On 3/31/18, 10:46, "John Bambenek" wrote:

The entire debate on ICANN and GDPR presumes the status quo in how we deal with domain registrations today, namely that the only way to protect privacy of registrants today is to pay for a "proxy registration". In short, people wanting their privacy rights have to pay for it and it is, by definition, not a free choice. A very easy change to this system would be at registration and any time thereafter, a natural-person not engaging in commerce who is a registrant can simply mark a domain as private and the information never get displayed. They can mark or unmark this however they see fit. Some basic information could be presented as to why they would choose or not choose to do this. If they do choose to publish, they do so knowing the information will be in a publicly available global directory (and it can be communicated as such). If a domain registrant WANTS their information to be available in a global and public directory, then there is no practical reason why such choice should not be allowed as long as it is freely given and the relevant information is given to them. They could even get annual privacy reminders.

There are, however, several benefits of having accurate domain contact information. The registration of a domain is, by definition, for the purposes of communication. In some forms of communication, all parties should know and be able to verify the identity of each other through an independent system. For instance, before I enter my credit card information into a website, I should be able to see who the beneficiary actually is. You "could" put this on a webpage, but if you compromise a web server, you can compromise all other information that webserver contains. Whois is an independent system that provides a second check. Is this website that says they are Microsoft really Microsoft. Identity and authentication are problems that have existed for internet communication since time eternal, it is better for all involved that we don't make such problems incrementally worse.

Whois information is also a critical component of anti-spam and security functions. GDPR is intended to protect privacy, and these professionals have spent their entire career doing the same. It remains the unambiguous and

unanimous opinion over almost every professional who has weighed in that removing Whois would led to a net reduction in global privacy and a major increase in crime and successful attacks on consumers with the net effect of compromising their privacy.

Whois information has proved a critical tool in proactively monitoring for attempts at election manipulation, but in the US and in Europe. Security professionals were able to see with domain registrant information that En Marche! was going to be under attack by alleged Russian state-sponsored actors BEFORE such attacks occurred. We see similar occurring now in the United States. This is equally true for trying to identify propaganda and influence operations. Not being able to examine Whois records READILY will make the fight against foreign manipulation of democratic processes.

It has been suggested some form of gated access could be granted. If that access could include bulk queries and the ability to search for domains matching registration information it may superficially appear that such a system would be a middle ground. But such a system would inherently not only require such researchers (who often operate in anonymity for fear of direct and targeted governmental retribution) to identify themselves, but would also log what exactly they are looking for. Such intelligence agencies, through their law enforcement functions would now not only be able to identify which researchers are attempting to unmask hostile intelligence agencies, but it would also give them exactly what we are looking at. To say this would lead to a chilling effect would be an understatement, especially in the light of the recent assassination attempt in the United Kingdom. Many professionals would just stop doing this work and make our democratic processes more vulnerable.

The problem here is that registrants are not given a free choice. To register a domain, they need to give this information or pay more (often more that the registration iteself) to have privacy. Simply make it an opt-out or opt-in system and let the consumer choose which information is displayed about themselves (like Twitter, Facebook, etc). Some will choose to publish this information (businesses for example) because they WANT to be contact. It provides a means to continue reputational analysis of domains so we can

protect against all spam (not just domain renewal scams), and it provides enterprises the tools to verify if they want to allow interconnection of networks. For those who want privacy, they have that choice too.

We need to specify a one-size fits all system for all consumers globally. Let the consumer decide, ICANN should mandate that either choice is free, and we by and large satisfy the regulatory needs here.

Sincerely,
John Bambenek