From: User
Date: Sunday, January 28, 2018 at 15:49
To: "gdpr@icann.org"
Subject: [Ext] WHOIS Models Feedback

Dear Sir/Madam,
I write with regard to the feedback requested on the three proposed WHOIS models. I am an individual who is closely involved in internet investigations but am making a personal submission as I am not in a position to speak on behalf of my organization.
Whilst I appreciate and support the need for protection of personal data, it is important that the very protection measures designed to protect the public do not actually assist those seeking to commit crime or other forms of abuse online. Having read the proposal in detail I am very concerned that all three models with only provide more barriers to the effective investigation of online abuse. My main areas of concern are as follows:

1) Removal of fields from the Public WHOIS record where they contain Personal Information.
All three models remove certain fields from the public WHOIS record, with models 2 & 3 removing all personal information relating to the Registrant. When investigating reports of online abuse one of the very first enquiries is a domain WHOIS check to see if any of the details listed match up with previously cases or known offenders. It is acknowledged that where online abuse takes place the true identity of the offender is rarely listed – however links between cases can be made through the use of names and contact details. Under model 1 the removal of the Registrants phone number and email address is likely to make it more difficult to link jobs together and identify the true identities of offenders, however this is still far less worrying that models 2 & 3 whereby all Registrant personal information would be removed. Therefore whilst model 1 will still have a negative impact on online abuse investigations it if preferable to models 2 & 3.

2) Data Retention

Where online abuse is carried out a domain name may only be used for a matter of days or weeks. This means that from the perspective of the retention periods listed in the models we would only have somewhere between 60 days and 2 years from the end of the registration to subsequently obtain the personal information from the Registrar/Registry. Where the Registry/Registrar is in the same jurisdiction as the individual making the request then all of these timescales are manageable (even if the 60 days would could be challenging) provided the investigation starts quite soon after the offence taking place, however when you add in the international element where the requester may well often be in a different county from the Registry/Registrar then the 60 days retention period would make it almost impossible to make a request under model 3 where legal due process would need to be followed. The international nature of the internet would mean that such cross jurisdictional enquiries would likely be common place and therefore model 3 would have a significant negative impact on the ability to investigate online abuse.

3) Access to Non-Public WHOIS data

Currently WHOIS data can be searched manually or programmatically in a matter of seconds which returns both personal and non-personal information. This ability to obtain this full data set quickly enables the prompt linking and prioritisation of cases of online abuse. As mentioned previously whilst it is acknowledged that where a domain has been registered to facilitate online abuse it would be expected for the provided details to often be false, any fake details provided can still be used to link crimes, prioritise workloads and identify the true offenders. Any barrier or restriction of the ability to gather such information in a timely and automated manner will likely be a significant hindrance to the ability to effectively investigate online abuse. Model 1's self-certification model is the least harmful of the three models, however as it is up to the Registrar/Registry to approve the request there is no guarantee that a legitimate request would be approved or that the request would be dealt with in a timely manner. In any case the process would be significantly longer that the current model and therefore would definitely negatively impact investigations.

Model 2's Formal Accreditation initially seems like a reasonable idea however I

have severe concern around how this would work in practice. Who would accredit the organisations/individuals? Would Registrars/Registries be mandated to accept the accreditations or could they refuse those accredited by certain accreditors? I am afraid I do not see how the formal accreditation process would work in practice.

Model 3's legal due process has already been shown not to work in the international sharing of data from other industries. Where data is requested by one country (e.g. Germany) for a provider in another country (e.g. Canada) then the provider will almost always say that they will only accept legal documents from their own county (i.e. Canadian Court Orders). This would then require the requestor in Germany to ask for an International Letter of Request (ILOR) to ask the Canadian authorities to obtain a Canadian court order for the data. This whole process takes a very long time (5+ months is common), is very labour intensive and only works where there is a Mutual Legal Assistance Treaty (MLAT) in existence between the two countries. Therefore whilst legal due process may seem like a very sensible way to go, where a geographical & political boundary exists between the requestor and the Registrar/Registry then this process would almost certainly be a huge barrier to the investigation of online abuse.

Summary

Whilst model 1 will still have a fairly significant negative impact on the investigation of online abuse it is far less catastrophic to investigations that either of models 2 & 3. Please do not consider either models 2 or 3 until you have fully understood the impact of such changes by discussions with investigators of such offences from a wide range of countries. **If one of these models must be selected then please select Model 1**.

From a concerned investigator