



COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

ICANN IMPLEMENTATION ADVISORY GROUP

on the Review of Existing ICANN Procedure for
Handling Whois Conflicts with Privacy Laws

November 17, 2015

On October 5, 2015, ICANN released a report proposing improvements to the current policy development process (PDP), the mechanism through which domain registrars can notify ICANN about conflicts between ICANN’s Registrar Accreditation Agreements (RAA) and privacy laws. In the preliminary report, entitled “Initial Report on the Implementation Advisory Group Review of Existing ICANN Procedure for Handling Whois Conflicts with Privacy Laws,” ICANN proposed a change to the PDP and requested public comment.

EPIC submits these comments to explain how the Implementation Advisory Group’s (IAG) proposal fails to ensure registrar compliance with privacy laws, and will not meaningfully change the system that allows for routine privacy violations of domain name registrants.

EPIC is a public-interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues, and to protect privacy, the First Amendment, and related human rights.¹ EPIC has served on ICANN’s Whois Privacy Steering Committee, and on the Non-Commercial Users Constituency Task Force. EPIC has also written extensively on the Whois database and its implications on privacy.²

In a 2001 letter to Congress, EPIC warned lawmakers of the privacy risks faced by U.S. Internet users who register domain names.³ In 2003, on behalf of the Non-

¹ *About EPIC*, EPIC (2015), <https://epic.org/epic/about.html>.

² *See Whois*, EPIC (2015), <https://epic.org/privacy/whois/>.

³ Letter from EPIC to Rep. Fred Upton et al. (Feb. 16, 2001) (describing the ease with which personally identifiable information about registrants is obtained and the practice by

Commercial Users Constituency, EPIC submitted a report to the Generic Names Supporting Organization's (GNSO) Whois Task Force urging the integration of the Organization for Economic Cooperation and Development's (OECD) Recommendations Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereinafter "OECD Privacy Guidelines") into the management of the Whois database.⁴ In a 2006 brief to the U.S. Court of Appeals for the Fourth Circuit, EPIC supported a challenge to a government policy to publish the personal contact information of all .us registrants.⁵ EPIC argued that "[T]he right to free speech is not only the right to speak without giving a name, but the right not to disclose personal information as a condition of speech."⁶ Then in 2007, EPIC submitted comments to ICANN on its "Preliminary Task Force Report on Whois Services," again urging ICANN to remove registrant information from the Whois database, and instead assign an operational point of contact.⁷

EPIC now submits the following comments on the proposed PDP change:

The "alternative trigger" proposal wrongfully shifts the burden of complying with privacy laws to registrars and government agencies.

According to ICANN, the original goal of the PDP was "to facilitate reconciliation of any conflicts between local/national mandatory privacy laws or regulations and applicable provisions of the ICANN contract."⁸ However, ICANN's current proposed amendments would not further that goal.

Under the IAG's "alternative trigger" proposal, a registrar would "seek a written statement from the government agency charged with enforcing its data privacy laws indicating that a particular Whois obligation conflicts with national law and then submit that statement to ICANN."⁹ This proposal fails to address privacy law conflicts for several reasons.

registrars to sell bulk access to registrant information sale of registrant data), https://epic.org/privacy/internet/ICANN_privacy.html.

⁴ EPIC, *Privacy Issues Report: The Creation of A New Task Force is Necessary For an Adequate Resolution of the Privacy Issues Associated With WHOIS*, (Mar. 10, 2003), https://epic.org/privacy/whois/privacy_issues_report.pdf.

⁵ See Brief for EPIC as Amicus Curiae Supporting Petitioner, *Peterson v. NTIA*, 478 F.3d 626 (4th Cir. 2007), https://epic.org/privacy/peterson/epic_peterson_amicus.pdf.

⁶ *Id.* at 2.

⁷ EPIC, Comments of EPIC to ICANN Whois Task Force on Preliminary Task Force Report on Whois Services (Jan. 12, 2007), <https://epic.org/privacy/whois/comments.html>.

⁸ Matt Childs, *WHOIS and national law conflicts IAG Home*, ICANN (last updated Dec. 9, 2014),

<https://community.icann.org/display/WNLICI/WHOIS+and+national+law+conflicts+IAG+Home>.

⁹ *Initial Report on the Implementation Advisory Group Review of Existing ICANN Procedure for Handling Whois Conflicts with Privacy Laws*, ICANN Implementation Advisory Group

First, the proposal wrongfully shifts the burden of assessing compliance with privacy laws to individual registrars. Many registrars do not have the capacity or resources to seek consultations from data protection agencies. Moreover, the proposal would improperly relieve ICANN of its duty to ensure that the organization's contracts comply with privacy laws. ICANN stores and processes the personal information of registrants, and therefore has a duty to safeguard that information. Additionally, ICANN exercises unique power and influence as an Internet governance body. Any procedure that relieves ICANN of the duty to ensure that its contracts are consistent with privacy laws is fundamentally flawed.

As IAG member and EPIC Advisory Board Member Stephanie Perrin noted in her dissenting statement, international data protection authorities have repeatedly expressed privacy concerns regarding the Whois database.¹⁰ Because ICANN is undoubtedly on notice that the Whois database conflicts with privacy laws, in particular the European Data Protection Directive, the “alternative trigger” would serve no practical purpose.

Second, it is not reasonable to expect government agencies to provide advisory opinions on private contracts. As a practical matter, data protection authorities lack the resources and legal authority to provide such opinions. Unless an agency has reason to investigate a particular registrar, the agency has no incentive to insert itself into the contracting process. Likewise, a registrar that is not under investigation has no incentive to bring itself to the attention of a data protection authority. In practice the “alternative trigger” would be no different than the current trigger.¹¹ In addition, many countries do not have data protection authorities. In those countries—the United States, for example—the addition of an “alternative trigger” would not provide any additional mechanism to identify a conflict.

ICANN should revise the RAA consistent with widely adopted privacy laws and standards.

ICANN's conflict procedure, focused on considering how privacy law might be consistent with the RAA contracts, is exactly backwards. ICANN should instead revise the RAA consistent with broadly adopted privacy laws and internationally recognized privacy standards.

at 5 (Oct. 5, 2015), <http://whois.icann.org/sites/default/files/files/iag-review-whois-conflicts-procedure-05oct15-en.pdf>.

¹⁰ Statement of Stephanie Perrin at 18–19 (Oct. 5, 2015), <http://whois.icann.org/sites/default/files/files/iag-review-whois-conflicts-procedure-1-4-appendices-05oct15-en.pdf>.

¹¹ *ICANN Procedure For Handling WHOIS Conflicts with Privacy Law*, ICANN (last visited Nov. 17, 2015), <https://www.icann.org/resources/pages/whois-privacy-conflicts-procedure-2008-01-17-en>.

i. The RAA is incompatible with the EU Data Protection Laws.

The “Data Retention Specification” section of the RAA is incompatible with a recent ruling of the Court of Justice of the European Union (CJEU). In *Digital Rights Ireland*, the CJEU set out clear and strict criteria about data retention that apply in every jurisdiction in the European Union.¹²

There, the Court found that a law requiring Internet Service Providers to retain user and subscriber data for law enforcement and national security purposes violates the fundamental rights to respect for private life and data protection because it (1) exceeds the database’s purpose (the purpose-limitation principle); (2) the framework covered, in a generalized manner, all individuals without any differentiation, limitation or exception; (3) the Data Retention Directive failed to lay down any objective criterion about access to the data; (4) the data retention period was set without making any distinction between the categories of data on the basis of the persons concerned or the possible usefulness of the data in relation to the objective pursued; and (5) because of risk of abuse.¹³

Although the Data Retention Directive governed a different type of data collection, the requirements set out by the CJEU should be incorporated into the RAA contracts. The data retention rules for the database at ICANN’s disposal lack the safeguards required by the CJEU’s decision. The RAA requires collection of data beyond what is strictly necessary for the original purpose of the data collection. Moreover, ICANN makes no distinction or exception to the rule that the personal information of every registrant should be public. This practice is not only a breach of privacy and data retention laws but might also cause serious harms to specific individuals or groups including portals of investigative journalists and human rights organizations. Furthermore, there is specified data retention period for the data collected under the RAA. EPIC has expressed before that it is problematic that every Internet user has access to the information collected on registrants. EPIC highlights that Whois data may contribute to identity theft and other fraud.

¹² Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others*, EU:C:2014:238, 2014.

¹³ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

ii. ICANN should look to the OECD's Privacy Guidelines as a starting point for revising the RAA.

As EPIC has previously urged, ICANN should look to the OECD Privacy Guidelines when revising the Whois privacy provisions in the RAA.¹⁴ The OECD Privacy Guidelines offer important international consensus on and guidelines for privacy protection. The OECD Privacy Guidelines establish eight principles for data protection that are widely used as the benchmark for assessing privacy policy and legislation.¹⁵ They provide a well thought-out solution to challenging questions about international consensus on privacy and data protection that directly implicate WHOIS policies and practices. More importantly, the OECD Privacy Guidelines serve as a basis for a sensible WHOIS policy.

iii. Significance of the Schrems Decision

Finally, we note that the recent decision of the Court of Justice of the European Union which invalidated the Safe Harbor arrangement could be directly applicable to the practices of ICANN concerning the collection and use of personal data. As the Court made clear in that judgment, the processing of data of Europeans must comply with the European Union Data Protection Directive, 95/46, and Articles 7, 8, and 47 of the Charter of Fundamental Rights. The Court's judgment also indicates that any one of the national data protection agencies in the European Union could enforce privacy and data protection rights.

Fifteen years of inaction is enough. We strongly urge ICANN to get its privacy house in order.

Marc Rotenberg
EPIC President

John Tran
EPIC FOIA Counsel

Fanny Hidvegi
EPIC International Law Fellow

¹⁴ EPIC Privacy Issues Report at 7.

¹⁵ See Marc Rotenberg, *What Larry Doesn't Get: Fair Information Practices and the Architecture of Privacy*, Presented on February 7, 2000 at the Stanford Law School Symposium on Cyberspace and Privacy, http://stlr.stanford.edu/STLR/Symposia/Cyberspace/00_rotenberg_1/article.htm.

Alan Butler
EPIC Senior Counsel

Khaliah Barnes
EPIC Associate Director