3. In cases where government agencies make allegations of political speech rising to the level of treason or other criminal matters, registrars may be forced to use expedited takedown, depending on the relevant law in the jurisdiction.

Even given these limitations, this service would provide much more security to vulnerable registrants than they currently enjoy, and if the new directory will require enhanced data accuracy and accountability, then a service such as this is required. The following key functions need to be developed:

1.A process needs to be developed to establish criteria for eligibility for secure credentials, starting with the example cases listed above and any others which the ICANN community deems appropriate.

2.Application forms, required attestations, and financial systems need to be developed, all with a focus on ensuring that the identities of the requestors and their agents are protected. In any anonymous system, this is one of the key weak points.

3.An entity such as an independent tribunal or board needs to be struck to evaluate applications for secure credentials. Such a board would evaluate the applications and the attestations of trusted parties such as governments who have authorized name changes, United Nations organizations engaged in the protection of refugees, international associations of journalists etc.

4.Accredited proxy registrars need to be found who would accept secure credentials, and the financial systems established whereby they would be paid.

5.Policies surrounding expedited takedown procedures and other mitigations of abuse need to be developed.

What Happens Next?

ICANN has closed the comment period for the working group's draft report, but there is still a great need for input if this proposal is going to proceed. Remaining questions:

- Is there a need for the service?
- Are there documented cases of abuse that would support this argument?
- Who is willing to lead implementation efforts?
- Are international press and human rights groups interested enough to attest to the validity of claims of reporters or refugees?

Documentation is available at https://community.icann.org/pages/viewpage.action?pageId=40175189

Please Send Input to:

input-to-ewg@icann.org

for further information contact

Privacy Enhanced Identity Credentials For Domain Registrations

Remodeling the WHOIS Directory Service for the Internet

What is the Expert Working Group on gTLD Directory Services at ICANN?

The Expert Working Group on gTLD Directory Services is a first step in fulfilling the ICANN Board's directive to help redefine the purpose and provision of gTLD registration data will provide a foundation to help the ICANN community (through the Generic Names Supporting Organization, GNSO) create a new global policy for gTLD directory services. In June 2013 the EWG proposed a paradigm shift – a new system in which gTLD registration data is collected, validated and disclosed for permissible purposes only, with some data elements being accessible only to authenticated requestors that are then held accountable for appropriate use. The EWG's objective is to reexamine and define the purpose of collecting and maintaining gTLD directory data, consider how to safeguard the data, and propose a next generation solution that will better serve the needs of the global Internet community.

Are there problems with the existing WHOIS System?

For many years, the existing WHOIS system has been criticized by human rights and free speech advocates, because the directory is open. Individuals who did not wish to be contacted were obliged to use proxy service providers of some kind to ensure that their address and contact information was not freely available to all actors on the internet. Those who were interested in contacting all domain holders, such as companies interested in trade mark protection, and law enforcement agencies, complained that there is too much inaccurate information in the WHOIS, and that proxy service providers are not responsive to legitimate inquiries.

The EWG has studied these alleged problems, and is seeking input on a novel approach to the protection of certain endangered groups. Reporters operating in hostile territories, groups such as religious or ethnic minorities, victims of domestic or cultural violence all may have needs to have domain names, but have legitimate fears that if their persecutors demanded to know who was behind a website, their registrar would give up their true identities and contact or banking information. Registrars have genuine concerns about being coerced by certain parties, private sector or government agencies, into revealing confidential customer data with or without proper legal authority. Can a solution be found that does not enfranchise law breakers, yet protects vulnerable groups?

How Could Privacy Credentials Work?

There are various secure credentials on the market, such as Microsoft's U-Prove (http://research.microsoft.com/en-us/projects/u-prove/) and IBM's Identity Mixer (http://researcher.watson.ibm.com/researcher/view_project.php?id=664).

These credentials permit the recipient to prove various attributes, such as that he or she has been recognized and authenticated by a trusted authority, that he has paid for a certain right or service, yet without revealing any personal information about themselves, nor providing any trace-back to the transactions which enabled the attributes. Relying parties have secure cryptographic proof that the entity has the authority they are attesting, without needing to know who they are or how they got that authority. This means that any of the vulnerable parties described above could go to a trusted authority, prove their situation, provide payment for the desired service, and get a trusted credential. They could then take or send the trusted credential to a proxy registration service and get a domain name. The registrar would have no information about who they are, beyond the requisite technical contacts, and would therefore legitimately not be able to respond to requests for personal or address information. Obviously, there are concerns about technical compliance and abuse and we will discuss the mitigations of these risks below, but the key point is that registrars and registries will no longer be the bearers of the risk and responsibility of identification of vulnerable individuals to their aggressors.

Operational Issues

In order to unpack the issues and risks associated with such a service, we have explored a few of the use cases below:

1. An information requestor wishes to establish the true name or address of an individual, for what they represent as legitimate purposes (allegations of trademark abuse, desire to buy or sell a domain name, wish to investigate product safety, etc.) Note that in a life and death situation, a registrar is in a difficult position when trying to determine whether the requestor is coming in under false pretenses, and staff cannot be expected to understand what kind of unknown threats people may live under, particularly in cases of identity change.
2. A requestor approaches the proxy registrar alleging some kind of criminal or libelous activity and demands to take the website down. In these situations, the due process procedures being developed for Proxy and Shielding Service Operators should be followed. In some instances, such as criminal activity, expedited takedown may be granted for these websites.