ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

September 4, 2015

VIA EMAIL TO: comments-rds-prelim-issue-13jul15@icann.org

Re: Preliminary Issue Report on Next-Generation gTLD Registration Directory Services to Replace WHOIS

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as the use of technology grows.

We write to provide our comments on the Preliminary Issue Report on Next-Generation gTLD Registration Directory Services to Replace WHOIS. We understand that at this point ICANN is primarily seeking feedback on the sufficiency of the Preliminary Issues Report rather than a substantive response to the issues that it raises. We are also taking this opportunity to provide substantive comments, because we hope to provide helpful insight into the framing of the Final Issue Report. In any case, we will likely reiterate many of these same points to the Policy Development Process Working Group (PDP WG).

Although the Expert Working Group on gTLD Registration Directory Services (EWG) purported to take a "clean slate" approach to designing a new directory service, the EWG report retains some deep unstated assumptions about the necessity for a directory of registration data at all, and a fundamental misunderstanding of why privacy needs to be built in to domain registration services. Although it is a longstanding practice for gTLD registries and registrars to provide information about gTLD registrants through WHOIS, this practice is not drawn from any ICANN consensus policy, but only from the private agreements that ICANN requires registries and registrars to sign. Thus, ICANN has the power to exempt registries and registrars from the requirement to provide a WHOIS service. Brand gTLDs are a good example of gTLDs for which there is no obvious need for a public WHOIS service; indeed, ICANN is currently proposing removing the requirement for a searchable WHOIS service for the .sharp gTLD.

Looking beyond gTLDs, further evidence calls into question the need for a central directory of registration data. The data as it exists is neither complete nor uniform. This is partly due to persistent privacy concerns. For example, ccTLDs determine their own policies for a WHOIS directory, and some of those policies are more privacy-protective, allowing narrower access to sensitive data than those of the gTLD registries. Additionally, it has never been possible to publicly query the ownership of domains at the third level and below (eg. ssd.eff.org). Nor it is possible to query the ownership of identifiers for web services outside of the ICANN-administered namespace (such as the .onion pseudo-TLDs of Tor hidden services). And a domain name can often be used with permission by parties other than the registrant—yet another way current data does not serve the purposes it is purportedly collected for. As these examples

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

show, it is impossible to bring every user of a domain name into privity with ICANN in order to mandate the use of any proposed new registration directory. This calls into question the efficacy and need for such a global directory.

While we believe there is merit in maintaining some registration data in a central database, primarily for technical purposes, the new Registration Directory Services (RDS) system proposed by the EWG is extremely complex and significantly over-engineered. For example, the proposed "rules engine" for applying local data protection laws would be a massive legal and engineering undertaking, untested and fraught with risk, all for the purposes of allowing the RDS to skirt as close as possible to the edge of such laws as it can get away with. A much simpler solution would be to scale back the collection of data to begin with, and to quash the unreasonable expectations of users who claim a need to access this data.

Based on these observations, we address some of the substantive questions that the Preliminary Issue Report proposes:

1. Should gTLD registration data continue to be accessible for any purpose, or should data be accessible only for specific purposes?

A fundamental principle of data protection laws worldwide is that personal data should only be processed for specific, explicit, and legitimate purposes. Therefore, it should go without saying that registration data that is personal data should be collected and used for specific purposes only. We strongly support the EWG report in this regard.

However, the EWG report does not take a critical look at the purposes that some stakeholders have identified as legitimate reasons for accessing more extensive registration data. The report fails to consider the possibility that the current system has led a wide range of parties that could profit from the use of such data to produce rationales for using it. It is no wonder that registration data has accumulated more and more such justifications over time, when they represent such a rich seam of data. We suggest that the PDP WG should look more critically at the claimed use cases, and reduce the scope of the specific purposes for access to extensive data.

The bottom line is that data identifying the registrant should not be made available in connection with content hosted at a domain, absent a court order. The domain name system is never a good substitute for the legal system in regulating the content hosted at a domain—particularly since such content is often posted by someone other than the registrant.

In addition to disclosures in response to a valid court order, some parties may legitimately need access to minimal registrant data for technical purposes, as explained below. For all other purposes, effective anonymity of the domain registrant should be possible. This reflects today's reality, given the availability of privacy/proxy services and the predominance of false information in the WHOIS database. To accomplish this, ICANN should create a channel allowing the public to communicate with a registrant, and to obtain technical information about the domain such as nameserver IP addresses without a court order, but without revealing any of the registrant's personal information.

On this approach, less personal information would be available than under the status quo without impeding access to information needed for technical reliability. Today, the WHOIS database exposes the personal information of the registrant unless a commercial privacy/proxy service is used, making the cost of such services a de facto tax on the most vulnerable registrants. By narrowing the information that is available to the public, privacy/proxy services will become largely redundant for most registrants, and will no longer present a barrier to access.

2. Should gTLD registration data continue to be entirely public, or should access to some data be limited to a subset of all users?

gTLD registration data should not continue to be entirely public. Just as ICANN must specifically define each purpose for which domain registration services collect personal data, it must also define the people who are authorized to access that data. We have concerns about the complex process that the EWG has suggested to accredit such users. We consider it difficult, costly and cumbersome to define procedures for the accreditation of different classes of user as part of the Registration Directory Service. It is also an unnecessary and unjustified expansion of ICANN's authority. We recommend instead that ICANN limit the subset of authorized users to those for which there is a legally authoritative determination of eligibility, which can be vetted in a much more lightweight process. Such a legally authoritative determination would be a warrant (for law enforcement agencies) or a subpoena (for private litigants). For technical uses (such as the registrant's access to their own domain information, domain name certification, or the transfer of a domain to a third party at the registrant's request), self-authentication of the involved parties is also possible. If neither self-authentication nor legally authoritative determination of a user's eligibility to access data is available, then a user should be restricted to accessing publicly available registrant data.

3. Is gTLD registration data sufficiently complete and accurate, or further steps should be taken to overcome barriers to accuracy?

In our opinion, the accuracy of registration information will improve immensely once the privacy of domain registrants is designed into the system. The lack of privacy protection for registrants is one of the main reasons why accuracy has been a problem. Any accuracy problems remaining in a system designed with privacy in mind will be narrower and more easily addressed. In the interim, the EWG's suggestions for the verification of registration data are overly costly and needlessly complex.

4. Are existing registration data elements sufficient for each stated purpose, or is a new purpose-driven policy framework needed to guide the collection, storage, and disclosure of data elements?

The legitimate purposes for accessing registration data require no new registration data elements. We agree that the data accessible to each class of requesting user should be determined by the legitimate purposes of the use. For example, a physical address may be required in order to serve legal process, but not to contact a domain registrant about a technical problem. We certainly do not believe that "legal contact" details ought to be made available by default, because service of legal process is a purpose for which more extensive accreditation of the user should be required.

5. Is a new policy framework needed to meet gTLD registration data requirements for each purpose in a manner that enables compliance with applicable data protection, privacy, and free speech laws and addresses the overall privacy needs of registrants?

Absolutely, yes. The framework should reflect the "greatest common denominator" of data protection laws in the countries in which accredited registrars operate. This would obviate the need to determine how registrars who are subject to conflicting laws should deal with such conflicts. By adhering to the highest global standards, ICANN can greatly simplify the certainty and predictability of the Registration Directory Service, and do away with the need for a complicated "rules engine" for applying differing privacy standards in different jurisdictions. Any Internet user can opt out of ICANN's management of registration data simply by using a country code TLD, a third-level domain, or an informal proxy. A system that does not protect privacy to the highest global standards will only create incentives for more users to opt out.

ICANN should base its new policy framework on the core concept of no disclosure of personal information without opt-in consent. We note that some country code TLD operators, in jurisdictions with high levels of data protection, already manage their own WHOIS rules in a manner that embeds a similar concept (for example in the Netherlands, users can opt out of the public display of their data). The EWG has suggested that registrants be required to opt in to the use of their data, but across all possible uses and users. We recommend going a step further by allowing a more granular opt-in, whereby the registrant has the opportunity to specify for exactly which purposes they approve their registration data being used.

The danger of a global opt-in is that this may open the door to a "contract of adhesion" approach, whereby every user clicks an "I agree" box when registering a domain and thereby makes all their data available to the public, possibly waiving their legal right that law enforcement authorities or litigants obtain a warrant or subpoena. This is not only unfair, it would likely not meet the requirements of the EU's Unfair Contract Terms Directive.

Allowing registrants to self-determine the availability of their data would also avoid the need for a complex and costly system to verify the status of "at risk" registrants whose data would be more strongly protected. The EWG proposal suggests an independent review board to assess the claims of individuals or groups who claim to be at-risk and granting successful claimants the ability to anonymize their data from the registry and registrar. Although we support the motivation behind this suggestion, it would be cumbersome and therefore is likely to be little used. It would place significant barriers in the way of marginalized user groups who currently use the self-help measure of the use of a privacy/proxy service or informal proxies.

In summary, ICANN must make user privacy a central tenet of any new registration data system. To achieve that goal, any new system should collect the minimum amount of data required for legitimate purposes, and make such data available only as needed to fulfill such purposes.

Respectfully submitted,

ELECTRONIC FRONTIER FOUNDATION

Jeremy Malcolm
Nadia Kayyali
Lee Tien
Mitchell Stoltz