On 1/8/18, 14:48, "Vittorio Bertola" wrote:

Hello,

I would like to provide a comment in personal capacity, as a long time participant in ICANN and online privacy discussions.

In the end, I think that the recommendations in part 3 of the memorandum are reasonable and pretty much the only thing that ICANN can do. ICANN should try to obtain an agreement with the appropriate European authorities (DPAs and EDPB/EDPS) on what would be considered acceptable under the GDPR, and the mechanism of the DPIA seems appropriate, especially if it can be used in a way so to prompt a discussion at the European level rather than just the interpretation of a single DPA (to this regard, ICANN may find it useful to submit DPIAs to multiple DPAs so to lead them to agree on a single point of contact and overall position). In the meantime, removing any public access to the data of natural persons and allowing authenticated access only by a limited set of well recognized actors (2.4-2.6) is the only option shielding the industry from legal liabilities.

At the same time, I have some reservations on some of the statements in section 2 of the memo.

First of all, section 2.7 seems to insist on the fact that there could be some "legitimate interests" by private parties that could allow to publish data of natural persons in the Whois databases without their explicit and voluntary consent. This idea has already been rejected in the past by the Article 29 Working Party, so while there is now a new mechanism to get a more binding opinion, still it would not fly well to get back again and again to that argument.

Also, I would not recommend ICANN to adopt the argument (stated in 2.7.10) that some personal data need to be published without consent because creating a layered access system that can take care of the uses specified in 2.7 is too hard and would be too costly for registrars.
It's not that you can break a law because getting to the same result without breaking it is harder!

In any case, even if the discussion with the European authorities led to

the conclusion that publishing a few basic data items in Whois could still be possible, I would strongly recommend to let the data subject (i.e. the person whose data are to be made public) to choose the type of data that they would like to make public to be contacted. Section 2.7.3 argues that the private home address of the individual, rather than their email, should be forcibly published - but in most cases the home address is a much more sensible piece of information than the email address, which can be shielded from interference and changed much more easily. So this choice should rest with the data subject, that could be asked to decide whether they want to make public an email address, a real world address or a telephone number (or all of them, if they freely decide so).

Finally, I found the comparison of the Whois case with trademark registries (2.8.2) and with company registries (2.8.4) definitely inappropriate. It is a bit troubling to read that the authors of the memorandum "have had difficulties seeing the difference between a trademark register and a domain name register from a public interest and integrity protection perspective" (2.8.2.6) - it makes you think that their views are inherently biased in favour of the commercial use of the Internet and against the non-profit, social and cultural ones, which instead are those that most usually apply to the natural persons that the GDPR tries to protect, and for which privacy protection is paramount. The only appropriate comparison in the document is the one against the rules that have been established for the Whois databases of the European ccTLDs, which could be taken as an initial guidance, even if they have been developed under the previous version of the European privacy laws and thus may need to be adjusted under the GDPR as well.

Regards,
--
vb.