**Law Enforcement Responses**

|  |
| --- |
| **1. Do you feel this definition is suitable in the context of this Review?** |
| A | Generally yes |
| B | Yes, but... |
| C | Yes, this is an appropriate definition for this context.  |
| D | Yes |
| **2. If not, do you have any suggestions/changes or additions?** |
| A | Law Enforcement (LE) are generally not responsible for maintaining or coordinating laws. We act as a general deterrent and enforce laws by investigating breaches and bringing offenders before the court system. This is done in line with government policy and the public interest. |
| B | ...keep in mind that there are many private initiatives by private entities that are doing a lot of great work in countering abusive behaviour on the internet. These organisations also make use of public WHOIS data. |
| **3. Does WHOIS policy and its implementation meet your needs?** |
| **a. If so, are any aspects of the WHOIS service more important than others?** |
| A | Generally, yes. Reverse IP checks, generic subscriber details and abuse contact details are particularly relevant to LE and used on a regular basis. |
| B | The registration date in the domain WHOIS is a very useful information: “Fresh” domains are more suspicious than long established ones.Network WHOIS provides leads to physical infrastructure and is therefore, from a technical point of view, more important than domain-WHOIS. |
| C | WHOIS data meets law enforcement needs when it is properly maintained, reliably accurate, and complete. In its current state much of the WHOIS data is inaccurate, incomplete, or intentionally false. All WHOIS information is important and relevant to law enforcement investigations.  |
| D | Accurate WHOIS information is a very important tool for law enforcement but false, out of date and inaccurate records are a barrier towards successful criminal investigations. WHOIS data is often the only way law enforcement can investigate criminal offending that occurs via the Internet so it is therefore vital the data is accessible and accurate.The email Address - this is accurate information as it is one way to control ownership of the domain (e.g. Registrar notifications, UDAI).The Registrar information – this is important as they can be the next contact point for false registrant details, potentially the Registrar can provide law enforcement with additional information such as billing records and connection logs. |
| **b. If not, what issues or problems have you encountered with WHOIS?** |
| A | When dealing with individual registrars, we often do not receive individual subscriber details as required. In addition, proxy services pose a problem for LE (addressed in a later question). |
| B | Criminals use fake-WHOIS or proxy/privacy-registration (with STILL fake data behind) which makes determination of the competent jurisdiction difficult. |
| C | WHOIS is inaccurate, incomplete and often, non-existent due to proxy/privacy registrations.  |
| **4. How important is WHOIS for law enforcement activities? Are there alternative data sources that you could use?** |
| A | Given the speed at which it is possible to register domains, change C&C servers and otherwise obfuscate electronic trails and information, WHOIS is crucial to the activities of certain LE groups. There are alternate sources that could be used, but none as comprehensive, straightforward or convenient.  |
| B | WHOIS is very important. It provides first leads. If accurate, jurisdiction can be determined and criminals may be found – if inaccurate, Domain can be revoked (violation of T&C). |
| C | WHOIS data is vital as to internet law enforcement investigations. WHOIS is an important tool in the initial phases of investigation. It helps determine probable cause for some cases and the location of the crime and criminals. While there are alternative sources, they are not as comprehensive, international and easy to obtain in a quick and efficient manner. The time routinely invested by law enforcement to validate WHOIS data that may be false, unavailable, incomplete, or proxied impedes investigations. |
| D | As per Q.3 - WHOIS records are vital to criminal investigations; a search of the WHOIS database is generally the first enquiry made by law enforcement towards identifying cyber- criminals and is often the only available enquiry that can be made. An alternative source may be DNS records; that is (1) email MX records (2) name server NS record and (3) web hosting A records. Unfortunately DNS record are often hosted in jurisdictions that lack reliable law enforcement or often are held by organised criminal groups, DSN records therefore are not always accurate, or made available to law enforcement.  |
| E | ICANN’s work with regard to the registration of persons responsible for websites (registrants) is of crucial importance.This data is often the fastest and only way for the police to investigate the persons responsible for websites being subject to an investigation. Investigations of websites are, for example, conducted against sites with illegal content, including child pornography, sale of drugs, weapons and stolen property. In order to quickly target these investigations, it is important that the data is accessible and accurate. In addition, it is essential that the data is updated continually and checked for accuracy. |
| **5. What changes to WHOIS would you recommend to better meet the needs of law enforcement? Please provide reasons.**  |
| A |  In particular, when LE requests a domain block (or similar) through the various registrars, which happens on a regular basis, the response back varies greatly. Many are actioned very slowly, while others are not actioned at all. The registrars should be required to act upon LE advice within a given time frame or face fines etc. Feedback on results would be of assistance as well. |
| B | “plausibility-check” of entered WHOIS-data can lead to better quality of data and might prevent fraudulent domain registrations. |
| C | Ensure WHOIS is accurate and complete, and open to all. As described above, the WHOIS is an excellent tool for triage investigations and provides good information on domain names, and associated information. It is the source of many clues in the beginning stages of an investigation. Without public and accurate information, law enforcement would be forced to pursue legal process for each and every piece of domain name information, which would overwhelm not only the international criminal and civil justice system, but the entire domain name industry. Therefore, enforcement of current ICANN policies and stricter requirements for entities involved in any type of e-commerce activity are recommended to provide for the investigative needs of law enforcement. In addition, prohibiting the use of proxy services for any domain used to sell a regulated product, such as pharmaceuticals, medical devices, dietary supplements, and tobacco products, would assist the accuracy of the WHOIS data and the ability for law enforcement to utilize WHOIS data in investigations. |
| D | (1) Public display of the registering IP address, date time and relevant time-zone. This will give law enforcement a potential line of enquiry in the event the WHOIS records are inaccurate (2) Accurate and confirmed record of the registrant’s physical address – this will provide another potential line of enquiry for law enforcement.  |
| **6. In your view, how well is ICANN performing against these requirements? Please provide reasons.** |
| A | Overall, ICANN and its associated registrars perform quite well against the AoC requirements, although access to some details is often difficult to obtain. Billing information is an example of that. Proxy services add a further layer of confusion and often present difficulties for LE. |
| B | ICANN just recently started to “de-accredit” registrars for non-compliance (before, there have only been cases of de-accreditation for non-payment of charges). |
| C | Since WHOIS is regularly incomplete, inaccurate and non-public, ICANN is not fully performing its duties. In addition, the continued issue of not being able to quickly identify the true owner of a domain name, indicates a need for improvement in this area.  |
| D | The WHOIS database contains many inaccuracies. Presently there is insufficient due diligence conducted towards ensuring records are accurate and criminals are quick to take advantage of this. The value of any database is in its accuracy.  |
| E | The current WHOIS Policy is not considered to be effective enough to validate and ensure ongoing control of registrants’ and other person’s authenticity. This data can be used for the identification of suspects. As such, it is still easy to enter fictitious or inaccurate names in creating and operating websites. |
| **7. Do you have specific examples of effective ICANN policies or implementation activities, or suggestions of how ICANN could improve its performance?** |
| A | No |
| B | ICANN should be able and willing to enforce its policies. WHOIS policy seemed long to be just a recommendation whose non-compliance didn’t have consequences for registrars. |
| C | ICANN should enforce its own contractual obligations with registrars, require that registrars, registries and resellers, collect and verify the appropriate WHOIS information. ICANN needs to increase staff levels if there is any hope that compliance can be enforced. |
| D | Adoption of the Law Enforcement Due Diligence Recommendations for ICANN. |
| E | There should also be a fast and effective consequence of missing or false data. Several times, the [responding LEA] has experienced it being impossible to identify the persons responsible for the websites resulting in the investigation being called off or carried out by other means. Moreover, it would be desirable to have access to payment information, etc. in order to enable useful and effective investigations. |
| **8. How can ICANN balance privacy concerns with its commitment to having accurate and complete WHOIS data publicly accessible without restriction?** |
| A | ICANN do not verify the details of the various subscribers for whom they provide a service. In order to balance privacy concerns with LE requirements, they could provide a separate verified record accessible by LE only. Warrants etc are generally not able to be readily used to access such information due to the jurisdictional issues. A separate way for LE to access relevant records could be created. |
| B | Define policy about usage of privacy/proxy-services Provide accreditation for privacy/proxy-services similar to registrar accreditation. |
| C | Private individuals engaged in non-commercial activity can apply to opt out of having their WHOIS information published, where the burden of proof would be on them. Anyone engaged in commercial activities should not be protected. As mentioned above, the use of proxy services should be prohibited for any entity engaged in e-commerce activities as well as for any domain used to sell a regulated product such as pharmaceuticals, medical devices, dietary supplements, and tobacco products. Anyone engaged in the legitimate sale of regulated products should have no need for privacy/proxy services. |
| D | Good quality WHOIS records must be retained but do all WHOIS records necessarily need to be publicly visible by default? Is there potential for law enforcement to access specific WHOIS data via a means, other than the open public WHOIS database? Could legitimate and verified law enforcement to access deeper WHOIS records upon a recognised, template, information request form? Any such process could satisfy the respondent that the request is authentic and in relation to a criminal investigation. The challenge will be to make any procedure timely enough to be effective; the current International Mutual Assistance Request procedures are completely antiquated and unable to facilitate such requests.  |
| **9. Are you aware of any efforts by country code Top Level Domain operators within your jurisdiction to find a balance with regards to WHOIS between potentially conflicting legal requirements for data protection, privacy and data disclosure?**  |
| A | No |
| B | In our jurisdiction, all data that has to be published needs to be defined by laws and bylaws. Email-addresses have been removed from the public WHOIS to counter spamming. |
| C | Registrant WHOIS data is a requirement in .us, as the database is considered a public resource.  Proxy or privacy services are not permitted in .us. The Europeon Union E-Commerce Directive, enacted in 2000, implemented transparency requirements for e-commerce businesses to self disclose various information about ownership and business location.  |
| D | .nz covers off the requirements of data required, WHOIS information etc in their policies.  The .nz policies are online at <http://dnc.org.nz/policies>.  One of the requirements is that registrants have to accept the terms and conditions of the registrar in order to register or transfer a .nz domain name.  Core requirements of the terms and conditions used by registrars are defined and the T&C's have to be approved by the Domain Name Commissioner as part of the authorisation of registrars process.  Regular checks are then done to ensure the correct version of the T&Cs are being used and that registrants have to accept them. Part of what the registrant accepts in the T&Cs are that they will comply with the .nz policies.  These policies include specifying what data is required, what will be publicly displayed in the WHOIS and what the obligations on registrants are in respect of the information in the register.One of the things required is 'contact details' and these include address and phone number. It is a requirement that the registrant can be contacted using the information in the register. |
| **10. What is the importance of WHOIS data being publicly available without restriction?** |
| A | To allow internet users to know who they are dealing with and create a level of trust in online transacting and searching. It is a thin layer of protection to the average internet user. |
| B | Providing contact address for issues with the relevant internet-resource. Indicating possible jurisdiction. “Know your business partner”: Possibility to check on registrant of domain name. |
| C | Very important, to ensure that WHOIS data actually assists law enforcement investigations, as opposed to impeding or halting them. In addition, consumers who purchase regulated products deserve transparency regarding the operation of the domain name/website they are purchasing from. It is the opinion of law enforcement that those involved in illegal activities and domain abuse are already taking advantage of proxy services, and will only further abuse the public if access to WHOIS is restricted. Legitimate businesses should have no issue with transparency. It is those individuals and entities engaged in illegal activity that are generally the most concerned about the availability of proxy services. The ability to hide ones identity in the global e-commerce marketplace creates and environment that allows illegal activities to flourish. It is imperative that law enforcement is able to identify the who, what, where of domain name operators immediately in order to effectively investigate.  |
| D | WHOIS is a public service related to the domain name registration and its operation and as such accurate information should be provided that allows contact with the registrant and technical contact in respect of the domain name and its operation.When the WHOIS output contains sufficient information, it allows someone who is considering doing business with an organisation or person to check out the details held. If it is clear from the information provided that the details are false then that might assist the person in making a decision as to whether to do business through that site or not.From a law enforcement point of view the issue is more about access to accurate records, be they public or not. |
| **11. How should ICANN address concerns about the use of privacy/proxy services and their impact on the accuracy of the WHOIS data?** |
| A | By creating a regime whereby proxy services have to provide details of the various persons they act for to the registrars, and tightly controlling who may act as a proxy service provider, this may mitigate some of the issues around proxy users. |
| B | Provide accreditation for privacy/proxy-services similar to registrar accreditation. |
| C | It has been shown that criminals do use proxy and privacy registrations to hide their identities and that the privacy/proxy services can be abused. To that end any entity engaged in e-commerce activities must be required to disclose name, physical address, city, state, zip code, and geographical area that is located in the country and state of the registrant’s residence or primary business. The location of the address is important to establish legal jurisdiction and is another means used by criminals to hide their identities and impede investigations. Specifically, the use of proxy services for any domain used to sell a regulated product (such as pharmaceuticals, medical devices, dietary supplements, and tobacco products) should be prohibited in an effort to protect public health and safety. |
| D | They should look at measure to prohibit proxies, or at least have a way to compel the information to be released in specified situations. There are some scenarios where not displaying the registrant’s information is appropriate, for example, if someone has a Family Protection Order (or similar) and displaying their information may put them at risk of harm. These circumstances however should be relatively rare and a way of managing these can be developed, perhaps on a case by case basis, without providing an anonymous service for potential fraudsters and other criminals to hide behind.   |
| **12. What is your view on the use of privacy and proxy services by registrants?** |
| A | Generally speaking, site owners engaged in legitimate activities would have no need of them, so those who do operate through proxies should be treated with suspicion. ICANN needs to more tightly control the use of such services, and ensure verifiable details can be obtained from the relevant registering body. At the least, domain registration systems that provide privacy protection mechanisms for Domain registrants should have a physical address and real person point of contact as mandatory. LEA must be able to ascertain the registrant details for any suspect domain that is involved in an investigation and therefore may require contacting a physical individual or contact address. The [responding agency] are aware of an online company providing a domain privacy protection service that actively promotes that they are uncontactable by any other means except through their website. This service is regularly utilised by criminals to register criminal based domains. Standards by which all domain registration providers providing this type of service are required to adhere to in regards to the provision of information to LEA, will assist in the investigation and shut down of criminal domains more effective. It may also assist in preventing criminals from registering their own online privacy protection service that can be utilised by other groups. |
| B | It’s a tool to remain anonymous which may be useful and justified in certain limited cases. Nowadays it’s mostly used by people who run illicit or “immoral” business and fear repression by law enforcement or private “cruisaders”. |
| C | If an entity is engaged in legitimate business activities, then a proxy service should not be necessary. |
| D | Those doing business on the internet should not be able to hide behind proxy services.  As stated in the previous question, there might be some situations where it’s appropriate to conceal the details of a third party but this shouldn't allow proxy registrations as a 'business' where someone is making money by providing a service that allows unscrupulous people to avoid being public. Proxy services play right into the hands of organised crime, they hide all their business behind them and this is a huge issue, not only for law enforcement, but for the wider internet community as a whole.  |