Summary of feedback on the proposed Proxy Services framework

Comments received between 10th September 2018 and 9th October 2018

Introduction

In March 2016, in response to increasing demand for privacy online, Nominet recognised privacy services for .UK domain names for the first time. Under the framework that was introduced, when a domain name was registered the registrant details in the .UK WHOIS were replaced by those of the privacy services provider. Nominet, however, requested and held the underlying registrant data and was able to disclose it in accordance with our data release policy.

We were conscious, however, that since its introduction in 2016 some registrars opted to provide privacy services to end-users outside of the framework. For .UK domain names registered in this way, via non-recognised privacy services, the privacy service provider did so at its own risk and accordingly assumed any liabilities associated with being the registrant. As part of the changes implemented to take account of GDPR in May 2018 this Privacy Services framework was discontinued, however we have been aware that a small number of registrars have continued to provide privacy services to their customers.

On the 10th September we launched a comment period inviting feedback from stakeholders on a proposal for a new Proxy Services framework designed to ensure that registrars wishing to offer these services meet agreed criteria in terms of data access, resilience and compliance.

Key features of the proposed framework included:

- Only Accredited Channel Partners would be eligible.
- Proxy service providers would be obligated to respond to LEA data requests within a 24-hour period.
- Built-in safeguards designed to protect registrants against the risk of registrar failure or non-cooperation. Participating registrars would be required to submit a suitable Proxy Service Incident Plan (PSIP), or ensure a suitable third-party data escrow scheme was in place.
- For DRS claims, the Proxy Service Provider (PSP) would have a 48-hour period in which to supply details of the underlying registrant.
- Participating registrars would be subject to an annual compliance audit to ensure underlying data is accurate.

A total of 25 responses were received from a range of stakeholders including Nominet members, registrars, civil society and individual registrants. The feedback from registrars represents a total of 49% of the domains under management. We are grateful to all those who took the time to engage in this process.

Feedback Summary

The principle of privacy online

Despite there being no specific question examining what constitutes a reasonable degree of privacy online in this day and age, it proved to be a theme that surfaced both directly and indirectly in approximately two thirds of the responses received. Perhaps unsurprisingly, opinion amongst those responses was roughly evenly split on the question of whether people should be able to take advantage of proxy services when registering a domain name in order to ensure their identity remains private.

Feedback from some individual registrants and Nominet members stated that "*I think post GDPR the proxy services should be dissolved*" and that "*under GDPR privacy should be [the] default [setting]*". Feedback from civil society was along similar lines suggesting that "*registrants should only be allowed to avail themselves of a proxy or privacy service in narrowly and publicly defined circumstances*" and that "*if a natural or legal entity chooses to establish a domain they are stepping into a public space. They must accept there are consequences which attach to doing that*". Analogies were also drawn with the ownership of land and the importance of public registers.

Conversely, a number of registrars took an opposing view arguing that "*in an age of increased emphasis on privacy, it is appropriate to enable registrars the ability to protect their customers data unless explicitly required to disclose under a court-order or similar*", and that a "*decision to disclose data without an enforceable legal requirement to do so exposes our registrants to risks*".

There was also feedback received calling on Nominet to delay making a decision regarding this framework until the court proceedings ICANN is involved with in Germany regarding collecting elements of WHOIS data are conclusively resolved.

Nominet response:

We accept that the issue of privacy is one that tends to provoke strong views from across a wide spectrum of opinion. Having listened to stakeholder feedback on this question for several years now, we recognise that there are legitimate reasons why a registrant would want take advantage of a privacy or proxy service. We are also conscious that feedback from our registrar channel indicates the demand for such services exists and may be growing as can be witnessed by the commercial availability in the gTLD environment. As such, we believe it is appropriate to proceed with the proposed framework to enable .UK to keep pace with developments elsewhere in the industry whilst also ensuring appropriate policies and procedures are in place to provide suitable safeguards.

The role of registrars

Under the proposal we suggested that the ability to offer proxy services should be an additional benefit only available to those registrars who operate on an Accredited Channel Partner (ACP) TAG in recognition of meeting the higher standards required. Under the .UK RAR those operating on the ACP TAG must demonstrate compliance with heightened layers of good practice standards, such as documentation regarding their business continuity plans and relevant insurance levels for the type and scale of business they operate. This aspect of the proposal garnered strong support from respondents, with a minority of 10% believing it should be an additional benefit available to all registrars regardless of TAG type. One of these respondents argued that "*privacy/proxy services are being provided without issue in many TLDs with no need for regulation of who may provide these services for whom. All Nominet registrars as well as unaffiliated third parties should continue to be to provide proxy or privacy services for their customers without limitation*".

A small number of registrars who responded, including those operating on an ACP TAG, raised concerns relating to the "*time consuming and expensive*" nature some of the additional requirements the framework would impose. This feedback suggested that the added resiliency measures contained in the proposal would "*drive up internal cost(s) of the provision of services*". One registrar respondent objected to the proposed requirement that PSPs validate registrant data on the basis it was "*unprecedented and goes above and beyond the abilities of a registrar*". It was argued such a requirement would have an "*immediate impact on the registration flow*" and that "*the responsibility for data accuracy lies solely with the registrant*". This respondent concluded that "*validation is not a requirement that should be pushed down to the registrar regardless of whether he is providing privacy services or not*".

A number of individual registrant respondents drew attention to what they perceived to be sharp practice within the industry arguing that they didn't believe proxy services "*should ever be something offered as a paid for extra service*" and that .UK WHOIS changes arising from GDPR should "*spell the end for the domain privacy industry which exploits [registrants]*". Disappointment was also expressed that Nominet would not have data for all domains with one respondent reflecting "*if only we could educate the end users that Nominet is the safest place to store your details*".

Nominet response:

As feedback was largely supportive on the question of which TAG types the new framework should be made available to, we have decided to proceed with an approach whereby the additional benefit will be limited to those operating on the ACP TAG. As we proposed, those registrars operating on an ACP TAG who make registrations under the new Proxy Services framework will be required to maintain full, accurate and validated details of each registrant using the proxy service. We continue to believe it is important these registrations comply with the existing requirements under our Data Quality policy which all other .UK domains are required to satisfy.

In light of the feedback touching upon the nature of the .UK WHOIS following the changes implemented as a result of GDPR, we believe it is important that any registrant who signs up to a proxy service does so on an informed basis. By this we mean it must be clear that Nominet does not publish registrant personal data unless the registrant has explicitly instructed us to do so. To curb what many respondents perceived to be sharp practice within the industry, registrars will be required to ensure the registrant is not led to believe that it is the proxy service which is preventing the publication of data in the .UK WHOIS when this is not the case.

Resiliency

In response to stakeholder feedback from earlier this year, the proposed new framework contained built-in safeguards designed to provide a greater degree of assurance and protection against the risk of registrar failure. In recognition of the range of business models and practices amongst registrars we proposed that those registrars who signed up to the framework would have a choice between two compliance routes. Firstly, in order to satisfy that they have appropriate measures in place to limit the extent of damage and disruption to registrants, registrars could elect to provide us with a Proxy Service Incident Plan (PSIP) in advance. This would detail the steps to be taken should a registrar enter insolvency or other form of default. We stated that we would look to work closely with each registrar who opted for this route to ensure a plan appropriate to the size and scale of their operation is in place. The alternative route for those registrars who decided against providing us with a PSIP was to submit data to a neutral third-party escrow provider. The underlying registrant data would only be accessible and released to Nominet under pre-defined and controlled conditions. Registrars who choose the data escrow option would have to meet any and all associated costs themselves.

Feedback suggested that "*to protect the .UK brand this really should not be a tick box exercise like ACP is to an extent".* Some feedback was critical that the resiliency measures did not go far enough, arguing that the measures in the proposal were "*unlikely to be 100% bulletproof and, when they fail, it will reflect negatively on Nominet*." There was however support for the proposed approach with feedback from registrars stating "*we welcome the dual approach, and appreciate Nominet's flexibility in providing both avenues*" and that it "*is unlikely to be one size fits all solution and flexibility should be allowed in how compliance to the policy is achieved*". A number of registrars called for more specific detail in relation to the PSIP by stating "*while we can appreciate and understand the desire to introduce escrow..... we are concerned that... It may increase barriers, risk and cost registrars offering .UK domains. While the alternative option of submitting a PSIP to Nominet detailing registrar contingency plan in case of fail seems a reasonable option, the lack of specifics required gives us pause*". Whilst feedback also suggested that "*robust escrow provisions within the ACP network should be allowed with an agreement of what happens in different scenarios*".

A small number of registrars and Nominet members believe the costs of "*third party escrow should be provided as part of the domain/registrar membership fee*" or that "*if Nominet would like registrars to escrow the data then it should either (1) provide an escrow service like Denic, or (2) Nominet should do a deal with Denic*".

We also received feedback of a technical nature relating to alternative escrow processes such as PSPs lodging encryption keys with escrow providers and encrypted data being submitted directly to Nominet.

Nominet response:

In proceeding with the proposal, we believe it is appropriate such resiliency safeguards form part of the new framework. As proposed, registrars who sign up to the new framework will have a choice of two compliance routes. We have published alongside this report further details relating to the PSIP which should provide greater clarity for those respondents who requested it.

The provision of privacy or proxy services to customers is not a compulsory requirement for registrars, and it may in fact form the basis of a significant revenue stream for those who decide to do so. As such, in relation to the third-party escrow requirement, we believe those registrars who choose to offer the service should meet any and all associated costs themselves.

In response to the suggestion of alternative escrow technical processes, we believe the best way to proceed at this moment in time is to proceed as suggested with one single process in the interests of simplicity and clarity. We will keep this under review and it may be something we revisit in the future.

Additional operational and compliance aspects

We proposed there would be a contractual obligation on PSPs to either provide Nominet, or a reputable third-party auditor selected by Nominet, with a statistically meaningful sample of domains registered using the proxy service during every twelve month period in order to check the accuracy of its data. The PSP would be responsible for the costs associated with conducting any third party audit, and should the audit results reveal data accuracy issues the PSP would be expected to submit a corrective action plan to the satisfaction of Nominet's compliance team.

The auditing requirement attracted few comments however there were a small number who felt it "*defeats the purpose of privacy/proxy service provision*" and there was also a question of how access could be granted if it was escrowed and encrypted.

In relation to the requirement to provide quarterly registration statistics, feedback from some registrars observed that "*Nominet is trying to give itself very broad powers of access to data*" and that "*while such statistics may have a certain value, the costs of adding such reporting framework functionalities outbalance such value*". Other registrars however commented that these "*reporting requirements are interesting, it looks fine overall*".

The proposed framework also stated in the event that a Dispute Resolution Service (DRS) complaint for an abusive registration is filed against a domain registered in the name of a PSP, Nominet would notify the registrar. Upon receipt of this notification the registrar would have a 48-hour window in which to remove the details of the proxy service and replace them with complete and accurate registrant information. The DRS claim would then proceed against the registrant as normal. If the proxy service was not removed within this time frame, then the complaint will proceed against the listed registrant (i.e. the PSP). Section 5.3 of the Dispute Resolution Service Policy would continue to apply with the result that there will be a presumption of abusive registration if the respondent has been found to have made an abusive registration in three or more DRS cases in the two years before the complaint was filed.

The majority of respondents indicated that this approach was sensible, with minor suggestions such as rather than a 48-hour window "*it would be more reasonable to require action within 2 business days*" to avoid difficulties arising around long weekends due to public holidays. One respondent believed that "*the DRS should provide a guarantee that the underlying registrant data will not be disclosed to the complainant or stored once the DRS case is closed*". There were concerns expressed regarding the potential for the DRS process to be gamed by multiple claims and the automatic sanctions that would be applied, and the "*chilling effect this could have on free speech*".

The PSP will also be required to provide appropriate responses within a 24-hour period, including provision of the underlying registrant contact data, to all reasonable and written legal enquiries from Nominet and UK public authorities with prosecution powers as well as the types of organisations listed in Schedule 4 of the .UK RRA. Concerns were expressed by a small minority of respondents regarding jurisdictional issues arising from requests from LEAs based in foreign territories. Whilst some suggested "*the ACP should be able to provide what they deem as legitimate requests*".

Nominet response:

As previously outlined, we remain committed to improving the accuracy of data for .UK domain registrations. The auditing requirement will therefore form part of the new framework, and we will work closely with each registrar to implement an annual auditing process that suits the needs of both parties. In terms of the quarterly registration statistics requirement, this will remain but will be limited to national geographic location as well as the abuse statistics

as we won't necessarily have sight of complaints in instances when the complainant liaises directly with the registrar. This will allow us to maintain an accurate picture of the geographic spread of registrations. The requirement to provide us with DRS statistics will be removed.

In response to the suggestions within the feedback, we will amend the wording for the response windows from hourly periods to business working days.

Conclusion

We would like to thank the respondents for their time and effort in providing responses to this comment period. Formal notice of the changes will be given at least 30 days prior to implementation.