1. Stakeholders key
2. Applicable laws - Definition & Overview of received comments
3. Producers and Maintainers - Definition & Overview of received comments
4. Law Enforcement - Definition & Overview of received comments

Annex A – Received comments on definitions in full

Annex B – Full results of Law Enforcement Survey

**1. Stakeholders Key:**

|  |  |  |
| --- | --- | --- |
|  | **Name** | **Background** |
| **BC** | Business Constituency | Represents both large and small commercial entity users of the Internet. |
| **CAUCE** | Coalition Against Unsolicited Commercial Email | An all-volunteer consumer advocacy group, defending the interests of the average internet user. |
| **ECTA+M** | European Communities Trademark Association & Marques | Main role as a spokesperson on problems relating to the use and protection of industrial trademarks / designs in the EU. |
| **IPC** | Intellectual Property Constituency  | Represents the views and interests of owners of intellectual property, with particular emphasis on trademark, copyright and related intellectual property rights. |
| **RSG** | Registrar Stakeholder Group | Working to ensure the interests of registrars and their customers are effectively advanced.  |
| **VOL** | Volodya | Independent person. OS search suggests he is a Moscow-based coder called Vladimir PRUS (Volodya is diminutive form of Vladimir). Volodya has posted to the ‘free net’ forums, showing an interest in privacy and freedom of expression.  |
| **LEX** | Lexinta | Intellectual Property Attorneys based in Belgium |
| **RG** | Ronald Guilmette | An anti-spam activist and frequest user of the Whois Data Problem Reporting System. He has been quoted in articles in Krebs on Security on problems with Whois Data.  |

1. **Applicable laws**

**Definition:** Includes any and all local and national laws that regulate and/or control the collection, use, access, and disclosure of personally identifiable information. It may also include other relevant legal obligations, including U.N. Universal Declaration of Human Rights and the U.N. Guidelines for the Regulation of Computerized Personal Data Files.

**Overview of received comments[[1]](#footnote-1):**

Seven parties provided feedback.

BC group supports the definition as it stands.

In other comments; the definition lacks precision on the following points;

* Lack of clarity when local laws and UN declarations conflict **(RSG & VOL).**
* UN guidelines are not legally binding **(RSG & IPC).**
* Currently, it only applies to registrant privacy. If the definition was to be used in a wider sense, there are areas other than personal data where laws might apply. For instance; child exploitation, fraud prevention, regulation of drugs, intellectual property etc **(CAUCE & ECTA+M)**.

There is also a pre-existing ICANN procedure which covers WHOIS conflicts with privacy law (See <http://www.icann.org/en/processes/icann-procedure-17jan08.htm>). Consideration should be given to this, and how it applies **(IPC).**

An alternative definition was given as:

*Includes any and all locally applicable laws and legislation in force that regulate and/or control use, access, and disclosure of personally identifiable information. It may also include other relevant legal requirements, including but not limited to U.N. Universal Declaration of Human Rights etc* **(LEX).**

1. **Producers and Maintainers**

**Definitions (approved 2 March 2011):**

A.   Producers:  The individuals or organizations supplying contact data for inclusion into WHOIS data.

B.    Maintainers: The WHOIS Review Team proposes to subdivide this category in to:

\* Data Controllers:  Individuals or organizations that define the data to be collected, require its release, and govern its use.  May or may not be directly involved in these functions.

\*  Data Processors:  Individuals or organizations engaged in the collection, storage, and release of data, according to the terms defined by the Data Controller.  They do -not- determine the nature or use of the data that they collect or maintain.

**Overview of Received Comments[[2]](#footnote-2):**

Five parties provided feedback.

Two groups support the definitions given **(BC & RSG)**.

In other comments; there is a question as to whether definitions of these terms are needed, given that they are not referred to in the AoC, the WHOIS RT Scope or the WHOIS RT Roadmap **(IPC)**.

The definition of ‘producers' does not recognise the different parties that may fill this role, and their differing objectives / perspective which may have an impact **(CAUCE & ECTA+M)**.

The inclusion of ‘may or may not be directly involved…’ in the definition of ‘maintainers’ has led to some confusion, and again it was felt that roles within the definition may have been grouped too generally. It was also felt that the use of terms from EU data protection legislation may confuse some parties  **(CAUCE)**.

The team also need to recognise that EU data protection rules apply only to individuals; businesses and organisations do not generally have a right to privacy **(ECTA+M)**.

1. **Law enforcement**

**Definition (adopted on March 2)**

Law Enforcement shall be considered to be an entity authorized by a government and whose responsibilities include the maintenance, co-ordination, or enforcement of laws, multi-national treaty or government-imposed legal obligations.

**Examples**

|  |  |
| --- | --- |
| **Included**  | **Excluded**  |
| Government executive agency (like police)  | Lawyers  |
| Secret service  | Intellectual Property industry  |
| Military intelligence service  | Abuse fighters  |
| Regulatory authority  | Network Operator  |
|   | Private or commercial organisations  |

**Overview of Received Comments[[3]](#footnote-3):**

Six parties provided feedback.

One group supports the definition as it stands **(BC)**.

In other comments; it was felt the definition was too broad, with no distinction being made between sworn officials and individuals working for private enterprise. There were also questions around whether intelligence services and military services should be included **(CAUCE)**. Additionally, the concept of civil proceedings was raised – would parties involved in those be classed as law enforcement if they are enforcing law? **(ECTA+M)**

One party stated they could not comment on the definition until they knew what access LE would get **(RG)**.

An alternative definition was suggested:

*Individuals who (1) have been sworn or commissioned as a law enforcement officer by a government agency of competent authority; (2) are charged with upholding the general criminal laws of an applicable jurisdiction, including having power to arrest; 3) typically have received specialized peace officer training* (see submission for examples); *4) who normally receive tangible official signs of their role such as police uniform or official credentials.* **(CAUCE)**

**Annex A**

|  | **Applicable Laws** | **Producers & Maintainers** | **Law Enforcement** |
| --- | --- | --- | --- |
| **Coalition Against Unsolicited Commercial Email (CAUCE)** | The definition is relevant if focus is solely on registrant privacy. Since this aspect must be balanced against the need to protect citizens, the definition should be widened to recognize the applicability of all criminal and civil laws on WHOIS policy, including laws against child exploitation and child pornography, against obtaining financial information by deceit/“phishing”, against spreading malicious software, against online sale of controlled drugs, against IPR violations, against various fraudulent schemes and against spamming activities.  | The definition of “producers and maintainers” mixes parties and roles with different perspectives and interests. A “producer” may be 1) the registrant; 2) a proxy; 3) a registrar or hosting company; or 4) a registrations service provider acting as a contractor or agent for the registrar. These roles may also change over time. The definition leads to confusion and so does the definition of “data controllers”, especially the final part of the definition. | The definition does not distinguish between sworn law enforcement officials and other entities with the mentioned obligations. Law enforcement officers should be narrowly defined as individuals: *1) who have been sworn or commissioned as a law enforcement officer by a government agency of competent authority; 2) who are charged with upholding the general criminal laws of an applicable jurisdiction, including having power to arrest; 3) typically have received specialized peace officer training* (see submission for examples); *4) who normally receive tangible official signs of their role such as police uniform or official credentials.* Adjusting this definition does not mean to exclude non-sworn officials from the scope, they just need another label. It should also be considered whether law enforcement should include national intelligence services and national/multi-national military services. |
| **European Communities Trademark Association & Marques (ECTA+M)** | The definition is narrowly focused on questions of personal data. The RT must also consider other applicable laws for the broader protection of consumers and the public at large, including laws on child exploitation, regulation of drugs and medicine, infringement of IP rights, fraud prevention and spamming. Given that the scope includes promotion of consumer trust, the RT must look beyond registrants and consider global citizens as users of Internet and buyers of goods and services. | The RT needs to remember that EU data protection rules only apply to individuals. Businesses and non-persons do not generally have any legal rights to “privacy” and this is reinforced by requirements in many countries for business to register their details in public registers. Whilst the *Producers* definition is broad, ECTA+M believe it is important for the RT to recognize the multiple players that may be involved in the registration of the domain and the scope for the provision of false or inaccurate data. *Maintainers*: ECTA+M recognize the use of language derived from EU data protection legislation, established in Europe for over 20 years with well-known meaning in the context of data protection. The RT should consider carefully how they intend to use this terminology to avoid unnecessary confusion. | The definition is very broadly drafted. Should private parties interested in enforcing civil law remedies fall within such a definition? If it is intended to refer to law enforcement in the sense of public agencies, then greater care needs to be taken in the drafting. Consideration needs to be given to the range of legitimate legal proceedings whether criminal, civil or administrative, for which access to WHOIS data or extended WHOIS data, should be available. |
| **Intellectual Property Constituency (IPC)** | This definition lacks the needed precision. The RT must focus on laws applicable to ICANN in carrying out this policy. It seems inconceivable that *any and all local […] information are applicable.* Which law is applicable to a particular registry or registrar in carrying out contractual obligations to ICANN regarding WHOIS? It is not helpful to assert that every law related to personal data applies. The RT should give consideration to the ICANN procedure adopted to implement a supermajority vote of the GNSO and unanimous vote of the ICANN Board for dealing with any situation in which contractual obligations appear to conflict with a law applicable to the operations of the registry or registrar. See <http://www.icann.org/en/processes/icann-procedure-17jan08.htm>. The policy recognizes that there will frequently be ways for registrars/registries to conform practices with applicable law in order to comply with WHOIS obligations. AoC 9.3.1 should be read in the same way. *Other relevant legal obligations* is also imprecise. ENISA has concluded that the UN guidelines are *not legally blinding, neither to natural persons, legal or countries*; see http://www.enisa.europa.eu/act/rm/cr/laws-regulation/dataprotection-privacy/un-guidelines and <http://www.un.org/documents/ga/res/45/a45r095.htm>. This falls short of establishing any legal obligation that could conflict with or override contractual obligations regarding WHOIS. The RT’s mandate in this field is narrow; the broad and imprecise definition proposed for “applicable laws” will do little to assist the RT in carrying out its assignment. Unless it identifies a particular law that has impeded or threatened to impede ICANN’s enforcement of existing WHOIS policy, it may not be necessary to reach agreement on a definition of “applicable law”.  | This definition does not refer to AoC wording and there is no explanation on why a definition of these terms is needed. IPC recommends that the RT drop this definition. | The RT reads this phrase as limited to governmental enforcement agencies but there is no evidence that the AoC drafters intended this reading. The RT should focus on whether this implementation meets the legitimate needs for the enforcement of laws, which mainly depend on the efforts of private parties. Reliable access to WHOIS data plays a significant role in advancing the legitimate needs of enforcement. |
| **Business Constituency(BC)** | The BC accepts the definition. | The BC accepts the definition. | The BC accepts the definition. |
| **Registrar Stakeholder Group (RSG)** | This definition is adequate with the exception that UN declarations and resolutions are often non-binding and as such inappropriate for the RT’s work. Non-binding resolutions do not meet the appropriate threshold for an applicable law and such references should be removed. | Support. |  |
| **Volodya** | Exclusion process should be defined: when local laws and a UN declaration conflict, which is applicable? |  | The term “law enforcement” is defined without making the scope clear: traffic wardens or NSA? The term “government” also needs to be defined. |
|  | **Lexinta** - Refine the definition as follows: *Includes any and all locally applicable laws and legislation in force that regulate and/or control use, access, and disclosure of personally identifiable information. It may also include other relevant legal requirements, including but not limited to U.N. Universal Declaration of Human Rights etc.* National is too narrow: the regulatory system may imply transnational prescriptions (e.g. treaty of law provisions that locally apply). *Legislation in force* reflects more accurately the intended reach of regulation. *Legal obligations* relate to engagement, *legal requirements* or *legal requirements and obligations* might be appropriate formulations. *Included but not limited to*: avoid any possibility of an excessively restricted interpretation. |  | **Ronald Guilmette** - Such a definition will only be useful if it has been decided that the WHOIS service will have (or does have) some special and particular intended uses unique to *Law Enforcement*. No opinion can be given until a document has been presented into which the definition fits. Should this definition grant LEA access to certain types of WHOIS then it should be drafted broadly. |

**Annex B**

|  |
| --- |
| **1. Do you feel this definition is suitable in the context of this Review?** |
| Yes, but... |
| Yes this definition is suitable.  |
| Yes |
| YES |
| No |
| No |
| Yes |
| YES |
| **2. If not, do you have any suggestions/changes or additions?** |
| ...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. |
| It should include references to the competence in criminal investigation activities, otherwise even CERT´s could be considered as LEA, and I don´t think ICANN will agree. |
| If anything I thing this is overwide and would cover just about everyone involved with Government or working in the public sector. I think this could be restricted to those bodies with Law Enforcement powers or regulatory functions. If it is as wide as this how will ICANN possibly be able to check the credentials of all government bodies.  |
| **3. Does WHOIS policy and its implementation meet your needs?** |
| **a. If so, are any aspects of the WHOIS service more important than others?** |
| 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. |
| In some parts yes. Serbian MoI and We think MoIs in many countries around the world have a problem with accuracy of data, some of register data are incomplete, many of them give an opportunity for anonymous registrations, some of them are not updated/data are old as example if some srevice is sold to other person etc |
|
| Yes it does, email accounts and registrar details are quite useful because they lead to payment details and connection logs. |
| **b. If not, what issues or problems have you encountered with WHOIS?** |
| Criminals use fake-WHOIS or proxy/privacy-registration (with STILL fake data behind) which makes determination of the competent jurisdiction difficult. |
| Whois does not provide the exact physical location of a computer nor does it guarantee that the information provided on entities/persons is correct. |
| It doesn’t fully meet our needs. The main problems are whois privacy (when there are no results in whois) and fake data (when details of the owner of resourse/IP range/AS appear to be fake).  |
| Some remarks: sometimes there is an information in registering data not about an end user but about a company by means of which the domain name was registered; and publication of fictitious data. |
| Lower level & free domain name and website access creates the opportunity for anonymous creation of websites with fictitious email and address details. Advertising revenue has created a situation where anyone can host anything for a given amount of time before checks are made and very often no checks are done until LEA intervention.  |
| **4. How important is WHOIS for law enforcement activities? Are there alternative data sources that you could use?** |
| 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). |
| WHOIS is very important because We think that the most valuable information’s could be found there. Alternative data sources could be forums and other services that have some kind of registers like national services etc.  |
| Important for finding location of devices, identifying subjects. Others sources can be used, but the don’t fully offer the same results if we had a proper functioning WHOIS |
| Whois is, of course, of a great importance. Sometimes we can use additional sources but also based on whois info. |
| It is considered vital in cybercrime investigation due to the fact that there is no other way to obtain data about the legitimate owner of a domain or IP range. |
| WHOIS is very often used in our work. There is an alternative data source – www.centralops.net |
| "WHOIS" is an important first step in the enquiry chain but cannot be relied on, often the contact details are dated and non-responsive on a 24/7 basis.  |
| **5. What changes to WHOIS would you recommend to better meet the needs of law enforcement? Please provide reasons.**  |
| Verification of registrant or at least “plausibility-check” of entered WHOIS-data can lead to better quality of data and might prevent fraudulent domain registrations. |
| We think that accuracy of data is important, some of register data are incomplete, many of them give an opportunity for anonymous registrations, some of them are not updated/data are old as example if some srevice is sold to other person etc. We need exact data of registrants, more informations about administrative contact witch are updated and correct (as example checking of those contacts to see are they real or fictive). The real reason is that We losing a lot of time to establish who is behind some services on the Internet. That would help to prevent anonimity of cyber criminals etc.  |
| Guarantee that a full ID or company (Chamber of Commerce) check had taken place before WHOIS info is entered into database. That the above information will be checked on accuracy regularly. That the exact physical location of server(s) (IP-based, AS-number) is stored in the relevant WHOIS (or RIPE/ARIN….etc) database, possibly including GPS-coordinates. That if incorrect information is provided, that IP/Domain/AS will be revoked. This only to enforce the entry of correct data.  |
| The main change it should be introduced is an effective check policy, in order to guaranty that the information provided is real and updated. If not user can still use any data to fill in the registration forms. |
| a) By legislation down level responsibility. b) by-monthly record updates from it and administrators. c) Immediate upward facing suspension for creating or permitting anonymous or false information for site ownership and responsibility.  |
| **6. In your view, how well is ICANN performing against these requirements? Please provide reasons.** |
| 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) |
| I am not very familiar with this topic |
| They appear not to be aware of LEA’s (and thus legitimate internet users) needs. |
| **7. Do you have specific examples of effective ICANN policies or implementation activities, or suggestions of how ICANN could improve its performance?** |
| 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. |
| If it is possible, it should be a good idea to start digital certificates as a requirement when someone tries to register a domain or IP range. |
| **8. How can ICANN balance privacy concerns with its commitment to having accurate and complete WHOIS data publicly accessible without restriction?** |
| Forbid private-registrations for commercial websites (commercial by content or by TLD – “.com” should be commercial by definition?!) or just allow private registration for private homepages. Define policy about usage of privacy/proxy-services – where it should be allowed (eg freedom of speech) and where not (commercial use). If someone wants/needs to remain anonymous, does he/she really need to register internet-resources or can they also publish content in other ways? |
| Some data could be given in a form that is available to wider public but it must have solution that involve some kind of protected database available only to restricted number of people who are authorised to have more details that are not available to regular users (data could be given as some protected link witch could be seen able only to people with authorization and maybe they could establish database with protected access with user name and passwords). Access should be given upon requests. It is important for the users to be aware of the scams that could be committed when clone Internet sites appears on the Internet as example in cases of phishing etc. If they are aware of this differences between real sites they use and falsh once they could give that information to police.  |
| Publicly accessible could data could show less info as LEA accessible data. This would help to keep up with local privacy issues. The problem will pop-up that foreign LEA’s won’t be able to see all data without permission of the “hosting” LEA. |
| Being stricter when somebody tries to register a domain or an IP Range. They should check that the data provided is real and corresponds to the legitimate user. Developing an effective inspection system. Obviously these inspection mechanisms should be accompanied by penalties, fines, or punishments in order to be effective. In Spain the Ministry of Industry has developed a very strict regulation about this aspects and it is working very good with .es domains. |
| I think this is difficult if not impossible to achieve, especially in relation to the EU and the EU privacy regulations and laws. We need to draw a distinction between privacy and anonymity which is why LE are not against proxy registration per se but that the accurate details of registrants needs to be obtainable by Law Enforcement swiftly and globally without the need to return to the International letter of Request route which is too cumbersome and slow to be effective. ICANN needs to implement a policy which, while respecting individuals rights to privacy allows authorised Law Enforcement (as per definition above) access to the data for the investigation and prevention of crime. Special attention needs to be paid to the “accurate and complete” part of the statement ensuring registrants details are correct. This relies upon ICANN and the TLDs (both cc and gtlds) to implement know your customer policies. A swift removal of infrastructure from any shown to have not supplied correct data is crucial to the effectiveness of the system. If there are no consequences to registering with false data, people will continue to do so.  |
| We think that it is really important to keep in mind the right of the Internet users to receive reliable data about the owners and registrants of the domain names providing services for them. Privacy protection should not infringe upon the right to receive accurate and complete WHOIS data.  |
| a) Information given to all registrants that administration information must be available to the public when a site is for unrestricted public access. b) Third party registered data controllers could be used for private or vulnerable sites (i.e. Schools, Financial Institutions etc.) c) Set levels of information similar to Companies House so that more detailed information requires at least a reason and some level of identification, email, incoming IP etc.  |
| **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?**  |
| In our jurisdiction, all data that has to be published needs to be defined by laws/bylaws. Email-addresses have been removed from the public WHOIS to counter spamming. |
| No, I am not.  |
| NL WHOIS is mainly closed for public now, only LEA is allowed access to full data. Works, but with the concern mentioned under 8. |
| .ES domains from Spain have an excellent system that has been approved by the Data Protection Agency. The information provided includes Name, address, and 4 different ways to contact the owner. It is regularly checked by the Ministry and if data is not updated a fine is issued. |
| Not within the UK to my knowledge.  |
| NO |
| **10. What is the importance of WHOIS data being publicly available without restriction?** |
| Providing contact address for issues with the relevant internet-resource. Indicating possible jurisdiction.“Know your businesspartner”: Possibility to check on registrant of domainname. |
| ICANN should rise awareness of governments in countries that are main sources of proxy services. Round checking should be one of solutions as well.  |
| Legitimate companies could use this data to improved their services to the public. |
| It is the single database in the world that can provide information about IP&domains owners. Those details are very useful because lead you to corporation that is in possession of the information that is relevant to the different cases. If WHOIS data was not public, it would be impossible to identify these corporations, so the investigation could not be carried out.  |
| It’s in direct proportion to the importance of Internet in modern world.  |
| To the general public, knowledge that it is available is sufficient but knowing that LEAs can access detailed accurate information readily and immediately is more important.  |
| **11. How should ICANN address concerns about the use of privacy/proxy services and their impact on the accuracy of the WHOIS data?** |
| Provide accreditation for privacy/proxy-services similar to registrar accreditation. |
| We think that this is a great problem because it could conceal traces and give an opportunity for anonymity and abuse of this services by criminals |
| See 5. |
| They should developed a strict regulation about the privacy services these companies can provide with, and when they are forced to disclosure that information |
| If a person goes onto the street wearing a face mask that person is likely to be detained for some purpose. Access to some buildings will be restricted for example banks. Then equally restrictions on access to and distributing information for or pertaining to the public or individuals are justified to protect the public interest.  |
| **12. What is your view on the use of privacy and proxy services by registrants?** |
| 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”. |
| No |
| See 3. |
| It turns the LEA job extremely difficult because most of these privacy companies are based in foreign countries, so it becomes quite hard to gather information about the real owners of the domains. Even somebody manages to contact them they rarely provide details about their customers. So, in fact, is like deleting the WHOIS databases |
| See previous.  |
| From the point of view of LEA the use of proxy services embarrasses the investigation. |
| a) Generally suspicious however they can serve to protect from some intrusive protocols. b) Reasons for use of proxy servers should be recorded when registering and later use without updating the Whois profile should result in punative reaction.  |
|  **13. Are there any other relevant issues that the review team should be aware of? Please provide details.** |
| This cannot be just more rhetoric and another talking shop but demands some action from the Internet community to protect their own space. Law Enforcement have been lobbying for change to the governance procedures for several years now and to my view absolutely nothing has so far changed. ISPs, Registrars appear to take the short term, fiscally rewarding routes at all times whilst ignoring the long term threat to the stability and international nature of the Internet posed by growing criminality affecting economies and business. Even small changes and steps towards a more transparent and creditable WHOIS system would be welcome. I welcome ICANN’s dialogue with Law Enforcement but t really does need to lead to something tangible, and soon.  |
| Not relevant to this questionnaire.  |

1. For full comments, please see Annex A [↑](#footnote-ref-1)
2. For full comments, please see Annex A [↑](#footnote-ref-2)
3. For full comments, please see Annex A [↑](#footnote-ref-3)