STOBBS
ENDURANCE HOUSE
VISION PARK, CHIVERS WAY
CAMBRIDGE CB24 9ZR

WWW.STOBBSIP.COM
INFO@STOBBSIP.COM
PHONE. 01223 435240
FAX. 01223 425258

Proposed Interim Model for GDPR Compliance

(The "Calzone Model", 28 February 2018) Prepared by: ICANN Org

Stobbs Comments on Proposed Model

Introduction

Stobbs is a brand consultancy and intellectual property law firm, that represents many brand owning clients around the world. We have been involved in many disputes relating to domain names, and represent many parties in this space. We are providing comments because we believe that the proposed interim model does not go far enough to balance the competing interests of brand owners in the context of compliance with the GDPR and the interests of privacy for individuals.

We understand and respect the fact that all parties have to be GDPR compliant in the new regime. However, we believe that the proposed interim model goes too far in favour of privacy of information in the balancing act between GDPR compliance, the need for a WHOIS system that supports trust in the domain name system (as referenced in para 2 of the proposed model) and the internet and the legitimate interests of brand owners to prevent abuse of their rights (clearly a "legitmate interest" under Art 6(1)f of the GDPR).

Why WHOIS is important

As many of the community comments have observed policing the internet for abuses of legitimate rights is a constant battle for brand owners. The internet has made it easier and easier to profit from rights abuses.

Most web based sales are facilitated through a domain, and the provision of legitimate WHOIS data is a hugely important tool for brand owners in the fight against abuse of their rights. Being able to contact the owner of a domain or website is the first step in relation to enforcement of rights, and having the information as to who is behind a website is an essential intelligence tool in the effort to understand both an individual abuse, but also whether this is linked to other infringement issues online.

The availability of this information is key in the fight against rights abuse, but also the immediacy of the availability is essential. The very nature of online infringement means

that it is very easy to move or hide, and any delay in the provision of information (or indeed notification to an individual of a request for information) provides another hurdle or bar for a brand owner, and tips the balance of interests further in favour of an infringer, which we do not believe is justified.

The proposed model goes too far

The proposed model goes further than it needs to in order to respect the GDPR. In doing so it does not give suitable weight to the interests of brand owners. In particular:

1. In allowing the model of restricted WHOIS to be available to Registrars and Registries that are not formally governed by GDPR requirements (for example because they are not within the EEA) the model effectively changes the whole WHOIS system because of European regulation. The justification given is that there are other similar legal requirements in other parts of the world and that applying this unevenly would favour European Registrars or Registries. However:
    a. Other legal requirements should be addresses specifically and not in general terms;
    b. The commercial interests of Registrars and Registries are not relevant in this discussion, or at least are not more important than the legitimate interests of brand owners.
2. In applying the model to the information of legal persons as well as individuals the model effectively applies the GDPR to huge amounts of data that it was not intended to protect. The reasons given are that not doing this would put a burden on Registrars to determine whether information relates to an individual or a legal entity, and that in some circumstances the information for a legal entity contains individual information. However:
    a. In general it is obvious whether the owner of a domain, and so the information provided, is an individual or a legal entity. It would be straightforward to put in place a rule whereby data that obviously relates to a legal entity can be made public, with a simple mechanism to lodge a complaint if you are an individual in order to take down information that has been made public in error;
    b. It would be very straightforward to impose a requirement to identify whether you are an individual when purchasing a domain. As you are still required to provide "thick" data this would not impose any additional onerous requirement. If this were done then only information relating to individuals would be put behind the GDPR shield. This alone would allow access to huge amounts of information that is not legitimately the subject of the GDPR.
    c. Personal information is not required in the WHOIS record for a legal entity, and this could easily be flagged during the registration process.
3. The proposed model imposes an accreditation programme for parties that can obtain information. Why should this be the case? If it is acknowledge that there are legitimate reasons to obtain the information in accordance with Art 6(1)f GDPR (albeit that IP abuse is not a significant enough reason to make the WHOIS a full exception to the requirements of the GDPR), why should the information

only be available to accredited parties? Surely if anyone can show a legitimate reason to have the information then they should have the information, whether they are accredited or not? This is further commented on in the section below.

4. It is unclear in the proposed model what level of information would be provided where a legitimate interest could be shown. Will this apply only to the information for the queried domain? If so this does not go far enough to protect the interests of brand owners. Obtaining information not just about an individual domain, but also the pattern of practice of a domain owner is an essential part of preventing abuse online. Indeed, the pattern of practice of a domain holder is one of the specific factors that is cited as relevant in establishing bad faith in accordance with the UDRP. Without being able to establish what domains are owned by a party or linked to a party this would make it almost impossible to establish patterns of practice by bad actors, and provide further assistance to those who seek to abuse the legitimate rights of brand owners. If there is a legitimate interest to obtain the registration information for one domain, then this would apply to the domains owned by that party (or linked to that party).

<u>What should change</u>

The importance of maintaining a credible WHOIS system, as set out in para 2 of the proposed model, means that the model should not go further than it needs to in allowing compliance to the GDPR. Whilst we respect the need to comply with local laws, and the general principle of privacy, other competing interests, including the legitimate rights of brand owners should also be taken into account. As such the following changes should be made:

1. The masking of WHOIS should only be possible for specifically defined situations relating to the EEA, or where the Registrar can show a legal reason for the masking of the data. Specific detailed requirements could be made for this model to differentiate situations where it should and should not apply;
2. The masking of WHOIS should only apply to the data of individuals and not legal entities. A requirement to identify whether you are an individual should be imposed on registration;
3. Anyone who can show a legitimate interest to obtain information should be able to do so without delay. In order to streamline this process there should be a list of specific requirements (non exhaustive) for this and a simple process (not including notification) to obtain the information, and the information should be provided immediately if these requirements are established.
4. If requirements are established to provide information for an individual domain, then this information should be provided for all domains owned by that individual.

In the interests of fairness provisions should also be made relating to the abuse of the process in obtaining information, to ensure that it really is only provided where there is a legitimate interest to do so.

<u>Accreditation programme</u>

If an accreditation programme for obtaining data is deemed to be suitable it is essential

that this does not in effect become a further significant bar to the exercise of legitimate interests of brand owners. In particular:

1. At present the proposal suggests that accreditation would be provided to law enforcement bodies and IP attorneys. This is too restricted. Many significant brand owners run IP enforcement programmes within their organisations, and whilst these are run by experienced professionals they are not all IP attorneys, and a requirement that only these groups can be accredited would force significant changes (and increased cost) for brand owners in running their programmes. The same would apply to small parties who do not wish to hire an attorney (perhaps because of expense) in this process;
2. Any accreditation programme would also need to apply to legitimate vendors of intelligence and platforms around online infringement. If these vendors (such as Pointer, Incopro, Yellow, MarkMonitor and others) could not obtain legitimate information they would be significantly prejudiced in the provision of their services, and the knock on effect would be that many brand owners would be held back in their legitimate efforts to battle online infringement of their rights;
3. There needs to be a clear indication of what information can be obtained through such a programme, and this has to include the provision of information relating to all domains owned by an individual or party, as outlined above;
4. Notification of a request to a domain owner CANNOT be a part of the process. If there is a legitimate interest to obtain the information, then the likelihood is that infringing activity is occurring through the domain, and a notification to the owner will allow them to move that activity to another masked domain;
5. Time is critical in this. In particular:
    a. There cannot be a delay in establishing how the accreditation programme works, as even a short period when brand owners cannot obtain information when they have a legitimate interest to do so could have a very significant impact on efforts to prevent infringement of rights;
    b. Any system that does not provide an immediate or near immediate provision of information will have a significant impact on enforcement activity. The bad actors can move very fast because of the nature of their activities, and with masked WHOIS it allows them to move activities to another domain very easily. As such providing a set of easy to understand rules and requirements for obtaining information, but then providing a function to provide the information immediately when those requirements are met is an essential.

We primarily act on behalf of brand owners, and of course understand the competing interests involved in this process. We understand that the GDPR cannot be changed and that the requirement to be compliant is fixed. However, bearing in mind the huge amount of data available around online infringement issues, and the huge part that WHOIS plays in combatting this, we feel strongly that any model should not go further than it legally needs to.