Hogan Lovells Comments on the 3 ICANN Models for WHOIS Compliance with GDPR published on 12 January 2018

Introduction

These comments are in response to the request from ICANN for comments on the three interim GDPR models proposed by ICANN. [i]

Hogan Lovells is one of the leading privacy and cybersecurity law firms in the world, we are involved in an ever-expanding array of matters at the cutting edge of legal, policy, and technical work. In 2015, we won the first ever Chambers Privacy and Data Security Team of the Year award. In 2017, we were awarded this honor once again. We counsel tech-sector titans in Silicon Valley and major financial services corporations in New York. The auto industry turned to us to help them develop "connected car privacy principles." We recently handled one of the largest retail data breaches. One of the largest health insurer data breaches. And one of the largest hospital data breaches — all within a few months of one another.

We are also heavily involved in the Internet and Domain Names. Our Global Domain Name and Internet Governance Practice has advised clients in this area for 20 years offering a unique, comprehensive and centralized online brand protection service called Anchovy. Hogan Lovells also specializes in all aspects of the ICANN new generic Top Level Domain (gTLD) process. We have been involved in the ICANN process for many years (since the fourth ICANN Meeting in Los Angeles, 1999), and as an example provided comments on every version of the new gTLD Applicant Guide Book. Hogan Lovells is also an accredited ICANN registrar. So we understand domain names and we use WHOIS daily working with a number of brand protection firms and cybersecurity companies to go after unscrupulous third parties who are involved in criminal activity, consumer scams and abusive registrations of domain names involving phishing, malicious emails, brands and individuals.

In my work as a Domain Name Panelist with WIPO for the UDRP as well as Nominet for .UK Disputes and the Czech Arbitration Court for .EU and the UDRP I have had in the last 15 years a plethora of cases brought concerning domain names registered by unscrupulous third parties looking to abuse and defraud consumers, sell counterfeit goods and counterfeit pharmaceuticals – the vast majority of these cases have seen the registrants bad faith proved by the evidence provided using reverse WHOIS look ups i.e. there is a pattern of such behaviour. Domain names used for malicious purposes, infringing IP rights, or defrauding consumers often share common registration data, such as registrant or admin email addresses. Indeed the UDRP itself requires a pattern of such bad faith conduct. WHOIS is needed for this.

It another role, namely as a member of the ICANN CCT Review Team where we have been looking into DNS Abuse and Trade Mark abuse amongst many other aspects and it is abundantly clear to me from the DNS Abuse Study[ii] that we commissioned that a restriction in the access to WHOIS or a fractioning of the current system into a patchwork of different solutions for access for those with legitimate purposes would be highly problematic for consumers and other Internet Users across the globe.

WHOIS is thus necessary. Necessary for trust. Necessary for safety. Necessary for the proper functioning of the Internet and to help ensure its security and stability. ICANN has stated that it is seeking to develop a WHOIS model that is GDPR compliant whilst preserving the current WHOIS data and access to the greatest extent possible. That is a considerable challenge.

It is still more of a challenge when the comment period on these 3 ICANN Models amounts to only 11 working days from their publication on 12 January 2018. Out of necessity these comments are thus limited in scope.

Who needs WHOIS?

WHOIS is a critical feature of the Internet and the Domain Name System. A means to know who is dealing with who and whether someone or some entity is who they say they are. Law enforcement, IP attorneys, cybersecurity experts, anti-abuse companies, brand enforcement companies, trust and safety certification companies and platforms, governments, registries, registrars, registrants and consumers as well as academics all require access to WHOIS data and with that access contribute to the security and stability of the Internet DNS. These groups have access for legitimate purposes and it is critical that this access for legitimate purposes continues and does not find itself throttled by a dash to avoid risk and the penalties which the GDPR is to apply from May 2018. A deficient interim model which is not adhered to across the community will serve no one well. A patchwork of varying solutions will leave gaping holes which the unscrupulous will thrive upon and the trust in the Internet and the DNS could erode forcing a plethora (tsunami) of claims, subpoenas and litigation which we have to date largely avoided.

We have looked at the three models which appear to draw on the Hamilton Memorandums as well as taking on board some aspects of the five community models proposed, though given the time between the publication of the three ICANN models and the end period for comments on the third Hamilton Memorandum and close date for Community models of just two working days there is understandable concern as to whether the communities views have been sufficiently considered and not just sidelined.

Support for Model 1 but with additional aspects

Given the above, and with a view to seeking to move towards one interim model we would be most supportive of ICANN's Model 1 but with the proviso that it had a number of additional aspects included.

Natural Persons

Model 1 makes a clear distinction between data belonging to a natural person and data belonging to a legal entity and calls for the registrant to identify itself as a natural person or legal entity. This is a critical distinction under the GDPR as it applies only to data belonging to natural persons and any model should not inadvertently extend the scope of the GDPR.

With regard to a registrant that is a natural person if that person is not using the domain name in the course of trade then they could opt in to self identify as a natural person resident in an EU member state. They would then not have their registrant name public but could have an email address remaining public.

Where a registrant is trading, then fuller information is needed in any event under the E-Commerce directive. This would be certain minimum information as required and such information must be easily, permanently and directly accessible including name, email address and geographic address together with company registration number. The sale of domain names could be deemed as trading.

Individuals who are demonstrated to be trading (looking at their website for instance) could have their registrations reclassified by the registry and the full contact information become public. This is what Nominet currently does with .UK for instance.

Third parties with a legitimate interest such as law enforcement, IP attorneys, cybersecurity experts, anti-abuse companies, brand enforcement companies, trust and safety certification companies and platforms, governments, registries, registrars, registrants and consumers as well as academics could seek further information from the registry or registrar and such

information would be tor the specific and limited purpose for which it was requested. There would be a cost component to this, but those ccTLDs that operate in this manner consider the cost to not be significant to the number of registered domain names they have in their zone file. Indeed it is one aspect that may also encourage registries to seek to minimize DNS abuse which is of benefit to the entire community.

Registrant Email Address

The Registrant email address is arguably the most valuable part of the WHOIS record for Cybersecurity and IP enforcement. It is used in order to cross check other domain name records to see if there is a pattern of bad faith or DNS abuse thereby being a key to preventing malicious cybersecurity threats, criminal activity, illegal activity and consumer abuse.

Model 1 proposes keeping most of the current WHOIS data collected and displayed except for the masking of the registrant name and email address. We would respectfully suggest that the registrant email address could be included. We assume that ICANN has based its assessment on the 3rd Hamilton Memorandum which states:

"our assessment is that access to the e-mail addresses of registrants which are natural persons is not necessary for the purposes listed in 2.7.1(i) - (v) above and that such e-mail addresses therefore should not be made publicly available through the Whois services"

However, the basis for such an assessment is not clear. One missing element for instance is what the data subject "can reasonably expect" (recital 47 GDPR), and whether and how the WHOIS practice during the last decades influences such expectation. There also appears to be no full analysis of the current use of email addresses for the discussed WHOIS legitimate access purposes (eg. Fraud, cybersecurity, IP infringements, business owner identification). We do not see how an email address, in particular one that is chosen by random or used only for this specific purpose, necessarily raises more privacy concerns than a name or a postal address as included in Model 1.

Registrars and Registries granting access

Model 1 states that "Registries and registrars may, but would not be required by ICANN, to provide additional access to non-public WHOIS as long as it complies with GDPR and other applicable laws." We would suggest that this should say "shall be required".

Bulk WHOIS access (port 43)

This is not covered in Model 1 but is a critical aspect for cybersecurity, law enforcement and brand enforcement. Bulk access to WHOIS by certain data requestors who have been validated and may also be requested to provide indemnities against any misuse of data should be possible and encouraged. We do not see that GDPR would exclude such bulk access for parties with the above WHOIS legitimate access purposes and who are adopting appropriate and verifiable means for protecting the registrants' legitimate interests.

Consent

We disagree with consent being discarded as per the Hamilton Third Memorandum, if consent is one of several options and freely given updating the consent procedures could make consent a viable option for ICANN. Indeed registrants have many good and valid reasons to give consent be it for ownership and identification, customers, domain name sales. It would make sense that where people wish to provide their contact information they can do so. Consent can easily be withdrawn at any time, thus protects the individual's

freedom of choice and privacy, and may therefore give a basis for even wider and easier access than as based on third parties' legitimate interests.

A layered access model

We think that such a model could be feasible. It is said that such a model would require registrars to perform an assessment of interests in accordance with Article 6.1(f) GDPR on a case by case basis. However we would argue that if the layered access model is based on "automatically qualified parties" having adhered to a Code of Conduct, or binding policy, such model could be feasible. The GDPR does not require an assessment on an "individual case-by-case basis", since the "purpose of specifying the application" of the GDPR with regard to the "legitimate interests pursued by controllers in specific contexts" is explicitly listed as an example for the content of a Code of Conduct (Art. 40(2)(b) GDPR). A binding policy can set out the carefully balanced interests and the appropriate means to protect also the registrants' interests. Such binding policy is quickly adopted, could include verification mechanisms, and can evolve into an approved Code of Conduct.

The power of law enforcement authorities for instance to access data through a centralized layered access model would be determined by national law.

The Network and Information Security ("NIS") Directive (2016/1148)

The GDPR itself acknowledges that ensuring network information security constitutes a legitimate interest for data protection (Recital 49, Articles 25 and 32). However there is also another relevant Directive, the NIS Directive. Under this EU Directive, operators of essential services must take appropriate and proportional measures to mitigate risks posed to network security and information systems which they use. Domain name registrars and registries would be covered by this Directive so would need to meet the obligations under this Directive and ensure that security risks and DNS abuse and consumer fraud are identified and dealt with appropriately and proportionally. Law enforcement, attorneys and cybersecurity companies play a critical role in investigating, preventing and mitigating malicious attacks and WHOIS access remains a necessity for this.

Conclusion

We applaud the wealth of input coming in to ICANN and sincerely hope that we can all work towards a universally accepted hybrid model. Any interim solution should not create costly administrative or legal processes which hinder such access to any non-public WHOIS. Of the three ICANN models proposed with a view to seeking one interim model we would be most supportive of ICANN's Model 1 but with the proviso that it had a number of additional aspects included as discussed above. It is critical that swift access to accurate WHOIS databases of IPaddresses and domain names is maintained, so that law enforcement capabilities and public interests are safeguarded. If the public WHOIS does not in the future provide the necessary information then that may be acceptable provided that the registries provide the appropriate data access to legitimate interest third parties without excessive cost or process hurdles.

Approved codes of conduct (Articles 40, 41 GDPR) may help demonstrate compliance with EU data protection law. Indeed such rules are flexible and provide a framework for data processors to provide access to the WHOIS system in order to develop pragmatic solutions, as we are seeking to develop here, in order to differentiate between those categories of data that can be made public from those which cannot.

The Article 29 Working Party In its recent letter to ICANN invited ICANN and its stakeholders to enter into a dialogue to discuss the data protection issues affecting the WHOIS system,

and this should be seized upon to ensure that possible ways to successfully address them are fully considered.

In any event ICANN needs to specifically set out the different purposes for processing, including the legitimate pursuit of certain public policy objectives as discussed above.

ICANN has stated that its interim model must ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible. It is clear that compliance with GDPR does not mean extending the scope of GDPR over and above what the European Commission intended. It is also clearly important for the interim model to be implementable by registrars and registries. The ability for those with a legitimate interest and purpose such as law enforcement, IP attorneys, cybersecurity experts, anti-abuse companies, brand enforcement companies, trust and safety certification companies and platforms, governments, registries, registrars, registrants and consumers as well as academics to access any non public WHOIS is critical to maintaining the security and stability of the Internet and DNS.

David Taylor, Partner, Hogan Lovells
Stefan Schuppert Partner, Hogan Lovells
29 January 2018

[i] https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf
[ii] https://newgtlds.icann.org/en/reviews/cct/dns-abuse