www.intellectualpropertymagazine.com
Intellectual Property Magazine

Picture: Ljupco Smokovski / Shutterstock

Clash of the ICANN

Toni Y Hickey and **Ariel Fox Johnson** look at how privacy laws and accountability clash in the debate on updating ICANN's registration accreditation agreement

Striking the right balance between openness and privacy is a delicate balancing act, and it is one that continues to prove elusive for the powers that govern the internet. Too much openness could leave individuals and businesses vulnerable to cyber threats. Yet too much privacy could make it impossible for law enforcement to respond to such threats. These conflicting interests have been making headlines lately, with Facebook® executives calling for an end to internet anonymity one month and US bills proposed to limit personal data collection the next.

This conflict is in the spotlight at the Internet Corporation for Assigned Names and Numbers (ICANN), an independent non-profit corporation acting as an internet governance body that operates the domain name system. Law enforcement officials and others are, however, putting pressure on ICANN to increase transparency among domain name registrars and registrants. Opponents argue that such a move will diminish privacy rights.

ICANN was created in 1998 and it is intended to offer a multi-stakeholder decision-making approach to the business of selecting and registering internet names and addresses, eg, domain names. ICANN enters into standard form contracts with registrars, such as GoDaddy, who apply for domain names on behalf of registrants. These contracts, known as a registration accreditation agreement (RAA), lay out the rights and obligations of the registrar. The RAA requires registrars to provide "free public query-based access to up-to-date" data for registrations involving the .com, .net, and .org top level domains (TLDs)[1]. The RAA was last updated in 2009, and ICANN is currently considering another update[2]. One stumbling block will be whether the mandatory disclosure provisions[3], required in the 1999 RAA and maintained as a requirement in the 2009 update, will be modified. It remains to be seen how ICANN will attempt to balance the level of privacy protection registrars and internet users would like to maintain, with the level of information subject to mandatory disclosure that law enforcement officials and intellectual property owners have come to expect.

Significantly, RAA contracts are renegotiated every 10 years. This means that in the near future, a number of contracts registered during the .com boom will be up for renegotiation. Additionally, many new contracts are expected to be entered into under the new generic Top Level Domain (gTLD) roll-out, when the application period to become a new registrar opens in early 2012. Further, registrars are required to comply with certain policies adopted pursuant to specific ICANN regulations and procedures, even if those policy decisions are made after the registrar has signed the RAA. Exactly what procedures must be followed in order to impose rules on already-signed RAAs, and what in the RAA is open to revision, is a matter of disagreement among registrars and ICANN. Any newly defined RAA and policy objectives are likely to affect a wide swathe of registrars and their current and future registrants.

Many expect that new RAAs will offer fewer privacy rights to registrars and registrants. Further, with external pressure mounting in favour of openness and public accountability, and ICANN leaders fed up with stalled industry self-regulation, few expect that this current revision will be any different.

What is WHOIS?

ICANN's WHOIS is a protocol which allows the public free access to data on registered domain names and other internet resources. ICANN requires that registrars collect and provide information to the public about the domain names they register, including the registered domain name, its name servers and contact information for the registered name holder.

There are potential conflicts between WHOIS requirements, domestic privacy laws, and consumer protection statutes. The WHOIS database was initially intended as a "white pages" for the internet, and ICANN is committed to ensuring its accuracy and completeness. Thus, unlike other directories, one is not allowed to opt-out of being included. In reality this seems to accomplish neither accuracy nor completeness. The inability to opt-out encourages registrants who would rather not be listed to provide incomplete or inaccurate information. Just how many of the WHOIS records are inaccurate? ICANN conducted a 2010 study of 2400 domain names registered with the top five gTLDS. The study found that close to 30% of sites listed information that turned out to be undeliverable addresses, names that did not link, or information that did not allow location of the owner. Only 23% of sites strictly complied with ICANN's requirements[4].

WHOIS has also led to the use of privacy and proxy service providers. A privacy service provider allows a registrant to hide their identity, by letting the registrant have the privacy service provider's phone number, address, and/or email address be listed as contact information in the WHOIS directory. A proxy service provider allows for even more anonymity. The proxy service provider will register the domain name for itself, and then license it to the registrant. ICANN has estimated that around 18% of domain names registered under the five top gTLDS (.com, .org, .net, .info, and .biz) have used privacy or proxy services, with proxy service providers being the more popular choice[5]. Private registration services represent an abyss for bad faith domain name registrations (ie, cybersquatters) or trademark infringers and significantly impact a brand owner's ability to identify and pursue the alleged infringers. Instead of being able to contact an infringer directly with a cease-and-desist letter or a subpoena, rightsholders can be forced to sue the registration service first. Namecheap, a proxy service provider that offers WHOISGUARD to protect registrant's identities, has been repeatedly sued based on complaints of infringing websites it registered. Under ICANN's uniform domain-name dispute resolution (UDRP), if there is a dispute, the private or proxy service providers must provide the registrant's name and contact information into

WHOIS to avoid potential liability for contributory trademark infringement[6]. The liability of the proxy service could in some situations provide little comfort for rightsholders, as at least one proxy service (Whois privacy protection service) has not only failed to reveal its registrants, but failed to respond to numerous complaints filed against it under the UDRP.

ICANN has a WHOIS review team seeking to resolve these issues. The review team assesses the "extent to which WHOIS policy is effective and its implementation meets the legitimate needs of law enforcement and promotes consumer trust". The WHOIS review team is also conducting analysis to determine whether ICANN has met its commitments to allow for timely, unrestricted and public access to complete WHOIS information. This includes registrant, technical, billing and administrative contact information and whether ICANN is appropriately enforcing policy related to WHOIS subject to applicable laws. Among these initiatives, there are studies to determine the extent of misuse of information in the WHOIS database, such as phishing (attempting to acquire information such as usernames by masquerading as a trustworthy entity) and identity theft. There are also studies to determine the extent to which harmful websites seek to hide between privacy/proxy services and how such services respond to requests for information.

Moving forward

These studies should provide a basis for ICANN's decisions moving forward. For years law enforcement officials have been putting pressure on ICANN to have more accountability and transparency. In 2009, law enforcement, including the US Department of Justice and the FBI as well as other national agencies, like the UK's Serious Organised Crime Agency, proposed 12 amendments to the RAA. These recommendations would require registrars to collect accurate and complete data of all registrants at the time of registration and verify periodically after to ensure such registry information is accurate and complete. Some of these recommendations are no-brainers, such as requiring that registrars provide a physical address and display the name of their chief executive officer, president, or other responsible officers. Others – such as a requirement to immediately publish WHOIS data for registrants using privacy and proxy services if violations are found – are receiving more pushback from registrars, who argue not all of the recommendations are even technically feasible. Additionally, law enforcement recommends that the RAA should not explicitly condone or encourage the use of proxy registrations or privacy services, and that ICANN limit proxy/privacy registrants and regulate them similar to other registrars. Law officials have also pushed for ICANN to perform due diligence investigations on registrar and registries before accrediting them to register names as well as periodically after. This would include conducting criminal, credit, financial and corporate structure checks as well as WHOIS compliance audits.

At the ICANN talks in October 2011 in Dakar, ICANN officials indicated that the industry's lack of consistent self-regulation was causing government bodies to threaten to move away from the multi-stakeholder, decision-making model and to force even more direct government regulation. Government bodies are not the only parties concerned with ICANN. ICANN is a self regulating body, and parties are concerned that they generate significant fees, but seem unresponsive to industry pressure (for example, going forward with the gTLD roll-out despite industry opposition). Governments have expressed frustration that after two years of discussion, some are still opposed to listing names and addresses on websites, for example. ICANN and registrars agreed to a renegotiated new RAA contract, with a deadline of March 2012, when ICANN will have its 43rd public meeting in San Jose, Costa Rica.

These renegotiations are likely to be very complex, with legitimate concerns from all parties that do not present a simple solution. The potential for immediate WHOIS information disclosure, when a registrant is using a proxy or privacy service, if such an entity is found to be violating "terms of service", "including but not limited to the use of false data, fraudulent use, spamming and/or criminal activity", could create enormous privacy concerns[7]. As the uproar over the US Department of Justice's proposed amendments to the Computer Fraud and Abuse Act (criminalising violations of "terms of service") have demonstrated, unintentional violations of "terms of service" are commonplace and creating criminal or other consequences for such violations seems heavy handed to various vocal contingencies.

And, at the same time that some government groups are asking ICANN to increase registrant transparency by providing full contact information online, others in government are introducing bills intended to limit information collection and dissemination. Recent US bills intended to strengthen consumer privacy protection are the Kerry-McCain Commercial Privacy Bill of Rights Act of 2011 and Democrat Rep Rick Boucher's proposed privacy bill in 2010. Both bills attempt to add meaningful restrictions to the unfettered access to private data that arguably currently exists.

Analysis

All of these conflicting proposals demonstrate growing concern over security on the internet, the safety of online data and the ability of law enforcement to respond to cyber threats. As RAAs are renegotiated, decision makers will have to grapple with whose rights are more important – the public, the government, the registrant, the registrar, or ICANN itself. ICANN must find a way to balance the privacy interests of domain name registrants with its commitment to publicly accessible data about registrants that is accurate and complete. If ICANN cannot find the right balance, government officials may take matters into their own hands, and lawmakers have certainly demonstrated a comfort level and a willingness to legislate in this area. Rightsholders may lose some ground with new RAAs, but a compromise solution is likely better for rightsholders in the long run than losing the ICANN multi-stakeholder model altogether.

Footnotes

1. ICANN registrar accreditation agreement, 9 November 1999, Section E 1 (a-f).
2. ICANN registrar accreditation agreement, May 2009, Section 3774.
3. Examples of mandatory disclosures required include the identity of the registrar, the original date of the registration and the expiration date of the registration.
4. http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf.
5. http://www.icann.org/en/compliance/reports/privacy-proxy-registration-services-study-14sep1--en.pdf.
6. See eg, *Solid Host, NL v NameCheap, Inc*, 2009 US Dist LEXIS 63423 (CD Cal 19 May, 2009).
7. Law Enforcement Due Diligence Recommendations for ICANN – Seoul (Oct 2009).

Authors

Ariel Fox Johnson is an associate with Foley & Lardner LLP and a member of the IP litigation and trade secret/noncompete specialty practices. She focuses on patent, trademark, advertising, privacy, copyright, trade secret, unfair competition and new media matters.

Toni Y Hickey is senior counsel with Foley & Lardner LLP and previously served as deputy chief of staff for the office of the under secretary of commerce for intellectual property.