Analysis

Want to set up a website? The 'Five Eyes' want your personal data

Chris Jones

New global rules agreed in June by the Internet Corporation for Assigned Names and Numbers (ICANN) mean that personal data of anybody registering a website domain name will be retained by private companies for up to two years. The provisions were included following demands made by law enforcement agencies and governments of the 'Five Eyes' intelligence alliance countries – Australia, Canada, New Zealand, the United Kingdom and the United States. EU member states' data protection authorities have argued that the new rules are illegal.

Names and numbers

An organisation called the Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for ensuring global coordination in the internet's technical infrastructure. [1] To do this it coordinates agreement on technical requirements and policies through a "bottom-up, consensus-driven, multi-stakeholder model" that includes, amongst others, governments, companies and non-governmental organisations. [2]

Companies that want to be authorised to sell new "generic top level domains" (gTLDs, current examples include .com and .org) are obliged to sign up to the 2013 Registrar Accreditation Agreement (RAA, agreed in June this year), which governs the relationship between ICANN and domain name registrars (companies that sell domain names). ICANN estimates that the new gTLD process will generate "possibly 1,400 new names" [3] and major domain registration firms have already signed up to the new RAA. [4] Current applications are seeking to add .food, .legal, .music and even .politie (applied for by the Dutch Police) to the more traditional .com, .net and .org. [5]

The previous RAA (agreed in 2009) required registrars to make available a variety of information about domain names (referred to formally as Registered Names) and their owners (Registered Name Holders). This included:

- The name of the Registered Name;
- The names of the primary nameserver and secondary nameserver(s) for the Registered Name;
- The identity of the registrar (the company which is used by a Registered Name Holder or registrant to register a domain name);
- The original creation date of the registration;
- The expiration date of the registration;

- The name and postal address of the Registered Name Holder;
- The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name;
- The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name; and
- The name and (where available) postal address, e-mail address, voice telephone number, and fax number of the billing contact.

This information is stored in the registrars' databases (or a subcontracters' database) and made available publicly through the WHOIS function, a protocol used for "querying databases that store the registered users or assignees of an internet resource, such as a domain name". [6] Registrants can exclude the publication of their personal details, for a fee, through the use of proxy registration services. If they do so their personal details will not be published and instead the contact details of the proxy service will be retained and made publicly available by the registrar.

Under the 2009 RAA there is also an obligation for registrars to retain other information for three years following the deletion of an account or its transfer to a different registrar. This includes the dates and times of submission of domain registration data, all written correspondence between the registrar and Registered Name Holders, and "records of the accounts of all Registered Name Holders with Registrar, including dates and amounts of all payments and refunds".

New rules

Under the 2013 RAA a host of new conditions and data retention obligations have been introduced on the basis of "recommendations" from law enforcement agencies from Australia, Canada, New Zealand, the UK and the US. Many major firms have already signed up to the new rules and eventually all but "rogue" registrars will operate by them. Those purchasing a domain name will be obliged to provide all the data listed above as well as doing the following:

- Verify your phone number or email address (when you register a domain, transfer it to a new registrar, or transfer ownership of a domain) – "if you don't do this within 15 days, your registration can be suspended or terminated. This applies to changes made to domains registered prior to the new RAA, too";
- Your contact information has to be kept up-to-date to the extent that you must inform the registrar within seven days of any changes, and "failure to respond to a registrar's inquiry concerning accuracy of contact details within 15 days can result in your domain being suspended or cancelled"; and
- If you use a WHOIS proxy or privacy service, they will have to escrow (keep in trust) your actual contact details, which can be accessed by ICANN only in the event the registrar loses its accreditation or goes out of business, a measure "designed to protect registrants. Previously, if a registrar went out of business, ICANN and the new registrar that took over the domains may have had no idea who actually owned a domain that was registered with a proxy". [7]

The data to be held under the 2009 agreement for three years following termination or transfer of a contract has had the retention period reduced to two years under the 2013 agreement. While this may sound more privacy-friendly, the same two year retention period following termination or transfer of a domain name will also apply to new sets of data about registrants not included in the 2009 agreement:

- First and last name or full legal name;
- First and last name or, in the event registrant is a legal person, the title of the registrant's administrative contact, technical contact, and billing contact;

- Postal address, email address, and telephone number of registrant, administrative contact, technical contact and billing contact;
- WHOIS information;
- Types of domain name services purchased; and
- To the extent collected by Registrar, credit or debit card details, current period third party transaction number, or other recurring payment data.

And, for 180 days following any "relevant interaction" with a Registered Name Holder:

- Information regarding the means and source of payment reasonably necessary for the Registrar to process the Registration transaction, or a transaction number provided by a third party payment processor;
- Log files, billing records and, to the extent collection and maintenance is commercially practicable or consistent with industry standards, other records containing source and destination information of communications relating to domain name registration, including and without limitation:
    - Source IP address, HTTP headers;
    - Telephone, text or fax number;
    - Email address, Skype handle/username, or instant messaging identifier;
- Log files and, to the extent collection and maintenance is commercially practicable or consistent with industry standards, other records associated with the domain name registration containing dates, times and time zones of communications and sessions, including initial registration.

ICANN is also due to establish a Proxy Accreditation Program by 1 January 2017 at the latest, which seems likely to permit the provision of proxy and privacy services only by "individuals or entities accredited by ICANN". [8] Until the Accreditation Program is established, a Specification on Privacy and Proxy Registrations attached to the 2013 RAA applies.

police.net

The new provisions in the 2013 RAA – which are a "highlight" of the agreement, according to ICANN [9] – came about after extensive lobbying by law enforcement agencies and governments of the countries that make up the 'Five Eyes' intelligence community – Australia, Canada, New Zealand, the United Kingdom and the United States.

The first formal approach to ICANN appears to have been made in October 2009 when the Australian Federal Police, the US Department of Justice, the FBI, the New Zealand Police, the Royal Canadian Mounted Police and the UK's Serious Organised Crime Agency supplied ICANN with "due diligence recommendations for ICANN to adopt". In a joint paper, the agencies argued that:

> "The amendments are considered to be required in order to aid the prevention and disruption of efforts to exploit domain registration procedures by Criminal Groups for criminal purposes. The proposed amendments take account of existing EU, US, Canadian and Australian legislation and those countries commitment to preserving individual's right to privacy. These amendments would maintain these protections whilst facilitating effective investigation of Internet related crime." [10]

In April 2010 the Chairman of ICANN's Governmental Advisory Committee (GAC), Janis Karklins, wrote to the ICANN Board's chairman, Peter Dengate Thrush, to inform him of support for the law enforcement agencies' proposals from two secretive, high-level working groups: the Interpol Working Party on IT Crime-Europe and the G8 Lyon-Roma Group's High Tech Crime subgroup. The G8 Lyon-Roma group aims to "better align G8 counterterrorism

and anti-crime policies" and has met this year in both the US (in January) [11] and the UK (in April and November). [12] The Council of Europe's 'Octopus Interface conference' on cybercrime also encouraged ICANN "to implement these recommendations without delay". [13] In March 2010 the GAC issued a communique which said it expected that the proposals would be "thoroughly examined and taken into consideration". [14]

The GAC is one of several groups that play a part in the complex "bottom-up, consensus-driven, multi-stakeholder model" through which ICANN functions. The model has apparently been the cause of some discontent to both the EU and US, [15] with the EU accused of seeking "to completely subordinate ICANN as an institution" through the publication by the Commission of six papers "attacking almost every aspect of ICANN". This was seen by Milton Mueller of the *Internet Governance Project* as "payback" for the ICANN Board's refusal to treat the European Commission's views on top level domains as binding instructions, something they are not obliged to do. [16]

The Register reported of ICANN's October 2011 meeting in Dakar that the Five Eyes governments had "forced domain name registrars into agreeing to renegotiate their contracts with industry overseer ICANN". This was expected to "water down domain name privacy services and could make it easier for law enforcement and intellectual property interests to take down websites". The UK government's representative, Mark Carvell (an official from the Department for Culture, Media and Sport), was one of many government and law enforcement representatives at the Dakar meeting who had "grown frustrated by the registrars' lack of progress voluntarily implementing [their] recommendations". He argued: "This is politically significant. They shouldn't mess around here. Cybercrime is on the agenda." [17]

By March 2012 the agencies had formulated their recommendations into a series of more formal proposals, [18] and during another round of negotiations on the new RAA, it was noted that law enforcement authorities were present "in full force". Alongside the US Department of Justice and FBI officials at the ICANN conference were representatives of the US Department of Homeland Security and Immigration and Customs Enforcement, as part of "a large group of over 10… from all around the world". [19] The agencies' demands were eventually met in the 2013 RAA, as outlined in an ICANN report on the negotiations, which contains a chart of the 12 law enforcement recommendations and "indicates how they have all been addressed". [20]

Data protection complaints

The new data retention provisions were included in the 2013 RAA despite data protection concerns raised by bodies such as the Council of Europe's Consultative Committee of the Data Protection Convention and the Article 29 Working Party (A29WP), which is made up of a representative of the data protection authority of every EU Member State, a representative of the European Data Protection Supervisor, and a representative of the European Commission.

The A29WP have said that companies based in the EU should be able to opt-out of the data retention demands, which they argue are in breach of European privacy laws. A letter from the Working Party to ICANN's chairman Steve Crocker and CEO Fadi Chehadé, sent three weeks before the approval of the RAA on 27 June 2013, argued that:

> "The proposed new data retention requirement does not stem from any legal requirement in Europe. It entails the extended processing of personal data such as credit card and communication data by a very large number of registrars. The fact that these data may be useful for law enforcement (including copyright enforcement by private parties) does not equal a necessity to retain these data after termination of

> the contract… the Working Party finds the benefits of this proposal disproportionate to the risk for individuals and their rights to the protection of their personal data.
>
> "Secondly, the Working Party reiterates its strong objection to the introduction of data retention by means of a contract issued by a private corporation in order to facilitate (public) law enforcement. If there is a pressing social need for specific collections of personal data to be available for law enforcement, and the proposed data retention is proportionate to the legitimate aim pursued, it is up to national governments to introduce legislation that meets the demands of article 8 of the European Convention on Human Rights and article 17 of the International Covenant on Civil and Political Rights." [21]

The Working Party had first raised its concerns in September 2012, and was joined the month after by the Council of Europe. In a letter to Robin Gross, head of ICANN's Non-Commercial Users Constituency, the Consultative Committee of the Convention Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data backed up the A29WP's position, saying that it "fully shares the concern raised". [22]

At this point, however, the European Commission, did not seem to agree. The Commission "stressed" during negotiations on the new RAA in October 2012 that the A29WP "does not represent the official EU position". A report for *Domain Incite* quoted the Commission's representative on ICANN's Governmental Advisory Committee:

> "Just to put everyone at ease, this is a formal advisory group concerning EU data privacy protection… They're there to give advice and they themselves, and we as well, are very clear that they are independent of the European Union. That gives you an idea that this is not an EU position as such but the position of the advisory committee." [23]

Despite the Commission's apparent dismissal of its concerns, the A29WP later told *Statewatch* that "the European Commission has always underlined the importance of compliance with the data protection legislation applicable in the EU and we can only support this position". EU officials dealing with internet policy have also expressed concern to *Statewatch* about the new rules. At a meeting of the ICANN GAC in July 2013 in Durban the Commission's representative joined the German and Dutch delegations in expressing "concerns as regards… data protection and in particular as regards the purpose of the processing and the retention of the data." [24]

However, concerns from all parties on the issue have been largely ignored by ICANN. It rejected the claims made by the Article 29 Working Party and does not consider its letter to be a valid basis for registrars to exercise the waiver from the data retention requirements. Journalist Kevin Murphy has remarked:

> "It seems that when the privacy watchdogs of the entire European Union tell ICANN that it is in violation of EU privacy law, that's not taken as an indication that it is in fact in violation of EU privacy law." [25]

"Make-believe security measures"

It has been suggested that the European Commission takes its lead in ICANN negotiations from the USA. Amadeu Abril of the Internet Council of Registrars (CORE, a business association for internet domain name registrars based in Switzerland) told *Statewatch* that EU governments and institutions "seem to buy the rhetoric from US law enforcement agencies and equate more security with more data retention and data publication, without

even giving second thought to it," and that US law enforcement agencies put "really heavy pressure" on delegations at ICANN. Abril said that the data retention requirements in the 2013 RAA are "make-believe security measures" that "create risks for legitimate users, burdens for registrars, and the bad guys have long learned how to deal with it all".

CORE plans to request from ICANN the waiver from the data retention requirements. However, it will not be able to use the A29WP letter to do so – ICANN does not consider this to be legal grounds to justify the waiver as it recognises the A29WP as "an authority, but… not a legal authority". [26] Registrars will instead have to identify "the specific [national] laws or regulations upon which the waiver request is based". [ref ICANN 20 September 2013 letter] This is despite the fact that the A29WP, made up of the EU's national data protection authorities, specifically stated in their June letter to ICANN that they sought "to provide a single statement for all relevant registrars targeting individual domain name holders in Europe," in order "to avoid unnecessary duplication of work by 27 national data protection authorities".

A Luxembourg-based company, EuroDNS, has announced its intention to apply for written guidance from the Luxembourgish data protection authority so that it can be submitted to ICANN. [27] When – or if – new EU data protection rules come into force, [28] companies will be able to refer to a single European legal regime to back up their arguments. In the meantime many more companies will be seeking the advice of their national data protection authorities.

Private contract, public law enforcement

In terms of its intrusiveness, it's not on the same scale as the Internet surveillance operations run by US and UK spy agencies, or the mandatory retention of telecommunications data. But the process by which the new ICANN RAA came about bears some similarities to that which led to the EU's notorious Data Retention Directive: law enforcement demands are cooked up in secretive 'global governance' bodies and working parties, taken up by national governments in negotiations, and eventually passed into law (or, in this case, a binding private contractual agreement) against the arguments of privacy advocates and, seemingly, against the law.

The new ICANN rules also reflect the Data Retention Directive in that they seek to make available to law enforcement authorities personal data obtained and stored by private companies. The EU's Passenger Name Record (PNR) agreements with the USA, Australia and Canada, where airline and travel companies are obliged to pass on information collected about passengers to state authorities for further processing, show a similar approach. The A29WP pointed out in its June 2013 letter to ICANN that just because "these personal data can be useful for law enforcement does not legitimise the retention of these personal data after the termination of the contract." This echoes a wider point made by the European Data Protection Supervisor. He has argued that "the general trend to give law enforcement authorities access to the data of individuals, who in principle are not suspected of committing any crime, is a dangerous one." [29]

Unlike the Data Retention Directive and the PNR agreements, companies based in Europe will at least have a chance to request to opt out of the RAA's data retention requirements, although these requests will be subject to the approval of ICANN. [30] As revelations about GCHQ, the NSA and other spy agencies' surveillance operations continue, the inclusion of the demands of the 'Five Eyes' in the new ICANN Agreement demonstrates in a smaller way the hunger of law enforcement agencies for personal data in the digital age.

November 2013

NOTE: This article was amended in January 2013 to take account of changes in the European Commission's position on data protection concerns over the new RAA.

[1] "To reach another person on the Internet you have to type an address into your computer -- a name or a number. That address must be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination, we wouldn't have one global Internet." More information: ICANN, 'Welcome to ICANN!', http://www.icann.org/en/about/welcome
[2] 'ICANN, 'ICANN Organizational Chart', http://www.icann.org/en/groups/chart
[3] ICANN, 'Internet Domain Name Expansion Now Underway', 23 October 2013, http://www.icann.org/en/news/press/releases/release-23oct13-en
[4] Andrew Allemann, 'First five domain name registrars sign 2013 RAA', *Domain Name Wire*, 15 July 2013, http://domainnamewire.com/2013/07/15/first-five-domain-name-registrars-sign-2013-raa/
[5] ICANN, 'New gTLD current application status', https://gtldresult.icann.org/application-result/
[6] Wikipedia, 'Whois', https://en.wikipedia.org/wiki/Whois
[7] Andrew Allemann, 'What the new RAA means for YOU, the domain registrant', *Domain Name Wire*, 23 April 2013, http://domainnamewire.com/2013/04/23/what-the-new-raa-means-for-you-the-domain-registrant/
[8] ICANN, 2013 Registrar Accreditation Agreement, http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm
[9] ICANN, 'Special Meeting of the ICANN Board', 27 June 2013, https://www.icann.org/en/groups/board/documents/resolutions-27jun13-en.htm#2.b
[10] ICANN, 'Report on the Conclusion of the 2013 Registrar Accreditation Agreement Negotiations', 16 September 2013, http://gnso.icann.org/en/node/41795
[11] U.S. Department of State, 'United States Hosts the G8 Roma-Lyon Group on Counterterrorism and Counter-crime', 14 January 2013, http://www.state.gov/r/pa/prs/ps/2013/01/202787.htm
[12] G8UK, 'Calendar of Events', http://www.statewatch.org/news/2013/dec/2013-g8-uk-pres-calendar.pdf; Foreign & Commonwealth Office, 'G8 Foreign Ministers' meeting statement', gov.uk, 11 April 2013, https://www.gov.uk/government/news/g8-foreign-ministers-meeting-statement
[13] ICANN, 'Final Report on Proposals for Improvements to the Registrar Accreditation Agreement', 18 October 2010, p.148, http://gnso.icann.org/en/node/15005
[14] Ibid., p.143
[15] Jennifer Baker, 'E.U., U.S. call for ICANN Internet governance reforms', *Computerworld*, 13 May 2011, http://www.computerworld.com/s/article/9216687/E.U._U.S._call_for_ICANN_Internet_governance_reforms
[16] Milton Mueller, 'Payback time: The European Commission papers on ICANN', *Internet Governance Project*, 2 September 2011, http://www.internetgovernance.org/2011/09/02/payback-time-the-european-commission-papers-on-icann/; background: Milton Mueller, 'Competition policy letters to ICANN part of a US-EC "plot"', *Internet Governance Project*, 19 June 2011, http://www.internetgovernance.org/2011/06/19/competition-policy-letters-to-icann-part-of-a-us-ec-plot/
[17] Kevin Murphy, 'Privacy warning as cops lean on domain registrars', *The Register*, 27 October 2011, http://www.theregister.co.uk/2011/10/27/privacy_warning_as_cops_lean_on_domain_registrars/
[18] 'Law Enforcement Recommendations Regarding Amendments to the Registrar Accreditation Agreement', 3 March 2011, http://www.statewatch.org/news/2013/dec/icann-raa-lea-recommendations-11-03-01.pdf
[19] Michael Berkens, 'One Things Is Clear From ICANN: Law Enforcement Is Out in Full Force & Your Registration Costs Will Go Up', *The Domains*, 14 March 2012, http://www.thedomains.com/2012/03/14/one-thing-is-clear-from-icann-law-enforcement-is-out-in-full-force-your-registrations-costs-will-go-up/
[20] ICANN, 'Report on the Conclusion of the 2013 Registrar Accreditation Agreement Negotiations', 16 September 2013, http://gnso.icann.org/en/node/41795
[21] Letter from Article 29 Working Party to Steve Crocker and Fadi Chehadé, 'Statement on the data protection impact of the revision of the ICANN RAA', 6 June 2013, http://www.statewatch.org/news/2013/dec/a29wp-letter-icann.pdf
[22] Letter from Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD) to Robin Gross, 'RAA's review and privacy compliance', 8 October 2012, http://www.statewatch.org//news/2013/dec/coe-whois-privacy.pdf

[23] Kevin Murphy, 'EU plays down "unlawful" Whois data worries', *Domain Incite*, 17 October 2012, http://domainincite.com/10771-eu-plays-down-unlawful-whois-data-worries
[24] ICANN, 'Transcript: GAC Plenary – Staff Update on New gTLDs', 13 July 2013, http://durban47.icann.org/node/40877
[25] Kevin Murphy, 'ICANN says Article 29 letter does not give EU registrars privacy opt-out', *Domain Incite*, 15 July 2013, http://domainincite.com/13724-icann-says-article-29-letter-does-not-give-eu-registrars-privacy-opt-out
[26] Kevin Murphy, 'ICANN says Article 29 letter does not give EU registrars privacy opt-out', *Domain Incite*, 15 July 2013, http://domainincite.com/13724-icann-says-article-29-letter-does-not-give-eu-registrars-privacy-opt-out
[27] Luc, 'Your privacy matters to EuroDNS', *EuroDNS*, 10 October 2013, http://blog.eurodns.com/privacy-matters-us/
[28] Jeremy Fleming, 'EU to push ahead on data protection despite UK opposition', *Euractiv*, 28 October 2013, http://www.euractiv.com/specialreport-digital-single-mar/commission-push-ahead-data-prote-news-531357
[29] European Data Protection Supervisor, 'Smart borders: key proposal is costly, unproven and intrusive', 19 July 2013, http://www.statewatch.org/news/2013/jul/eu-edps-smart-borders-prel.pdf
[30] ICANN, 'ICANN Process for Handling Registrar Data Retention Waiver Requests', http://www.icann.org/en/resources/registrars/updates/retention/waiver-request-process