BACKGROUND PAPER ON OPEN FORUM: ICANN, PRIVACY AND DATA PROTECTION

This is a brief Paper explaining the background to some of the issues addressed in the ICANN Open Forum

Objective

ICANN is involved in a Community wide discussion to evolve a contractual regime for Registries and Registrars and related policies which reflects global consensus on data protection and privacy requirements, while at the same time recognising the legitimate interests of registrants and other stakeholders such as law enforcement.

The impetus for this work, although not the sole focus, is the Regulation on Data Protection in the European Union (the GDPR) which talks effect in May 2018.

Background

ICANN over many years has developed contractual arrangements with Registries and Registrars who issue and sell, respectively, generic names. In particular all registries responsible for the new, post 2012 generic top level domains (gTLDs) and registrars selling them have contractual obligations which include making certain forms of registrant data available in the public WHOIS database.

From May 2018, the requirements laid down in the European General Data Protection Regulation (GDPR) will affect all bodies both in the European Union, and potentially those elsewhere, that process the personal data of EU citizens. Many Registrars and Registries contracted with ICANN will, therefore, be subject to the Regulation.

WHOIS Database

WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of, typically, an Internet domain name and an IP address block, though is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format. It is used by nearly all registries and registrars and for contracted parties there is a minimum data set of registrant information that has to be included.

The evolution of the Internet ecosystem has created challenges for WHOIS in every area: accuracy, access, compliance, privacy, abuse and fraud, cost and policing. Questions have arisen about the fundamental design of WHOIS, which many believe is inadequate to meet the needs of today's Internet, much less the Internet of the future.

ICANN has had to modify WHOIS over the years; the consensus policies on accuracy are a prime example, as well as the introduction of validation and verification requirements in the new form of the 2013 Registrar Accreditation Agreement).

Evolving regional and national data protection requirements are increasingly affecting the data registries and registrars are able to place in WHOIS, while enhanced concerns on fraudulent and criminal use of domains may well require such information to be included.

The evolution of WHOIS, is therefore, part of a policy development process (on next generation Registration Data Services) taking place at ICANN; see https://gnso.icann.org/en/group-activities/active/rds

European Regulation

Up until May next year the obligation on members States to enact data protection legislation derives from the 1995 Directive (95/46/EC). The latter lays down reasonably comprehensive, but broad, principles on how personal data should be handled and protected. Enacted through different national legislation in the 28 member States, registries and registrars in some countries were obliged to see specific waivers from their ICANN contracts in the way they processed and stored data. In other countries the national legislation adopted, pursuant to the directive, did not necessitate the request for such waivers.

The General Data Protection Regulation (GDPR) – which was agreed by the European Parliament and Council in 2016 – has built upon the requirements of the directive in a number of ways, not least in the penalties that can be applied for a body deemed not to be in compliance and the territorial reach of the Regulation, potentially affecting numerous bodies outside of Europe which as part of their business model targets European customers and thus collect personal data of such.

Development of proposals

There are a number of initiatives underway in ICANN (both in the Organisation and in the Community) which will, hopefully, be in state of maturity by the IGF in December.

The Organisation had initiated two specific initiatives; the first looking at what is needed in terms of possible contractual changes for contracted parties to work with ICANN in ways which are acceptable to the requirements of the European Regulations and reflect a general consensus on the way that personal data (of whatever genesis) should be collected and processed by ICANN Registries and Registrars. The second initiative is focused on the Organisation itself and the requirements it may be under with respect to both the way it collected data, for example for personnel reasons, and the responsibilities it has for the contracted parties. Consideration here regarding the legitimate needs of law enforcement authorities to types of data will need to be given.

Within the Community there is also discussion proceeding between contracted parties and the Organisation in terms potential changes to contract.

European Union and beyond

While the current focus is primarily on the effect of the agreed European Regulation on Registers and Registries that handle the personal data of European registrants, ICANN recognises that there are wider regional and global discussions taking place on data protection which should be taken account of. ICANN will probably not be in a position to have contractual arrangements that satisfy all national legislation but hopefully they will take account of the main regional approaches; for example, those evolving in Africa and in APEC.

Issues for consideration

As the ICANN Community develops policies and processes there will be a number of issues that will no doubt need debate and resolution.

On the European front, while the EU Regulation has direct effect (in that it applies across the EU irrespective of any national implementing legislation) it does not of course preclude the Data Protection Commissioners in the EU issuing guidance for particular actors. This could be a useful approach to take given the complexities DNS players may encounter.

As noted above it is unlikely that any agreed arrangements in contracts will satisfy all global legislation on data protection thus potential need for waivers in certain circumstances. How broad these waivers should be is almost certainly a question on which many will have views in the ICANN Community.

Looking Forward

This Paper is simply some background to the discussions that will hopefully be taking place at the IGF and elsewhere. Within its mandate ICANN will work to evolve arrangements for registries and registrars that are appropriate and take into the need of stakeholders, including registrants, while not being inconsistent with emerging data protection legislation in Europe and beyond.

ICANN, July, 17