ICANN's WHOIS System Must Follow Local Laws and Best Practices in Data Protection

The Internet operates in a space far removed from Westphalian sovereignty, where mostly self-regulated private entities set policy through network architecture and engineering decisions. Among these bodies, the Internet Corporation for Assigned Names and Numbers (ICANN), a California-based not-for-profit, holds a monopoly over the technical and functional workings of the Internet's domain name and numbering systems. It is also responsible for the operation of the WHOIS database, a global directory service of domain name registrants. LSE alumnus and member of ICANN's Non-Commercial Users Constituency, Ayden Férdeline, argues that ICANN needs to do more to address concerns about the handling of sensitive personal data, and should adopt international best practices in privacy and data protection.

ICANN has long been accused by detractors of mission creep, but there is one activity that is unquestionably within its remit: allocating unique identifiers like domain names "in the global public interest" and coordinating policy development processes which are "reasonably and appropriately related to these technical functions." ICANN's articles of incorporation also require the organisation to conform to relevant local and international laws. The inconvenient truth, however, is that as a US corporation operating in a transnational space, ICANN cannot be compelled to comply with laws outside of where it has offices, assets or staff, nor has it shown a willingness to do so voluntarily.

National privacy laws around the world are a patchwork quilt of legislation, co-regulation and self-regulation, and the cross-border nature of the Internet can create confusion or ambiguity as to which rights to privacy apply online. But data protection is no longer an abstract concept, with 108 countries now having data privacy laws on their books according to research by the International Privacy Law Library. (Notably, the United States, where ICANN is based, does not extend privacy rights into the digital world). The global trend, as identified by the Organisation for Economic Cooperation and Development, has been towards ensuring that only the absolute minimum amount of information is collected, is done so with the knowledge and consent of the data subject, is used only for the stated purpose, is retained only for as long as is necessary, and is safeguarded against unauthorised access.

The Electronic Frontier Foundation says that ICANN's WHOIS system is "woefully out of step with global best practices in personal data protection and with the associated laws of many countries." This is because when a new domain name is registered, registrars collect personally-identifiable information from the individuals or entities responsible for the operation of this network resource, and this information is then automatically published in an online database accessible to any party that wishes to view it. There are no formal opt-out provisions and there is not enough evidence available to properly assess whether or not consumers consciously or consentingly allow their records to be included in the database. My hunch is that most domain name registrants are unaware of its existence.

WHOIS was launched as a directory service to allow Internet service providers to contact a network resource's owner in the event of a technical issue with their website. Over time, use of the directory has evolved organically, and it is now a tool utilised for other purposes: to determine whether or not a domain name is available for purchase; to allow law enforcement agencies to contact the owner of a website; and to aid holders of intellectual property in protecting their assets. However, it has also been used for more nefarious purposes including extortion, cyberbullying,

and identity theft. Intellectual property attorney Karl Auerbach wrote in 2006 that the database causes real and substantial harm "so deep that families who use the Internet to communicate are forced by DNS WHOIS to expose their names, their addresses, their phone numbers, their affiliations – not just of parents but also of their children – to anyone, including predators, 24x7x365."

Over the past 20 years, WHOIS has been subject to dozens of studies, working groups and task forces, which have assessed the usage of the directory and the accuracy of the data it holds, as well as the privacy implications of the collection and provision of access to this data. Stephanie Perrin of consulting firm Digital Discretion has recorded 11 complaints in relation to the database since 1998 from what she terms "the two most relevant associations of global data protection authorities": the Article 29 Working Party on Data Protection, and the International Working Group on Data Protection in Telecommunications. In addition, the European Data Protection Supervisor of the European Commission wrote to ICANN in 2014 to advise that ICANN was collecting data contrary to the "provisions … of the fundamental rights to privacy and the protection of personal data laid down in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union".

As an advocate of data minimisation and protection, I consider it imperative that ICANN clarifies in precise terms what the legitimate purpose is – if, indeed, there even is one – of the registration directory service in today's information-based economy. That there are already third parties such as spammers and criminals who can profit from the existence of these records is reason enough to question the continued collection and publication of this information. There may well be a legal justification or business necessity to collecting accurate contact information of domain name registrants, but the European Court of Human Rights has ruled that the term "necessary" is not synonymous with "indispensable", and the Inter-American Court of Human Rights has said that invasions to privacy must be "proportionate" to the legitimate aim pursued. I find it difficult to imagine that the publication of sensitive personal information in an open database available to everyone on the Internet is the least invasive method of fulfilling data collection requirements.

Given the nature of the Internet as a global network of networks, once sensitive data is out there, the privacy breach is permanent. That's not only bad news for Europeans wanting to exercise their right to be forgotten, for bloggers writing about repressive governments, and for victims of domestic abuse being stalked by former partners, it's also a poor situation for all private subjects whose personal data is being, to paraphrase J.D. Lasica, etched like a tattoo onto their digital skin.

My view is simple: the principle of privacy-by-default strengthens consumer trust in the Internet both as a safe place for commerce and as a uniquely self-governed realm of individual liberty. That ICANN is headquartered in the only economically-advanced country not to have a general right to information privacy is simply not an acceptable reason for an organisation which has committed itself to operating in the "global public interest" to continue to disclose sensitive personal information in a public directory. The good news is that ICANN, unlike many other global decision-making bodies, is fast-moving and has shown itself to be receptive to feedback from the multi-stakeholder community. Its Board welcomes large and complex questions, and empowers the ICANN community with the resources to propose solutions through an open and transparent governance model that treats all stakeholders – be they from academia, business, civil society, government, or another sector – on an equal footing. This results in consensus-based decision-making that is responsive to the concerns of those who must bear the consequences. As a newly formed, Board-initiated working group considers if and how WHOIS should be replaced, I trust that the privacy implications of the WHOIS system will be successfully addressed once and for all.

This blog gives the views of the author and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics and Political Science.

April 21st, 2016 | Data Protection, Featured, Internet Governance, Privacy | 0 Comments