Response to the public consultation on Mozilla's TRR policies

About Derechos Digitales

Derechos Digitales is an independent non-governmental organization, founded in 2005, its main offices located in Santiago de Chile. Our aim is the defense and promotion of fundamental rights in the digital environment of Latin America. Standing up for a social change around the respect and dignity of people by using advocacy tools among policymakers, private companies and the general public.

I. Introduction

In response to the public consultation made by Mozilla, the following are a series of legal and technical recommendations to take into account when implementing the Trusted Recursive Resolvers (TRR) Policy in Latin America. As part of our commitment with human rights in the digital environment, we consider DNS encryption mechanisms a necessary advance in privacy and security, and against censorship. The deployment of DNS over HTTPS (DoH) by major browser vendors, and gradually also by ISPs and operating systems is on that path.

Actions adopted at the DNS level has by definition a global impact, proportionality requires that only a particularly high level of abuse and/or harm could potentially justify resorting to such a measure. The DNS actions can severely impact privacy and freedom of expression, amounting for censorship. It is worth recalling the Human Rights Council Resolution on the right to privacy in the digital era, *"the right to privacy can enable the enjoyment of other rights and the free development of an individual's personality and identity, and an individual's ability to participate in political, economic, social and cultural life, and noting with concern that violations or abuses of the right to privacy might affect the enjoyment of other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association"*.[1] The same

[1] A/HRC/42/L.18, available at:<https://undocs.org/A/HRC/42/L.18t>

resolution calls to companies *"to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity, and calls upon States not to interfere with the use of such technical solutions, with any restrictions thereon complying with States' obligations under international human rights law"*.[2]

Metadata retention by the resolver in the course of adoption of any filtering/blocking through the DNS action can impact in the access to information and the right to "digitally" exercise the right to peaceful assembly, among others. In his latest report the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association has observed how, *"over the past decade, States have used technology to silence, surveil and harass dissidents, political opposition, human rights defenders, activists and protesters, and to manipulate public opinion. Governments are ordering Internet shutdowns more frequently, as well as blocking websites and platforms ahead of critical democratic moments such as elections and protests. A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world. While the role that technology can play in promoting terrorism, inciting violence and manipulating elections is a genuine and serious global concern, such threats are often used as a pretext to push back against the new digital civil society"*.[3]

Ensuring to users the benefits of anonymity in the access to content and services in political and rights restrictive contexts can be vital in order to provide protection to the general public, and particularly to ensure the possibility for human rights defenders, journalists and technical experts to continuing using digital services to organize and mobilize for the protection of rights. These are some of the fundamental reasons why we believe that DoH is a technical contribution that could support the better exercise of human rights in our region.

In line with what Mozilla has stated,[4] we also consider that no technical solution is enough to fully guarantee users' rights if it is not complemented with appropriate data policies. This falls fully on line with what has been expressed by the Human Rights Council by saying that *"international human rights law should guide private sector actors and be the basis for their policies"*.[5] Following this

---

[2] Ibid.

[3] UN Special Rapporteur on the rights to freedom of peaceful assembly and of association. A/HRC/41/41, of May 17 2020. "Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", available at: <https://undocs.org/A/HRC/41/41>

[4] See <https://blog.mozilla.org/netpolicy/2019/12/09/trusted-recursive-resolvers-protecting-your-privacy-with-policy-technology/>

[5] See Human Rights Council resolution 38/7 of 5 July 2018. "The promotion, protection and enjoyment of human rights on

address the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, have provided complement to add precision over the digital technology companies' responsibilities to respect human rights in the way is provided by the Guiding Principles on Business and Human Rights.[6] In his opinion, *"In order to fulfill [sic] this obligation, business enterprises should have in place human rights policies and processes –including a policy commitment to meet their responsibility to respect human rights; a human rights due diligence process to identify, prevent, mitigate, and account for how they address, their human rights impacts; and processes to enable the remediation of any adverse human rights impacts that they cause or to which they contribute"*.[7] In the same lines the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression had stated before that *"human rights law gives companies the tools to articulate and develop policies and processes that respect democratic norms and counter authoritarian demands"*.[8]

On the other hand, given the unbalanced configuration of the market and the diversity of regulatory landscape in data protection across jurisdictions, we recognize some of the risks associated with current DoH implementations.[9] While strong policy standards can protect users from being tracked by browsers and DoH providers, there is no control over the potential market centralization[10] with just a few providers set by default in some of the most used browsers worldwide, such as Firefox.

We welcome Mozilla's initiative to crowd-source ideas, not only to deploy DoH by default in clients outside the US, but making their TRR Policy more viable in a diversity of jurisdictions and for a diversity of resolvers. We are convinced that this provides the right incentive for the industry to adopt better privacy standards and a basis for limiting blocking and filtering systems to guarantee both user consent and proportionality. Users' privacy should be the default feature worldwide, not just an option.

---

the Internet", available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/215/67/PDF/G1821567.pdf?OpenElement>

[6] See Human Rights Council resolution 17/4 of 16 June 2011. "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework", available at: <https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf>

[7] UN Special Rapporteur on the rights to freedom of peaceful assembly and of association. Op. Cit.

[8] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/38/35 of 6 April 208. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", available at: <https://www.undocs.org/A/HRC/38/35>

[9] See "US companies to implement better privacy for website browsing" available at <https://edri.org/our-work/us-companies-to-implement-better-privacy-for-website-browsing/>

[10] See "Centralized DNS over HTTPS (DoH) Implementation Issues and Risks", available at <https://tools.ietf.org/html/draft-livingood-doh-implementation-risks-issues-04>

As a Civil Society Organization, our contribution is not focused on technical and operational challenges to adopt DoH, or the state of IT industry in our region. Rather, we offer an overview of desirable human rights standards to be acknowledged in policy regarding DoH deployment. Regarding **privacy and security**, our focus is on exemptions for additional data collection in emergency circumstances; and considerations for third party audits and transparency reports. Regarding **online safety** we take a look on the documented legal requirements to block domain names in Latin America; provide recommendations on how to ensure effective transparency and accountability after required blocking practices for TRRs; share ideas about how to deal with parties that maintain and create block lists; and how to better present information about opt-in filtering endpoints to end users. Finally, we share a few documented cases in Latin America we consider DoH can protect against in the future.

II. Privacy and security

1. Exemptions for additional data collection in emergency circumstances

There are cases in which judicial or law enforcement orders might require additional information in order to identify and adequately protect or repair victims of illicit actions through DNS abuse. In the Inter-American System of Human Rights, the Special Rapporteur for Freedom of Expression has declared that under the regional standards, any regulation requiring ISPs to deploy content blocking or filtering should be restricted to exceptional cases such as child pornography, war propaganda, and hate speech constituting incitement to violence or incitement to genocide, with the additional protection that an independent judge should determine the illegality of the content.[11] The expedition of those actions might require in some circumstances that the exceptional blocking measures are executed immediately but a longer process might follow to identify and remediate victims, for which data might need to be available for a longer period of time. In that sense, a longer period of data retention could be established by a competent judicial authority in emergency circumstances claimed to request technical action at the DNS level by the resolver. It is difficult and mostly arbitrary to define such a period, given that different jurisdictions have very varying procedural periods and capacities to

[11] CIDH. Informe Anual 2008. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo III (Marco Jurídico Interamericano del Derecho a la Libertad de Expresión). OEA/Ser.L/V/II.134 Doc. 5 rev. 1. 25 de febrero de 2009. Párr. 261. CIDH. Informe Anual 2015. Informe de la Relatoría Especial para la Libertad de Expresión . Capitulo IV (Discurso de odio y la incitación a la violencia contra las personas lesbianas, gays, bisexuales, trans e intersex en América). OEA/Ser.L/V/II. Doc. 48/15. 31 de diciembre de 2015. Párr. 18

execute them. The rule could be something in line with demands for minimizing the period of data retention, establishing a maximum period of retention (per example 90 days), and establish the obligation of the requesting authority to specify and justify in its request the extended duration of the data retention demanded within that framework.

Regarding transparency obligations, resolvers should maintain a publicly available policy with a clear process to trigger emergency circumstances requests, including a clear point of contact to submit the emergency circumstances request. The policy should provide clear information about the specific fields for data that will be retained for extended period of time in emergency circumstances, how will be defined those emergency circumstances and what will be the authorities able to make those requests (in Latin America given the aforementioned standard only judicial authorities should be considered, in other jurisdictions this might vary.

Additionally, the transparency report published yearly should provide statistics as detailed as possible, and to the extent such disclosure is not prohibited by law, about the number of received emergency circumstances requests over the year, the categories of abuses related to those requests, the type and jurisdiction of the demanding authorities, and the responses to those requests. All these statistics are essential to provide a record of the policy implementation and to shed light on how the resolver handles law enforcement requests for user data. This is essential for transparency and predictability of the system, as well as provide opportunity to better educate all system's participants.

2. Considerations for third-party audits to confirm compliance with TRR Policies

To be meaningful, third-party audits need to be conducted by entities with the ability and knowledge to approach the assessment from a human rights impact perspective. Other institutions conducting this type of external audits usually create a pool of accredited auditors, from which the companies assessed can select a qualified auditor.[12] Auditors must be independent of the companies they assess, and they must be competent by adhering the highest professional standards in their work, grounded in the fundamental principles of integrity, objectivity, confidentiality, and professionalism.

The prospective auditors should be able to demonstrate knowledge, expertise, and experience with the relevant legal and human rights standards, compliance practices and auditing techniques.

[12] See Company Assessments carried out by the Global Network Initiative. The organization has established the requirements for Independent Assessors, available at <https://globalnetworkinitiative.org/wp-content/uploads/2018/08/Independence-Competency-Criteria.pdf>

Mozilla could consider creating a specific training program for selected auditors prior to their assessment. The combination of these elements would help with standardizing the process in making it less costly for the resolvers of any size.

The audit reports would highlight the good practices that could be shared with other resolvers, besides any gaps in the fulfillment of the TRR policies and concrete recommendations of improvements to be carried out. It will be relevant to state the mandatory nature of those third-party audit recommendations for the resolvers in the TRR policies.

3. Transparency report of government requests for data

Transparency is essential in a democratic society, and because of that according international standards of human rights, States must publish statistics on the number of requests made, the number approved, the number rejected, the type of investigations for which the requests are made, the duration of the measures, a breakdown of requests by provider, etc.[13] However, in order to conduct oversight and make governments accountable, it is essential that intermediaries publish as much disaggregated information of users' data requests as possible as part of their transparency reports, and that they are issued regularly, at least annually, in order to be able to evaluate its evolution.

Transparency of users' data requests by governments to Internet's intermediaries also plays a particularly important role to protect intermediaries ensuring that their commitment with human rights protection cannot be circumvented by governments excessive requests. The Joint Declaration on surveillance programs and their impact on freedom of expression holds that in order to monitor the legality of the various instances of surveillance, States should allow and even encourage intermediaries to disseminate information on the processes they implement, indicating at least in aggregate the number and scope of requests from State agencies received and granted.[14]

Additionally to the requirement of periodic transparency reports in the TRR policy, Mozilla could encourage the engagement of civil society organizations for compiling and sharing to the broader public easily accessible information that allow to compare the performance of different resolvers

[13] Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression (2017). Standards for a free, open, and inclusive Internet, OEA/Ser.L/V/II CIDH/RELE/INF.17/17. para. 225.

[14] United Nations. Human Rights Council. Special Rapporteur of the United Nations (UN) on the Promotion and Protection of the Right to Freedom of Opinion and Expression and Special Rapporteurship for Freedom of Expression of the Inter-American Commission of Human Rights (OAS). Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression. June 21, 2013. Para. 169.

regarding the TRR transparency requirements, similar to what several civil society organization have already being doing by leveraging methodologies developed by Electronic Frontier Foundation (EFF)[15] for ISPs and other intermediaries or Ranking Digital Rights (RDR) for ICT companies with global operations.[16] It is also relevant to establish mechanisms to follow up on past processes, comparing and allowing evaluations of progress.[17]

The EFF and RDR projects present key examples where year-by-year comparison provides a larger view of the progress of companies shifting their policies to provide services with higher respect for the rights of users, often in response to the measurements themselves. Closer to our experience, the national instances of EFF's project in Spain and Latin American countries, measuring ISP compliance with data requests, can also show varying degrees of willingness to respond to civil society's demands and expectations above and beyond transparency, data protection and confidentiality rules, with favorable reputational impacts and low costs of implementation for every instance of change, often as an explicit response to the reports.

III. Online safety

1. Legally required blocking in Latin America

There are diverse provisions spread through criminal law, telecommunications regulations and intelligence services statues that could be used to demand some kind of action from DNS resolvers outside their jurisdiction. However, the Inter-American human rights standards have clear requirements to identify when those requests could be considered compatible with human rights protection, and therefore legitimate.

First, all restrictions to the right to privacy, including the right to be free from arbitrary or abusive interference with communications, must pass the test of legality, proportionality, and necessity established in the American Convention on Human Rights and reaffirmed by the Inter-American Court.[18] Therefore, any request of outside jurisdictional reach coming from countries part of the Inter-

[15] See Who has your back, available at <https://www.eff.org/pages/quien-defiende-tus-datos>
[16] See more about the Index Metodology, available at < https://rankingdigitalrights.org/2020-indicators/>
[17] See the above, as well as BSR Progress Report on the Oversight Board, published a year after the initial assessment and recomendations, available at <https://www.bsr.org/reports/BSR_Facebook_Oversight_Board_Report_on_Progress_Dec_2020.pdf>
[18] Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression (2017).

American Human Rights System (most of the countries in the Americas) should be assessed by the resolver according this tripartite test.[19]

According to the IACHR, this "includes both cases in which the State itself collects the communications and cases where States outsource that work—for example, by requiring servers and service providers to collect data and then demanding access to it, regardless of where it is stored, as a condition for the servers or providers to operate, or when they reserve the right to access data flows for local purposes such as pursuing criminals, oversight, etc. The standards developed in both the Inter-American and the European system aim at protecting not only the content of communications but also the data about the communications, or the metadata in the case of the Internet (…)".[20]

The IACHR adds that "all network surveillance constitutes interference with individuals' privacy. However, not all interference is *per se* illegitimate, and in exceptional cases, different degrees of interference are justifiable depending on the circumstances. Terrorism and the fight against organized crime are examples of instances where the State has an obligation to prevent and protect that constitutes a legitimate objective that justifies the exceptional and supervised use of surveillance technologies and mechanisms. However, 'it is crucial to understand that given the dynamic character of the Internet and of communications technology in general, this type of surveillance may constitute a particularly invasive act that seriously affects the right to privacy and freedom of thought and expression.' The United Nations General Assembly has highlighted that although public safety can justify the collection and systematization of certain information, states must guarantee that these measures respect human rights".[21]

The permissible instances of and conditions for surveillance must be established beforehand in a law and established explicitly, strictly, precisely and clearly, both substantively and procedurally. In view of the inherent risk of abuse of any surveillance system, these measures should be based on legislation

---

Standards for a free, open, and inclusive Internet, OEA/Ser.L/V/II CIDH/RELE/INF.17/17. par. 193. I/A Court H.R. Referring to the Case of Fontevecchia and D'Amico v. Argentina.Judgment November 29, 2011. Merits, Reparations and Costs. Series C No. 238, and I/A Court H.R., Case of Escher v. Brazil.Judgment of July 6, 2009. Merits, Reparations and Costs. Series C No. 200.

[19] In line with the European and universal systems, the Inter-American system established a three-prongtest to verify the legitimacy of State or non-State interference with privacy, including electronic surveillance. Pursuant to this test, surveillance must be legal—both formally and materially—necessary, and proportional. Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression (2017). par. 216.

[20] Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression (2017). par. 213.

[21] Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression (2017). par. 215.

that is particularly precise, clear and detailed, and States have to ensure a plural, democratic, and open consultation prior to the adoption of the applicable regulations. The objectives for which surveillance or the interception of communications would be permissible must be explicitly established in the law, and in all cases the laws must establish the need for a prior court order. The nature of the measures, as well as their scope and duration, must be regulated, establishing the facts that could lead to them and the bodies responsible for authorizing, implementing and monitoring them.[22]

The laws and policies governing the nature, scope, and implementation of interception and surveillance mechanisms and when they are in force must be public, and the State is required to apply the principle of maximum disclosure developed in the framework of right to access information. The maximum disclosure requirement covers both policies and practices on electronic surveillance, including the acquisition, development, or updating of systems available for it; the protocols for its use; the conditions and guidelines for its authorization; and which authorities are in charge of its implementation, authorization, and supervision.[23]

Some governments in the region are known for their practice of DNS blocking, although this measure is not widespread in the region as a whole. Some examples from Latin America regarding regulation that could be used to demand interventions at the DNS level, but they do not fulfill the aforementioned human rights standards, are the following:

- Recently, the Venezuelan Government blocked the Tor network, a tool that allows users to browse the Internet anonymously. The blocking was executed by the government-owned Internet service provider CANTV, the largest ISP in the country. In order to access the blocked tool, Venezuelan users had to rely on virtual private networks (VPNs) to circumvent government regulations.[24]
- In Cuba, the institutional architecture that restricts and filters content available online, denounced by the Special Rapporteur for Freedom of Expression of the IACHR. Worth mentioning are Cuban resolutions No. 127/2007, which deals with information technology

[22] Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression (2017). par. 217.
[23] Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression (2017). par. 218.
[24] Economic Commission for Latin America and the Caribbean (ECLAC)/Internet & Jurisdiction Policy Network (I&JPN), Internet & Jurisdiction and ECLAC Regional Status Report 2020 (LC/TS.2020/141), Santiago, 2020, p. 110, available at <https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-and-ECLAC-Regional-Status-Report-2020_web.pdf>

security, and No. 179/2008, a regulation for Internet service providers dealing with public access to the Internet. The former forbids the circulation of data or information contrary to "the social interest or public morals and mores". The latter creates an obligation for Internet service providers (ISPs) to monitor and "regulate" online content and establishes a regime of direct liability for intermediaries. These pieces of regulation are deemed to impact freedom of expression and freedom of access to information.

- In Argentina, the Argentine Chamber of Phonogram and Videogram Producers and other copyright management companies filed a lawsuit and were granted an injunction to block Pirate Bay, a very popular file-sharing website. The injunction ordered ISPs to block several domain names associated with the file-sharing website, such as thepiratebay.org and thepiratebay.se. Rather than blocking links to works for which an infringement is suspected, to the work of a particular artist or group of artists or to musical or phonographic works in general, the decision was taken to prohibit access to the entire website, which does not fulfill the proportionality criterium of the tripartite test.[25]
- In Mexico, the domain name "1dmx.org" was registered in order to host a website protesting against excessive use of force by the police in Mexico in reference to the day Enrique Peña Nieto took the oath as President in December 2012. That day a number of protests erupted, were repressed by the police, and at least one demonstrator died. A year later, the website was shut down following a request to suspend the domain name received by GoDaddy, the domain name registrar, from the United States Department of Homeland Security. The reason alleged for the take-down was that the website was part of an ongoing law enforcement investigation and that its content violated the company's terms of service.[26]
- In Peru, a decree from the Ministry of Transport and Telecommunications allows blocking websites and mobile applications offering motorcycle taxi services, which the Ministry has used to block a series of URLs. Additionally, the Institute for Intellectual Property (INDECOPI) has ordered administratively the blocking of websites suspected of linking to copyright-infringing contents,[27] regardless of whether that is the case, without judicial review, and with no consideration whether non-infringing communications happen therein as well.

[25] See Lara, J. Carlos. "Bloquean The Pirate Bay en Argentina", Derechos Digitales, available at <https://www.derechosdigitales.org/7608/internet-bajo-censura-bloquean-pirate-bay-en-argentina/>

[26] See García, Luis Fernando. "Political Internet censorship: a reality in Mexico (with a little help from the United States and GoDaddy.com)", Digital Rights: Latin America and the Caribbean, E. Magrani (ed.), Río de Janeiro, GV Direito Rio, 2018, p.65, available at <https://itsrio.org/wp-content/uploads/2018/01/digital-rights.pdf>

[27] See Hiperderecho, "Error 404", available at <https://hiperderecho.org/error404/sitios-bloqueados>

3. Transparency and accountability in legally required blocking practices

TRRs should maximize the amount of information they disclose to the public about their received requests for action and practices of implementation, absent any specific prohibition by their own jurisdiction law. Such transparency will help citizens hold their governments accountable. In Latin American region, Mexico's General Law on Transparency and Access to Public Information has been highlighted as a good step in that direction because encourages providers to publish information related to governmental requests for users' data. Actions to the DNS level should follow analog measures of transparency because their impact in the human rights exercise that is comparable to the access to users' data.

TRRs should publish periodic transparency reports, showing disaggregated statistics about the nature and number of requests received by governments (and eventually other parties) and their responses to those requests. This reporting should include notification from resolvers when government authorities have requested any action at the DNS level, and sufficient information for the affected parties to be able to pursue revision or redress before the resolver or the competent authority. In analogous way, European courts have asserted that this right stems from privacy and data protection safeguards for the access to users' data.[28]

As part as the aforementioned proposal to extend the DoH protocol to include an optional service to declare policies and conditions of use, an access to the user-readable reports could be available.

4. Requirements for parties that maintain and create blocklists

Taking action at the DNS level should only be under consideration when it can be reliably determined that the domain itself is used with a clear intent of significant abusive conduct. Furthermore, because the suspension of a domain has by definition a global impact, proportionality requires that only a

[28] In the Tele2 Sverige AB and Watson cases, the EU Court of Justice (CJEU) held that "national authorities to whom access to the retained data has been granted must notify the persons affected . . . as soon as that notification is no longer liable to jeopardize the investigations being undertaken by those authorities." Before that, in Szabó and Vissy v. Hungary, the European Court of Human Rights (ECHR) had declared that notifying users of surveillance measures is also inextricably linked to the right to an effective remedy against the abuse of monitoring powers. See Rodriguez, Katitza et al. "A Look-Back and Ahead on Data Protection in Latin America and Spain", EFF, September 21, 2020, available at: <https://www.eff.org/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain>

particularly high level of abuse and/or harm could potentially justify resorting to such a measure. It is important that the impact of a specific action at DNS level is well understood.[29]

We believe that a clear catalog of the possible actions and the increasing level of adoption of them should be clarified in the policies, as well as the impacts of each one of the measures defined, in the registrant and users. A useful typology is provided by I&J in the documents produced for making operational their policy recommendations that could be considered as reference.[30] The DNS resolver should conduct proper and thorough due diligence before any action on the domain is taken.

Additionally to that, some form of complaint and redress should be established in connection with the different categories of action identified. For that purpose a clear responsible for communicating any claim should be identified in the policy. For example by inserting in the policy: "For inquiries regarding actions taken pursuant to this policy, please contact [review@example.example]".

In the case of actions carried out pursuant to a court order from the DNS resolver's jurisdiction or other, this fact should be informed to whom presents the claim, at least is prohibited by law. Through this process should be possible for the complainer to submit clear evidence of why any technical measure should be reversed, including cases such as: (i) evidence provided by the registrant to show the domain was compromised without her knowledge (and the measure could be reverted); or (ii) evidence to demonstrate there have been a formal error, such as suspending the wrong domain name (example1.example instead of example11.example), or if a domain was removed from a blocklist that was relied upon prior to suspension.

5. Information about opt-in filtering endpoints to end users

Given that Firefox already has some infrastructure in place to filter content, a more user-friendly way to present the available configurations—and its safety, security and privacy consequences— would make it easier for users to enable such capabilities, and would help them to notice the protections or lack of protections of their given configuration settings.

---

[29] Internet & Jurisdiction Policy Network. Domains & Jurisdiction Operational Approaches Norms, Criteria, Mechanisms. April 2019, available at <https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf>p. 26

[30] Internet & Jurisdiction Policy Network. I&J Educational Resource on Effects of Actions at the DNS Level, available at <https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-101-Effects-Action-DNS.pdf>

While ensuring a successful web browsing could be done by setting up a trusted resolver at the operating system level, and while in the face of surveillance or censorship there are many circumvention tools on the web such as VPN or Tor Browser,[31] among others, for the average user it is not clear how to interact with a low layered protocol as DNS. There is no doubt for us that DoH is a relevant alternative to enhance privacy on the web for non-technical users.

However, there are also many cases where users *want* to filter specific content, call it parental control or blocking of harmful content, among others, and there is a diverse market for it. But in use cases where the "user" is a local network administrator in an institution, end-user rights such as the freedom of expression, freedom of association or access to information can be in tension.[32] This is not the place to discuss the legitimacy of these practices, but we consider it fundamental that users have sufficient information to consent or otherwise question the navigation policies implemented in spaces where they access the Internet, such as public libraries, digital access points, schools, private companies or governmental entities.

Considering that explaining DNS might not be the most effective way to ensure non-technical users get informed and consent the default browser configuration, or explore alternatives, we recommend to use an icon that displays a window with more information, similar to the icon to check SSL certificates used in all web browsers, or the Tor logo used in Tor Browser to check the connection relays circuit, both placed in the URL bar. The window displayed by clicking this icon could contain information of: the DoH or DNS resolver configured, and a link to other options, with a color indication of the privacy level it offer, taking into account it is possible for the end-user to configure a specific DoH resolver even if it is not part of the TRR Program; if any opt-in filter running, information of it, and a link for more information on the filter type and who activated it (local network administrator, ISP, an app, the end-user).[33] In any case, an emphasis on privacy protection in the communication of the feature is probably the best approach in order to get people's attention.

As a complement, we propose the design of a DoH API extension that allows servers to communicate their Privacy Policies regarding DNS services. This would allow intermediate technical users (from

[31] See Tor Project, available at <https://www.torproject.org/>

[32] For a discussion on these tensions see McMenemy, D. (2016), "Rights to privacy and freedom of expression in public libraries: squaring the circle", available at: https://pureportal.strath.ac.uk/files-asset/54531639/McMenemy_IFLA_2016_rights_to_privacy_and_freedom_of_expression_in_public_libraries.pdf

[33] There are many cases in Latin America where internet connection devices are shared by several people in a family, school or office.

network administrators to curious people) to choose with more information and clarity the options available to protect their browsing, be it either the default ISP/OS servers, manually chosen ones, or the TRR providers.

IV. Building a better ecosystem

1. Exploitations of the DNS in Latin America DoH could protect against

In recent years, various cases of vulnerabilities in devices with DNS manipulation and interference as a consequence have been reported. In 2017 there were reported attacks on routers hijacked via remote access in Argentina and Chile,[34] which consisted of altering DNS records to malicious spoofing domains; in 20018 it was reported in Brazil GhostDNS,[35] a DNSChanger based attack which altered DNS records for a large variety of Brazilian customers as it came pre-loaded with a local bank's malicious DNS domain.

As you may know, these type of attacks are common in several countries, and are usually launched after a balance on impact and costs used as a measure of feasibility. The common circumstances and vulnerabilities across the equipment and configurations by regional ISPs in Latin America make them a particularly vulnerable surface of attack.

While tampering with DNS records might occur on an operative system wide level, and while the use of DoH by itself does not protect against some of those issues, trusted DoH resolvers (which is the purpose of the TRR Policy) can mitigate the threat of these type of attacks, which enhance users' safety. Similarly, DoH together with a TRR policy may also protect against blockages that are not made within the legal framework of each jurisdiction. In Latin America, there have been reported at least two cases y the last years.

Thanks to OONI Probe,[36] a free and open source network measurement tool, it has been possible for many people to test websites blocking, presence of middleboxes, and network performance. During the parliamentary election campaign in Venezuela, between November 2015 and January 2016, 43

[34] See "Linksys Smart Wi-Fi Vulnerabilities" available at < https://ioactive.com/linksys-smart-wi-fi-vulnerabilities/>
[35] See "70 different types of home routers are being hijacked by GhostDNS", available at https://blog.netlab.360.com/70-different-types-of-home-routers-all-together-100000-are-being-hijacked-by-ghostdns-en/
[36] See Open Observatory of Network Interference at <https://ooni.org/about/>

cases of websites were found to be systematically blocked by DNS, by one or more internet providers. According to the research,[37] no other censorship mechanisms were used such as IP blocking, blocking based on content or keywords or content alteration.

Another case is the DNS blocking and manipulation of websites with information on women's sexual and reproductive rights, in 2019. In Brazil, voluntary termination of pregnancy is restricted to cases when the pregnancy is the result of rape, if the life of the woman is at risk, and in the case of anencephaly. There, it has been reported DNS interference to connect womenonwaves.org, by some ISPs.[38] This website, and its partner womenonweb.org has reportedly being blocked by different techniques in other countries around the world, not limited to DNS blocking, and it is worth to mention than at least in the case of Brazil or Spain,[39] there has not been a clear answer by the ISPs or the government what legal framework they comply with in order to carry out such blockages.

We hope this comments can be useful in your TRR refinement process, we remain available in case you should want to expand in any of the aforementioned points, please reach us at juliana@derechosdigitales.org or mariapaz@derechosdigitales.org

Juliana Guerra
Advocacy Officer– Derechos Digitales

María Paz Canales
Executive Director - Derechos Digitales

[37] See Ipys Venezuela, "Principales hallazgos de la navegación en Venezuela", available at <https://ipysvenezuela.org/navegarconlibertad/2016/03/29/principales-hallazgos/>

[38] See Coding Rights, "On the blocking of pro-choice websites: Women on Waves and Women on Web" available at <https://medium.com/codingrights/on-the-blocking-of-pro-choice-websites-women-on-waves-and-women-on-web-505ed6f17b63>

[39] See Vasilis Ververis, Fadelkon, Ana, Bita, Samba, "Women on Web website censored in Spain" available at <https://sindominio.net/sincensura/en/post/informe/>