOIS information and over paid, value-added services derived from the WHOIS information. The proposal states that the ARDS itself may be able to provide value-added services (e.g., reverse WHOIS lookups) for a fee.¹ But the proposal states that the ARDS would “manag(e) licensing arrangements for access to data”² — a significant departure from the current system in which nobody owns WHOIS data (and therefore, nobody can “license”

¹ EWG Initial Report, Page 27.

² EWG Initial Report, pages 4, 26, and 31.

it). Granting the ARDS the ability to “manag(e) licensing arrangements for the data” indicates that value-added services, or distribution to clients or customers (as firms such as domaintools.com and others currently do in a competitive market), by third-parties may be prohibited or significantly restricted: whether a company could pass on the WHOIS data, or its analysis of the data, to a client would be up to the ARDS. At the same time, the ARDS could set its own prices for these value-added services and exclude any competition. In other words, the ARDS would not only have sole market power to control the information and set prices for accessing it, but it could exclude and even levy punitive measures against other entities that attempted to compete with it or offer a better or different service — a perfect monopoly that would stifle both competition and innovation in this space.

1.4 Prohibitions on Redistribution

Although not explicitly stated in the EWG report, LegitScript reads the report to recommend against any third-party value-added redistribution of gTLD domain name registration data (since the ARDS would only approve specific requestors and their purpose, and would be empowered to audit those requestors to ensure compliance). There are two overriding reasons that this prohibition would be poor policy, and access to WHOIS records should permit reasonable levels of value-added redistribution (provided that the purpose does not violate prohibitions against using the records for marketing purposes).

First, when Internet start-ups are first created that have some sort of use for WHOIS data, they may not have the resources to identify and collect the information they need directly. Even a process as simple as grabbing zone files and processing the data, let alone obtaining and analyzing WHOIS records via Port 43, can be a daunting, expensive task for a young company. In cases like this, the company may rely heavily on third-party

providers to begin obtaining the WHOIS data it needs, such as DomainTools.com or a similar company. This is cost-effective and supports innovation.

Second, restricting access to WHOIS records will have a chilling effect on future innovation. The EWG cannot possibly contemplate of all future use cases in which a visionary entrepreneur might seek to incorporate WHOIS data into a new, valuable product or service on the Internet — a product or service that nobody has yet contemplated, but that might fall into a category of use that the ARDS would not immediately recognize as pre-approved. Nor should that visionary entrepreneur be subject to the whims of whether the ARDS agrees with his or her contemplated use of the gTLD registration data. Indeed, DomainTools’ value-added organization of all WHOIS data, and LegitScript’s use of a large swath of WHOIS data to help make determinations about healthcare website legitimacy, likely would not have been foreseen, or perhaps, agreed with by other ICANN stakeholders, before those respective organizations were created. Those are but two examples among many.

In response to this, some may suggest amending the EWG’s proposal (e.g., in Annex B) to add a new category of acceptable users (e.g. “by entities for legitimate uses not currently contemplated”) or a new process by which future legitimate uses may be approved by the ARDS. While well-intended, any such proposal misses the point; the beauty of the Internet has been that innovation may come from anywhere, at anytime, by anyone, unencumbered by traditional barriers to entry (e.g. registration, pre-approval, authorizations, etc.). By definition, any proposed acceptable use category or ARDS authorization process aimed at creating a pathway for future innovators to access WHOIS data creates barriers to entry, slows speed to market, and burdens small, start-up businesses. Such outcomes undermine the value of the free and open Internet as we know it today by stifling future innovation and creativity.

To drive this point home, there are legitimate reasons for Internet users to need access to republished WHOIS data, as in LegitScript’s case, where reasons may range from providing Internet users in general, or our clients specifically, information about a legitimate or illicit Internet pharmacy’s WHOIS record to support a determination that the website is not operating as a safe, licensed Internet pharmacy. Also in the online healthcare space, patients sometimes need access to the republished data too: in direct point of fact, when an Internet user chooses to fill a prescription online, LegitScript recommends that they verify who actually operates the website, and where the website operator is located — information we can provide (and do) by republishing the WHOIS data. Also, if the Internet user does fill a prescription online and has an adverse reaction to the drug, in some cases, the WHOIS record may be the only way to attempt to reach the Internet pharmacy, especially in grey-area or rogue cases in which the contact information is not published on the website. In these cases, the average Internet user is not running their own WHOIS query, but relies on the redistributor of the WHOIS information, such as LegitScript, to obtain the WHOIS records, analyze them and put them in context, add other information (e.g., “This Internet pharmacy purports to be in London but the domain name is registered to a person in China who has registered other domain names engaged in the sale of counterfeit drugs.”) and redistribute the WHOIS record together with other information in a value-added package.

1.5 Accurately Defining Why Internet Users Access WHOIS Information

LegitScript’s understanding about how Internet users utilize WHOIS records (and why) is largely informed by our extensive work in the area of healthcare fraud via the Internet, with a focus on “rogue” Internet pharmacies and illicit dietary supplement websites. LegitScript works extensively with registrars as well as members of the general public, and we accept and process literally hundreds of abuse reports a day about fraudulent or illicit healthcare websites from average Internet users, many of which are passed on to domain name registrars, content hosting providers, social media companies, domain

name registrants (e.g., in the event that a website’s content has illicit content uploaded to it without the registrant’s permission) or other members of the Internet infrastructure.

It is important for the EWG to understand that many Internet users who submit abuse reports to LegitScript, and other anti-abuse companies, would never be “credentialed” — they are simply average Internet users — but who, sometimes only on a single occasion, engage in valuable “amateur research” of a rogue Internet pharmacy domain name based on any or all of the fields in a WHOIS record, including the email address. For example, there are thousands of “fake CVS” or “fake Walgreens” rogue Internet pharmacies. (Note: these do not necessarily contain those trademarked terms in the domain name, so it is not necessarily resolvable as a brand protection issue.) It is common that an Internet user will review the full WHOIS record and based on any one of the fields in the WHOIS record, conclude that it is an illicit website and submit an abuse report. In many cases, this may specifically include analysis of the WHOIS record’s email address. Indeed, anti-abuse firms can only do so much; it is often the public who notice odd things and then research and find abusive behavior on their own volition, or as a result of a fraudulent transaction on their credit or debit card.

It is also critical that the EWG understand that these abuse reports may be generated by average Internet users even in the case where a WHOIS record is accurate. (In other words, even domain names with accurate WHOIS records may still be rogue Internet pharmacies.) There are numerous cases in which a WHOIS record is accurate but, based on any or all of the fields in a WHOIS record, the Internet user determines that — for example — the address, email or phone number of a seemingly legitimate Internet pharmacies can be connected via a search engine query to a website or business elsewhere identified as engaged in fraudulent or other illicit activity.

To provide another example specifically in the area of online healthcare, if an Internet user fills a prescription online and has an adverse reaction to the drug, in some cases, the

WHOIS record may be the only way for the user to attempt to reach the Internet pharmacy, especially in grey-area or rogue cases in which the contact information is not published (or is incorrectly published) on the website. In such cases, time can be of the essence, and the full WHOIS record, including the email, is required.

The extent to which the ability of everyday Internet users to support anti-abuse and reputational efforts on the Internet rests on full and complete access to WHOIS information cannot be understated. In many cases, the individual is not even a hobbyist in the anti-abuse or reputation space; rather, they have personally interacted with a single website, had a negative experience and spent five or ten minutes doing their own research. Or, the individual is an occasional user of a service such as — for example — the Web of Trust (mywot.com) who are not employed by, or agents of, that company, but who occasionally make use of the full information in a WHOIS record to make reputation determinations. To withhold this important piece of Internet data from these average Internet users until and unless they are credentialed by the ARDS would, as a practical matter, destroy the right and ability of average Internet users to engage in this sort of valuable activity.

1.6 Procedural Objections to EWG Scope and Violation of Affirmation of Commitments

Additionally, LegitScript raises two chief procedural objections to the EWG report. First, the EWG's proposal violates the ICANN Affirmation Of Commitments (AOC). Second, the EWG's proposal exceeds the scope of what the ICANN Board of Directors directed the EWG to do.

1.6.1 Affirmation of Commitments. As to the first objection, ICANN notes that the rationale for the EWG's research is based on the Affirmation Of Commitments, which requires that ICANN implement measures to maintain timely, *unrestricted and public access* to accurate and *complete WHOIS information*, including registrant, technical, billing, and administrative contact information (emphasis added). The closed-by-default

WHOIS structure proposed in the report directly violates the AOC, by *restricting* and making *complete WHOIS information non-public* — exactly the opposite of what the AOC requires. LegitScript thus objects to the proposed new structure on the basis that it violates an important provision of the AOC.

1.6.2 Scope of EWG Mission. Second, and by way of background, we note that the EWG’s report states that the purpose of the report is to “to help resolve the nearly decade-long deadlock within the ICANN community on *how to replace the current WHOIS system*, which is widely regarded as ‘broken.’” (emphasis added). The use of the word “replace” (and the entire proposal involving replacement of WHOIS) in the EWG report indicates that the EWG misunderstood and exceeded its mission: the ICANN CEO and Board of Directors nowhere instruct the EWG to come up with a proposal to discard and replace the current WHOIS system. Note that a key rationale for the EWG’s report are the findings of the WHOIS Policy Review Team’s Final Report,³ accessible at <http://www.icann.org/en/about/aoc-review/WHOIS/final-report-11may12-en>. The WHOIS Policy Review Team’s Final Report states that “...the current (WHOIS) system is broken and needs to be *repaired*.” It does not use the word *replace*.

These distinctions may seem academic, but they are important: “repair” means to fix or mend something, causing its improvement without discarding the object itself. “Replace,” by contrast, means to discard the original and find an entirely new object or system. By proposing to implement a closed-by-default gTLD domain name registration data system that would *replace* (not repair) the current system, doing away with WHOIS as we know it, and implementing a structure that would make most gTLD domain name registration data restricted and non-public, the EWG exceeds the scope of the its mission as described by the ICANN Board. There is no evidence of community consensus to do away with the existing structure entirely and start over, and LegitScript suggests that it is not

³ <http://www.icann.org/en/groups/board/documents/prelim-report-08nov12-en.htm#1.a.rationale>

appropriate for the EWG, of its own accord, to expand the scope of its mission beyond stakeholder community consensus.

It is true that the ICANN Board of Directors’ resolution provided that the ICANN CEO should “launch a new effort to redefine the purpose of collecting, maintaining and providing access to gTLD registration data, and consider safeguards for protecting data, as a foundation for new gTLD policy and contractual negotiations, as appropriate.” Here, however, the EWG appears to interpret the word “redefine” to mean that it is empowered to dictate to Internet users which reasons for accessing gTLD domain name registration data are legitimate and which ones are not — a power that the ARDS (or a policy-related committee such as the EWG) would be granted. However, a historic reading of various documents such as SAC055 suggest that the correct interpretation of the word “redefine” in this case is the reverse of how the EWG has interpreted it: the EWG should seek to better understand the various reasons that Internet users may wish to access WHOIS records and ensure — as the AOC requires — unrestricted access, not restricted access, except for reasons defined as illicit in the WHOIS Marketing Restriction Consensus Policy.⁴ In other words, the EWG should utilize a from-the-ground-up approach and be informed by Internet users’ use of WHOIS and seek to expand access, not seek to tell Internet users from the top down of how and why they will be allowed to use WHOIS and restrict their access.

Accordingly, LegitScript objects on procedural grounds to the EWG report as violating the AOC and exceeding the scope of authority granted to the EWG. The EWG acts properly and within its scope if it identifies ways to retain and improve WHOIS both as to accuracy and access. By proposing to discard the existing WHOIS structure and restrict, not improve, access, the EWG exceeds its mission, fails to develop a plan to achieve half of the mission (improving access), and proposes a plan that would be contrary to the Affirmation Of Commitments.

⁴ <http://www.icann.org/en/resources/registrars/consensus-policies/wmrp>

2.0 Suggestions For Achieving the EWG’s Mandate

The purpose of this section is to provide suggestions that LegitScript hopes will be useful in structuring a system that retains the open nature of the Internet, yet achieves the goals outlined by the ICANN Board.

As noted above, the EWG is directed to repair (not “replace”) the current WHOIS system, by redefining the purpose of collecting, maintaining and providing access to gTLD registration data; considering safeguards for protecting the data; and identifying solutions to improve accuracy and access to gTLD registration data.

In addition to the concrete recommendations outlined below, we note that the 2013 RAA contains several new provisions and requirements pertaining to WHOIS accuracy and access, and proxy and privacy services. LegitScript therefore recommends that the new RAA provisions, including those pertaining to WHOIS, be implemented and their effect evaluated, before the stakeholder community can accurately evaluate whether supplemental policies and structures, such as the ones described below, are necessary.

2.1 Standardize WHOIS Record Format

As a first step, the EWG or another ICANN-led working group should lead an effort to standardize the format of WHOIS records across registrars and registries. The reason for this is not merely convenience: the verification of WHOIS record authenticity requires the ability to validate WHOIS record data with 100% accuracy; this, in turn, is made exceedingly more difficult by the lack of a universal format. Consequently, a registrar attempting to use an automated verification system cannot tell whether, for example, “New York” is properly in the city field or improperly in the country field (thus flagging the WHOIS record for further scrutiny). Because part of the EWG’s mission is to identify a solution to improve WHOIS accuracy, the necessary first technical step is to standardize WHOIS formats. Standardization also contributes to improved access, for example,

through improved ability to accurately reverse query specific WHOIS data fields for known parameters. Finally, as an added benefit, as seen in other industries (manufacturing, transportation, and software, to name a few), technical standards also pave the way for innovation by lowering barriers to entry, an outcome that benefits Internet users worldwide. This standardization should apply to all current and future gTLDs.

2.2 **Release a Request for Proposal (RFP) For WHOIS Verification**

The objective of having a third party verify WHOIS records (or, at least, identify those that are not authentic or accurate) is a good idea that should be explored further. We note, however, that having third parties verify WHOIS records does not require that all of the WHOIS data be housed in and controlled by a single entity. It also does not require access to be restricted to WHOIS records.

We suggest that ICANN release an RFP and accept competitive bids from companies to engage in active, ongoing analysis and identification of falsified or improper WHOIS records. One model for this system — given the different subject matter it is an imperfect analogy — may be the WIPO model used for resolving trademark disputes. Possible models that the EWG may wish to consider would include:

- There could be five companies charged with WHOIS verification and/or identifying incorrect WHOIS records, one for each of the five geographic RIR jurisdictions. (An open question would be whether “jurisdiction” in this context — determining which of the five verifiers has the responsibility to review a WHOIS record — is based on the Registrar’s country or the registrant’s country. The latter is probably more feasible, so that each verifier could specialize in verifying addresses in a given region.) LegitScript does not strongly object to having a single company engage in WHOIS verification, but it may be worth considering whether geographic diversity would make the system stronger.

- The verification companies should have the ability to utilize algorithms to identify potentially improper WHOIS records (e.g., by identifying particular registrars, resellers, IP addresses, name servers, etc. linked to problematic WHOIS records, as well as instances in the WHOIS text of data that appears to be falsified), and also to manually (that is, via human-led analysis) review WHOIS records for accuracy.
- The EWG or another ICANN-approved group should determine processes for when and whether registrants must, for example, provide identification (e.g., at the time of registration or only when challenged), what kinds of identification will suffice, and so forth. The EWG or another group should also determine when an appeal to the determination is appropriate. These are all questions that can be addressed later.
- As with WIPO trademark determinations, the five organizations' determination as to the WHOIS accuracy would be dispositive and binding, unless successfully appealed.
- The five organizations would not be the central repository for all WHOIS data. (Certainly, they would have unfettered access to it, just like any other Internet user — although the Registries and where necessary Registrars should ensure a full, accurate data flow to the verification services.)
- The EWG should view the five verification organizations' services as a way to strengthen the WDPRS process, which could be kept open and available to Internet users at no cost.

In other words, the verification component of what the ARDS would have been charged with is a solid concept and should be retained. The general outline above is intended to be just that — a general outline — and additional details would need to be worked out. However, the fundamental structure above appears to both be consistent with the new RAA and other ICANN requirements and responsive to the EWG's charge to improve accuracy and access to gTLD registration data.

2.3 **Privacy Protections**

LegitScript supports the availability of proxy protection services in appropriate circumstances. We recommend the following approach:

- First, as a general principle, proxy WHOIS services should be available to non-commercial registrants only. It should not be available to businesses or entities conducting commercial activity over the Internet, or for educational institutions or non-profits, et cetera.
- In accordance with the new RAA, there should be a verification process for proxy services: like Registrars, proxy services should be required to be accredited. LegitScript has observed, on multiple occasions, criminal organizations simply setting up their own “fake” proxy privacy services.
- Clear standards should be set for when proxy services may (and should) release WHOIS information.

2.4 **Redefining Purpose of Accessing WHOIS Records**

The EWG is charged with redefining the purpose of accessing WHOIS records. As noted above, this should not be read to imply a grant of authority for the EWG to tell Internet users what the purpose of accessing WHOIS records *should be*; rather, it should be understood as an opportunity for the EWG to understand *what those purposes are* — that is, to set the groundwork for “improved access” to WHOIS by understanding and documenting the various reasons that Internet users seek WHOIS records to ensure both access and accuracy. Within the universe of *what those purposes actually are*, it is appropriate for the EWG to propose specific use cases that constitute the exception to the rule and are not permitted, such as abusive marketing.

In this context, it is also appropriate for the EWG (or, the ICANN community in general) to seek information, collected on an ongoing and anonymous basis, that provide data as to the reasons that Internet users access WHOIS records. Toward this end, the EWG's report is a good start in identifying various reasons that Internet users may seek to access WHOIS records; however, we urge the EWG to update its report in light of the various use cases described in this letter, as well as other public input.

To effectuate this part of the EWG's mission, we recommend the following steps:

- The EWG should recommend that ongoing data be collected on a voluntary basis from Internet users who access WHOIS records seeking their input as to the reasons for such access. This should merely be a voluntary survey that does not impede access to WHOIS records in any way and that permits but does not require disclosure of the Internet user's identity. These voluntary surveys would be available on web-based WHOIS pages, and automated Port 43 queries could return a line of text encouraging those who utilize Port 43 queries to fill out the survey.⁵
- The results should be made available on an annual basis to the public (including registrars and registries) to continually inform policy regarding WHOIS access and accuracy. This will be valuable data to assist in identifying changes in the reasons that Internet users access WHOIS over time.
- Over time, this data will help ICANN ensure that it has a data-based understanding as to the reasons that Internet users seek access to WHOIS records and, from time to time, conduct assessments to ensure that Internet users' needs in accessing this data are being met.

As a general matter, the EWG should use this opportunity to publicly reaffirm the community's commitment to an open Internet, including "timely, *unrestricted and public*

⁵ Although we're not entirely sold on this idea, it might be worth considering whether this survey could be used in place of a CAPTCHA in some cases on web-based forms.

access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information” — the language in the Affirmation of Commitments.

2.5 Safeguards For Protecting Data

At the same time, there is strong community consensus around the notion that there are a limited number of reasons for acquiring and using WHOIS data that are not legitimate. Examples include acquiring WHOIS records for the purposes of sending unsolicited marketing material, or for monitoring domain name expiration dates for the purpose of hijacking a domain name registration. It is important to note, however, that even the EWG’s report identified “miscreant” cases as the minority of cases: the exception, not the rule. It is entirely within the ambit of the EWG’s responsibilities to identify methods to safeguard and protect WHOIS data from miscreants. We believe that these three cases are accurately captured in the EWG report: domain name hijacking, malicious domain name registration, and mining for spams and scams. It is appropriate for the EWG to consider restrictions to WHOIS records as the “exception to the rule” — that is, although WHOIS will, by default be open to the public, what steps can be taken to surgically target miscreants.

Before suggesting concrete means of reducing access of WHOIS by miscreants for these purposes, however, we note that there appears to be a paucity of concrete data identifying the extent to which this sort of illicit access occurs, both in general, and as a percentage of all WHOIS access. To be clear, there is no shortage of anecdotal information, but LegitScript strongly urges the EWG to obtain rigorous data as to the extent of this problem — data that was not referenced in the EWG report and, to the best of LegitScript’s knowledge, does not exist as of this writing. The only way for the stakeholder community to engage in a cost-benefit analysis is to understand, based on rigorous data and analysis, the extent of the problem.

Accordingly, LegitScript suggests that the EWG should either await the results of research pertaining to the extent of the problem of accessing WHOIS records for illicit purposes, or request an analysis, based on concrete data, of the extent to which — for example — harvested WHOIS records constitute the basis for spam email lists and, if spammers were theoretically made unable to access WHOIS records, whether it would have any measurable impact on spam levels.

2.6 **Thick WHOIS Access at Registry Level**

Finally, it must be noted that while most registries maintain and make available their “thick” WHOIS data, the one registry that does not — Verisign — has most of the world’s domain names (.com and .net, in particular). Although perhaps inconvenient for Verisign, much of what is proposed in this document, in particular involving WHOIS record format standardization and ensuring access, requires Verisign to finally follow the lead of other registries and make full thick WHOIS data available at the registry level. To the extent that the EWG proposal was driven by, or took into account, the inconvenience to Registrars related to maintaining Port 43 and web-based WHOIS access, some of these problems may be ameliorated by Verisign committing to provide unrestricted access to .com and .net WHOIS records.

If this were to occur, LegitScript believes that there would still be value for Registrars to be required to provide Port 43 access, so that the registries do not, for their respective TLDs, become a “single point of failure.”

Conclusion

The EWG was charged with an important responsibility: to “repair” (not replace) WHOIS by “launch(ing) a new effort to redefine the purpose of collecting, maintaining and providing access to gTLD registration data, and consider safeguards for protecting data, as a foundation for new gTLD policy and contractual negotiations, as appropriate.”

However, the EWG exceeded the scope of that mission by proposing a system to replace WHOIS and implement a single global authority with the power and (under the EWG report) mandate to restrict access to WHOIS records, determine which Internet users could access full WHOIS records (or which fields), and audit the subsequent use of WHOIS record data, backed up by the power to penalize users. It gives the ARDS a monopoly over the world’s WHOIS data, and along with the power to license (which also includes the power to not license), a perfect monopoly over that information.

Importantly, the EWG proposal does the exact opposite of an explicit policy requirement: instead of improving access (as also required by the Affirmation of Commitments), it significantly restricts it in moving from an “open-by-default” system to one that is “closed-by-default.”

The consolidation of this much power, and creation of a monopoly, will stifle future innovation, and fails to take into account the various legitimate that Internet users access WHOIS data. Importantly, the EWG has not taken into account the important reasons that some companies redistribute WHOIS data (with value-added services attached to the redistributed data), and the reasons that Internet users find value in the redistributed data — not merely data directly from the original source.

There are, however, alternate, less-intrusive methods that the EWG should consider to achieve its mandate. It would have significant value to launch an effort to standardize WHOIS formats, a *de facto* technical requirement for enabling companies to perform any sort of

automated WHOIS verification. ICANN should release a request for proposals for companies to engage in WHOIS verification, thus identifying specific cases as well as broad patterns of abusive WHOIS registrations. These verification systems should be given the authority to back up falsified WHOIS record findings — not completely dissimilar from the authority that WIPO has in trademark disputes under the UDRP trademark process.

Similarly, registrants' privacy can be protected by proxy privacy registration services, but this should only be available for non-commercial entities, and there should be strict accreditation requirements for the proxy services themselves. To better respond to miscreant-use cases of WHOIS data access, we first urge the EWG to look to the current and envisioned provisions in the RAA and try to resolve the issue at that level. The EWG should also ensure that rigorous data exists as to the scope and nature of the problem, and from there, to surgically target the miscreants and, as necessary, implement any limited restrictions as the exception to the open-by-default rule — not as the rule itself.

Ultimately, the EWG should use this opportunity to recommit the stakeholder community to an open Internet, with the understanding that WHOIS records are not distinct from the Internet — they are an important part of it.

LegitScript appreciates the work of the EWG and the opportunity to submit these comments. Please do not hesitate to contact us should you require any additional information.

Yours Truly,



John C. Horton
President, LegitScript