A possible global process for collection, storage and access of Registrant Data

Background

A Domain Registrar, either directly or through a Reseller collects a Registrant's personal data at the time of registering a Domain Name. With over 300 million domain names registered worldwide, this becomes Big Data as a collective.

ICANN coordinates the allocation of Domain Names (and associated Number resources), but does not make "rules" concerning the handling of Registrant Data, which is valuable to the Registrant who parted it with the Registrar/Reseller in Trust.

Due to the cross border nature of the Internet, a Registrant in one country, say, India, registers a Domain Name which on the Top Level is delegated by ICANN, a non-profit Corporation Registered in the State of California, United States, to a Registry operating from, say, Gibraltar, who appoints a Registrar based in Germany, who in turn appoints a Reseller based in South Africa who registers the Domain Name to the Registrant based in, say, India. The Reseller retains some of the Registrant Data, and parts with part of the data (or a copy of all Data) to the Registrar, who passes on a part of the Data to the Registry, and a certain mandated components of the Registrant Data gets published in the whois database for public access. (This has not been described with schematic accuracy, but in general it works more or less in this manner at present)

The Registry, Registrar and the Reseller might be using the Registrant Data for their own essential commercial operations, or at times sharing it with third parties by commercial arrangements. In addition, there are periodic requests from the Law and Order Agencies for access to the Registrant Data. Complications arise when one country demands access to Registrant Data stored outside its jurisdiction, and further complications arise when the data so released pertain to the citizens of another country. Also, "the problem of cross-border data requests arises when one government's laws compel the production of information while another government's laws simultaneously forbid that same production."

It can not be denied that some of these Law and Order requirements are in the National or Global public interest, but the focus of this paper is on possible excesses or abuses.

A possible global process for collection, storage and access of Registrant Data:

If some data is held by Registrar, some by Registry and some by the ISP, there may be a way of streamlining this by modifying the manner in which Registrant data is gathered and stored at the time of registration. Some attention to the VISA/MASTERCARD method of collecting and handling credit card information could help ICANN come up with a streamlined design for handling Registrant data.

If such a model is to be emulated, a Registrant going to a sub-Reseller going through a Reseller going through a Registrar under a Registry would gather the Registrant data on a secure form interjected by an operator like Verisign. ‘Verisign’ here is not to be confused with Verisign the Registry, or Verisign the RZM operator, but that division of Verisign which serves the secure form in credit card transactions. In the Domain registration scenario, ‘Verisign’ would, by a secure protocol, interject a registration form on the Reseller interface, that would be a secure form independent of and regardless of the insecurity of the Sub-Reseller's webspace. In DNS, this could indeed be a verisign form or an IAB/IETF/ICANN designed secure form, or a form designed by the ICANN Technical expert volunteers from the Community, or even by any other commercial contractor designated by ICANN. This verisign form (I call this the Verisign form, for illustration. Not implying that the system peculiar to DNS must only be designed by Verisign. However we could continue to refer to this as the 'Verisign form' for the purpose of this discussion) could then be used to collect:

a) all Registrant data and then automatically distribute the basic data back to the Sub-Reseller and Reseller, basic + quasi-sensitive data to the Registrar under whom the Reseller operates and retain a copy of the above + Sensitive data with the Registry, while ultra-sensitive data, if any so categorised by any name, together with all of the above would stay only with ICANN. (the categorization of data as basic etc is arbitrary. This is a generalized description of how it would work, there may be existing classes and sub-classes or ICANN may come up with suitable sub-classes of Registrant data)

Or, optionally,

b) The Sensitive and Ultra-sensitive user data alone could be gathered by the Verisign form after the basic data is collected by the Reseller in his own form that may be shared with the Registrar.

Any of the above options would prevent Registrant data abuse in a situation where there are a multitude of Resellers. If such a process could be designed and implemented, the Resellers would retain the basic contact information for them the opportunity to maintain contact with their customers, Registrars would get a copy of whatever commercial data that they require from the Resellers or from their direct customers, the Registry would still retain most of the data with a copy for the ICANN in a database, and only ICANN retain the ultra-sensitive data, if there is any part of Registrant data is ultra-sensitive by any other name.

Law and Order Requests:

Such a new process would require a system of handling Law and Order Requests. ICANN could facilitate/ help to create/ or actually ‘own’ a well designed process involving a highly ethical team of community members to screen requests from Law and Order authorities anywhere to access data, and to determine what portion of data to be released or allowed access.

The caution needed here is that such a system may have to be well thought of, the privacy and security concerns to be examined in extensive detail, the commercial privileges

concerning Registrant data prevailing among Resellers, Registrars and Registries have be examined, the ability of ICANN / Internet Community to judge the validity of Law and Order requests and the strength of ICANN to deny some requests if deemed necessary - all these aspects have to be examined in detail.

If the question "where does data reside" extends beyond Registrant data, the answer would be far more complicated. That would draw the Internet Community's attention to questions concerning content in a very interesting way.

The details: (with some repetion)

1. What I suggested was use of this form as a globally central system of collecting all Registrant data from Registrants through any Reseller/Registrar, across the world, across all gTLDs. Sounds a bit scary, but could be fair.

2. The data collected by using the 'Verisign' Domain Name Registration form would be 'owned' by ICANN, the term 'owned' implying responsibility.

3. By an automated process, the data entered by the Registrant as received in total by ICANN could get classified according to predetermined and gradually increasing levels of privileges between the Reseller who registered the domain name for the Registrant (for example, the information gathered from form fields 1-5), the Registrar under whom the Reseller operates (for example, the information gathered from form fields 1-5 + fields 6-7), the Registry who operates that TLD (for example form fields 1-7 + form fields 8-10) and ICANN (all form fields 1-20). Without any discernible delay, ICANN Storage returns the information from 1-5 to that Reseller, 1-7 to that Registrar, 1-10 to that Registry and retains a copy of all of 1-20 in its highly secure storage with community oversight.

4. The same method could be used to determine what information gets published on whois. (for example, it could be agreed by the ICANN community that form fields 2, 4, 5, and 7 gets published in the public whois database.

5. If there is agreement that Law and Order Agencies could UNIVERSALLY access an additional portion of the Registrant data over and above whois, WITHOUT the need to make a request or produce a warrant, we could agree to transfer a copy of all form fields in whois (2,4,5 and 7) + the information gathered in form field 14 and 17 to, lets say, to the Interpol data base.

6. Apart from the Domain Registration form, for Law and Order requests, as in cases where the FBI or the police in any other country require specific information, a similar, possibly even a relatively less transparent form could be designed to allow the Law and Order Agency

to document their requests to ICANN to release information. This could be the form to fill in, for FBI to make a request for all Registrants' 1-20 data on .terror, or for a culturally aggressive Government to make a request for all Registrants' 1-20 data on .wildsex. Or for the Law and Order Agency of another country to make a more specific request for 16-18 of a particular domain registrant.

7. This relatively less transparent form as described in (6) above, would be visible to the Trustees of Registrant Data, (loosely we could say at this stage, for the purpose of illustration, this could be a Board or Council of 30 or more Nominees by ICANN, ISOC, IETF, Privacy Organizations, Government representatives from such Departments as Department of Culture, other Civil Society organizations of relevance, Trustees to be drawn for their individual propensity to be trusted and for their ability to judge the merits of Law and Order requests). The trustees would make the Law and Order requests transparent only in extremely difficult cases, for example in the case of a request for 1-20 data on .sex by a country known for culturally extreme positions, request denied, and the Trustees politically challenged.

8. The relatively less transparent form as described in 6, could also be so designed as to accept "a secret law enforcement request (warrant or other legal document), and manage the expiry date of the secrecy of the warrant". The idea of designing this second Law and Order Access form would be to "to deal with law enforcement's demands that their investigations be private".

9.Even the doors opened on specific requests would be in such a manner as to ensure that the Law and Order Agencies do not "go for a romp in the system, for an indefinite period."

10. Such a collection, Storage and Request for Access system, in combination, would make it rare for ICANN to consider, or even reasonably deny, excessive backdoors for Law and Order access, not to FBI, nor to Scotland Yard, not to the Interpol, not to the CBI of India.

This proposal could be discussed, or even tested, by ICANN delegating a test domain, .test, or .dnsdata, to itself, make it somewhat privately operational, assign roles as "Registrars", "Resellers" to volunteers from Business, ask Community participants to take up the role of Registrants and register .test names, first to test the technical feasibility of such a system, then to determine what personal data is absolutely needed, what is commercially desirable, what is needed for National Security, and what safeguards are needed for sharing this data between the Registrar and Registry, and what would be routinely made available to Law and Order, what part of the data would be released on requests and how, for what time frame,

and what would be denied. This test TLD could also be more vividly used to simulate content regulation scenarios.

Sivasubramanian M