# Gap Analysis

**This chapter examines gaps between ICANN’s policies and their implementation, and between ICANN and its contracted parties’ respective commitments and the services they actually deliver.**

**Consistent with the review team’s scope, the chapter focuses on the extent to which existing WHOIS policy and its implementation is effective, meets the legitimate needs of law enforcement, and promotes consumer trust.**

**The chapter covers three broad areas:**

1. **WHOIS data accuracy**
2. **Data accessibility and privacy**
3. **The roles and responsibilities of contracted parties**
4. **Data accuracy**

[draft not yet finalised]

1. **DATA ACCESSIBILITY AND PRIVACY**

**ICANN’s commitment to unrestricted public access**

**The Affirmation of Commitments provides that ICANN will** implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information.

In responses to the public Discussion Paper, several respondents **supported this commitment to open access, and argued that it is consistent with practices and arrangements in comparable offline situations. For example, INTA stated that it**

**supports open access to accurate ownership information for every domain name in every top-level domain registry via a publicly accessible WHOIS database...in most circumstances, publishing on the internet is a public act, and the public should be able to determine who they are dealing with.**

**Similarly, the IACC argued that**

**WHOIS is only an address book: something that does not adversely affect free speech, and one that carries far more benefits than potential drawbacks ... most other parts of the world require accurate information for business licenses, trademark registration, and other services; domain name registration should be no different.**

**Concerns about privacy**

**This universal commitment to unrestricted public access to complete WHOIS data was questioned by some respondents to the Discussion Paper, who argued that it raises a range of privacy related concerns. These concerns primarily relate to:**

* **the potential for conflict with privacy or data protection laws;**
* **the potential for misuse of WHOIS data (e.g. for spam); and**
* **protecting the privacy of individuals, including potentially vulnerable registrants (e.g. political dissidents).**

**Under the current WHOIS arrangements, ICANN has established procedures and policies intended to directly address the first two of these concerns.**

With regard to potential conflicts with privacy laws, ICANN has established a consensus procedure for “Handling WHOIS conflicts with Privacy Law” (this became effective in January 2008). This procedure details how ICANN will respond to a situation where a registrar or registry indicates it is legally prevented by local/national privacy laws or regulations from complying with the provisions of its ICANN contract regarding the collection, display and distribution of personal data via WHOIS.

**Several respondents argued that this procedure is appropriate, and that ICANN had therefore taken sufficient measures to address potential conflicts with privacy law. For example, the IPC argued that**

**ICANN is subject to a commitment ‘to having accurate and complete WHOIS’ ... ICANN is not required to implement national safeguards for individuals’ privacy. Given ICANN’s commitment to having accurate and complete WHOIS data, the burden of restricting access to such data in a particular locality should fall on the locality, not ICANN.**

**Similarly, the COA argues that**

**The issue of balancing registrant privacy against the need for publicly accessible WHOIS data has two aspects. The first involves situations in which registrars (or registries) are authoritatively advised that their compliance with ICANN contractual obligations would bring them into conflict with applicable national privacy laws ... ICANN policy already provides a mechanism for resolving such conflicts. COA is unaware of any need for further policy development in this area.**

ICANN staff have advised that the consensus procedure has only been used on one occasion, by Telnic, to address concerns raised in relation to UK privacy law. In that case, it was agreed that some public WHOIS data could be limited for natural persons who had elected to withhold their personal information from disclosure by the WHOIS service.

The consensus procedure also appears to be consistent with t**he GAC Principles on gTLD WHOIS services, which state that**

gTLD WHOIS services should provide sufficient and accurate data about domain name registrations and registrants subject to national safeguards for individuals' privacy.

With regard to potential misuses of WHOIS data, the ICANN community has developed consensus policies to prohibit bulk access to WHOIS information for marketing purposes (effective November 12, 2004), and prohibiting resale or redistribution of bulk WHOIS data by data users (effective November 12, 2004). ICANN has also commissioned a study to examine the scope of WHOIS misuse in detail.[[1]](#footnote-1) This study will analyse the extent, nature, and impact of harmful actions taken using WHOIS contact information, and is intended to provide the ICANN community with the empirical data needed to inform any future actions in this area.

With regard to the potential need for special protections for some registrants, **the most widespread way of addressing these concerns is the currently unregulated use of ‘privacy’ and ‘proxy’ services.**

**Privacy and proxy services**

**Privacy and proxy services are offered commercially by a wide range of service providers, including some registrars, and limit publicly accessible information about domain registrants.**

 *Privacy* services limit certain user details from WHOIS by offering alternate contact information and mail forwarding services, while not actually shielding the user’s identity.

*Proxy* services have a third-party register domain names on the user’s behalf and then license the use of the domain name so that a third-party’s contact information (and not the licensee’s) is published in WHOIS.

**As noted earlier in this report, privacy and proxy services are referred to in provisions** 3.4.1 and 3.7.7.3 of ICANN’s RAA [confirm that both are covered]. The review team notes that the current use of these services is widespread, with a 2009 study determining that privacy and proxy services are used in 15%-25% of WHOIS records.

There are diverging views from stakeholders about the use of privacy and proxy services. For example, the NCUC argued that “ICANN should recognize that privacy and proxy services fill a market need; the use of these services indicates that privacy is a real interest of many domain registrants”.

On the other hand, one law enforcement agency argued that ‘if an entity is engaged in legitimate business activities, then a proxy service should not be necessary’. Another stated that ‘privacy/proxy services can be abused’, and that ‘criminals do use proxy and privacy registrations to hide their identities’. A recent Knujon report suggests that privacy-proxy usage is significantly higher among illicit domain registrations that in the broader community.[[2]](#footnote-2)

**Do privacy and proxy services undermine WHOIS?**

A significant number of public responses to the WHOIS discussion paper, and input from law enforcement agencies via the review team’s targeted questionnaire, argued that privacy and proxy services undermine the effectiveness of the WHOIS service**, both in terms of its ability to meet the legitimate needs of law enforcement and to promote consumer trust**. One law enforcement agency argued that

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.

**Another law enforcement agency argued that: “The time routinely invested by law enforcement to validate WHOIS data that may be false, unavailable, incomplete, or proxied impedes investigations”. Similarly, the International Hotel Group argued that**

privacy services have frequently frustrated our ability to protect our hotel brands online, which, unfortunately, often leads to confusion and other problems among consumers.

**S**ome respondents to the Discussion Paper also questioned whether the use of privacy and proxy services was consistent with ICANN’s commitment to the provision of unrestricted public access to complete WHOIS data. For example, Time Warner urged the review team to

identify the proliferation of proxy registration services, and the consequent inaccessibility and inaccuracy (for all practical purposes) of a huge swath of gTLD WHOIS data, as a major flaw in ICANN’s implementation of its WHOIS policies.

The COA also stated that

Until ICANN is able to bring some semblance of order, predictability and accountability to the current ‘Wild West’ scenario of proxy registrations, it will be impossible to make significant progress toward improving the accuracy of WHOIS data, so that the service can better fulfil its critical function to internet users and society as a whole.

In spite the broad level of concern about privacy and proxy services, a significant number of concerned respondents to the public Discussion Paper and law enforcement questionnaire did not advocate for their abolition. For example, some law enforcement agencies noted that privacy and proxy services are a ‘tool to remain anonymous which may be useful and justified in certain limited cases’, such as ‘if someone has a Family Protection Order (or similar) and displaying their information may put them at risk of harm’.

Rather than arguing against the use of proxy and privacy services *per se*, many stakeholders identified the unregulated environment in which they operate as a major underlying problem. For example, Time Warner noted that while it did ‘not oppose the concept of proxy registration in limited circumstances’, it did see

the development of a vast universe of 20 million or more gTLD domain name registrations, for which the identity and contact data of the registrant is hidden and, all too often, completely inaccessible, [as] a direct attack on ICANN’s chief policy goal for WHOIS.

Similarly, the COA acknowledged that some registrants may require specific privacy protection, but that these only accounted for ‘**an infinitesimal fraction’ of current privacy and proxy registrations, and that the**

creation of a vast unmanaged database of tens of millions of effectively anonymous domain names ... is an irrational and socially damaging ‘solution’, one that inflicts far greater costs than warranted upon legitimate e-commerce, consumer interests, law enforcement and the public at large.

**Specific concerns with the current unregulated environment include that:**

* it impedes investigations and makes determination of the competent jurisdiction difficult. In this context, **one law enforcement agency argued that they 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’;**
* **it increases risk for law enforcement agencies by exposing investigative activities to unknown and untrusted parti**es. The BC clearly illustrates this risk when it states that its members have ‘experienced situations where the registrar’s ‘proxy service’ is simply a shell behind which to shield the registrar’s own cybersquatting and illegal activities’); and
* **the responsiveness of proxy or privacy service providers varies widely, with no current recourse for failure to disclose data.**

In terms of responsiveness, the MPAA stated that

To date, only one proxy service has complied with MPAA requests to reveal contact information that would enable the service of a cease and desist notice to suspect operators. Seven other have refused to do so or have simply not responded. Even the one more compliant service has recently changed its policies so that it takes up to ten days or more (after notifying its customer) before it will disclose the information. This gives the suspect ample time to transfer the domain name to another suspect entity or take other steps to evade detection.

Similarly, TWI argued that

Whether or not a member of the public would ever be able to learn the identity or be able to contact the party actually responsible for the registration ... depends entirely on whether this proxy registration provider chooses to make that information available. In Time Warner’s experience, some proxy registration providers are responsible, and will divulge this information upon being presented with evidence that the registration is being used to carry out abusive activities. Many others, however, do not.

**Balancing privacy and public access**

**To address these concerns about lack of regulation, several respondents to the public Discussion Paper and the law enforcement questionnaire argued that ICANN needs to regulate privacy service providers. In most cases, respondents argued that this should include the accreditation of service providers and the imposition of minimum conditions for their operation. For example, the IPC argued that**

ICANN should undertake to create an official set of guidelines for what constitutes a valid privacy/proxy service and best practices for such services.

**Several law enforcement agencies suggested that this type of regulation could mitigate some of their concerns with privacy services, and assist in the investigation and shut down of criminal domains.**

Suggestions for regulatory conditions put forward by respondents to the public Discussion Paper and the law enforcement questionnaire related to the development of clear, workable, enforceable, and standardised processes to regulate access to registrant data when requested. For example, INTA recommended that

where a domain has been registered using a privacy or proxy service, there should be clear, enforceable contract mechanisms and procedures for the relay of communications to the beneficial owner, and for revealing the identity and contact information of the beneficial owner ... privacy/proxy services should be governed by a uniform body of rules and procedures that is overseen by ICANN, including standardised relay and reveal processes.

Compliance issues are substantively addresses in the next section of this chapter. Consistent with that section, the review team considers that an important part of any privacy accreditation process will be to ensure that appropriate and graduated enforcement mechanisms are in place.

Several stakeholders also emphasised the need to limit their use of privacy services in various ways – for example, to private individuals not involved with selling products or otherwise collecting or soliciting money.

Another issue raised by respondents to the public Discussion Paper and the law enforcement questionnaire relates to which data fields should be able to be limited by a privacy service. This issue is central to reaching an appropriate balance between personal privacy and ICANN’s commitment to publicly available information. In this context, one law enforcement agency argued 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.

As noted above, several respondents argued that there may be a case to limit access to some registrant information, and some respondents focused on specific data fields (such as personal addresses, phone numbers and email addresses). For example, NOM stated that ‘in line with UK data protection law, a registrant who is a non-trading individual can opt to have their address omitted from the WHOIS service’.[[3]](#footnote-3) Similarly, FC argued that

Balancing privacy, security and the right to know is the question. Minimal data requirements that allow a quick identification would be ideal, like Registered Name Holder, State/City/Country, email and telephone.

**In terms of balance, some respondents argued that it was important to retain enough publicly available data to establish domain name ownership and registrant identity. For example, INTA argued that**

**INTA supports open access to ownership information for every domain name in every top-level domain ... Available information should include the identity of and accurate, reliable contact details for the true owner of the domain name.**

**The question of ownership and identity is central to the distinction between privacy and anonymity, and several stakeholders raised specific concerns about lack of public access to a registrant’s name and identity.** For example, one law enforcement agency argued that

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.

**While several law enforcement agencies argued that privacy services could be regulated to provide special access to underlying registrant data (including registrant name) for law enforcement agencies, this would not address the broader consumer trust concerns associated with anonymity. For example, INTA argues that ‘in most circumstances, publishing on the internet is a public act, and the public should be able to determine who they are dealing with’. The GAC Principles similarly note that WHOIS data can contribute**

**to user confidence in the Internet ... by helping users identify persons or entities responsible for content and services online.**

**The review team is not aware of any compelling reason to hide a registrant’s name, and notes that a registrant’s name is not allowed to be hidden as a result of the only existing use of ICANN’s consensus procedure to address potential conflicts with privacy law.**

**Findings and recommendations**

**The review team has considered input from stakeholders, its own experience, and earlier work undertaken by the community in developing its recommendations on these issues.**

**On balance, the review team considered that it is possible that, in some circumstances, an individual could have a legitimate reason to withhold some WHOIS information from the public which may not be addressed by the existing consensus policies and procedures. However, the review team considered that the current unregulated use of WHOIS privacy and proxy services is too broad, provides no consistency or predictability for law enforcement or other users, and had significant potential to be abused. The review team considers that this situation has undermined the effectiveness of the WHOIS service, and its ability to meet the legitimate needs of law enforcement and to promote consumer trust.**

**While noting community concerns about the current use of privacy services, the review team considers that reform of these arrangements is more appropriate than developing a new mechanism to address privacy concerns raised by some stakeholders.**

**A critical part of any privacy mechanism will be to determine an appropriate** balance between personal privacy and ICANN’s commitment to publicly available information. In this context, the review team considers that, at a minimum, the publicly available WHOIS information should be sufficient to enable contact with a relevant individual for technical, security and other issues. In addition, the review team considers that a registrant’s name should be publicly available. This would be consistent with arrangements in other public registers, and make clear to the community who is responsible for each domain name.

The review team considers that definitive guidance on the potential to limit other registrant data should be developed through existing ICANN processes, in close consultation with the GAC, privacy advocates, law enforcement, and other interested stakeholders.

The review team is concerned that the existing arrangements relating to proxy **services can serve to complicate the chain of contractual rights and responsibilities between ICANN and its contracted registries and registrars. Recognising a third party as a ‘proxy’ for an underlying registrant also creates an inability to publicly identify who is responsible for a given domain in a timely and unrestricted manner (i.e. an interested party would have to ask the proxy who they are acting for), which is contrary to ICANN’s WHOIS commitments.**

**The review team considers that once a party becomes a registrant, they should accept all the rights and responsibilities of a registrant. If they choose to have an agreement with a third party, then that should have no effect on their rights and responsibilities (including any legal implications) as a registrant from ICANN’s perspective. The review team therefore sees no need for continued recognition of ‘proxy’ service providers by ICANN.**

**The review team therefore recommends that:**

1. **ICANN should develop and manage an accreditation system to allow registries and ICANN-accredited registrars to become privacy service providers.** [the rationale for this limitation to already contracted parties needs to be developed, and centres on concerns that unknown parties with little or nothing to lose from de-accreditation pose a significant risk to the system]
2. Once the accreditation system is operational, ICANN should take the necessary steps to ensure that registrars and resellers cannot accept registrations from unaccredited privacy service providers.
3. **The ICANN community should develop policies to restrict access to privacy services to [limited classes of?] natural persons. This should involve the explicit exclusion of any domain used in the sale or trading any goods or services, or otherwise accepting or soliciting funds.**
4. **As a condition of accreditation, privacy service providers should be required to comply with best practice guidelines. These should provide for:**
	1. standardised relay and reveal processes and timeframes;
	2. guidance on the appropriate level of publicly available information on the registrant;
	3. **maintenance of a dedicated abuse point of contact;**
	4. **public disclosure of contact details and the physical address of the privacy service provider; and**
	5. privacy service providers to conduct due diligence checks on registrant contact information.
5. The best practice guidelines should be developed in close consultation with the GAC, privacy advocates, law enforcement, and other interested stakeholders.
6. ICANN should develop a graduated and enforceable series of penalties for privacy service providers who violate the terms of their accreditation, with a clear path to de-accreditation for repeat, serial or otherwise serious breaches.
7. **ICANN should clarify that the full rights and responsibilities of a registrant accrue to the entity identified as the registrant. As such, ICANN should not acknowledge proxy registrations.**
1. <http://blog.icann.org/2011/04/cylab-at-carnegie-mellon-university-selected-to-conduct-study-of-whois-misuse/> [↑](#footnote-ref-1)
2. [www.knujon.com/KnujOn\_security\_abuse\_report\_031411.pdf](http://www.knujon.com/KnujOn_security_abuse_report_031411.pdf) [↑](#footnote-ref-2)
3. The review team notes that this is consistent with ICANN-approved arrangements in place in the UK based Telnic. [↑](#footnote-ref-3)