DNS Transparency Reporting Guide

VERSION 2.3 (last update: 3 December 2018)
Contact: collin.kurre@gmail.com

PART I: BACKGROUND

Despite becoming an industry standard among platforms and telcos, transparency reports have yet to percolate to internet infrastructure providers such as registries and registrars. A recent study revealed that perceived cost and unclear benefits have been a primary barrier to adoption of transparency reporting and other due diligence practices, particularly when companies are not public facing.[1] However, that calculus could be changing in the face of effectual data protection legislation, cautionary industry scandals, and a lack of strategy or coordination in global standards and regulation.

Beyond conforming with established best practice in the internet industry, transparency reporting offers many benefits to companies large and small. These include:

- **Reputational** – signals company values, eases customer fears or suspicion by disclosing threats to user rights
- **Operational** – highlights burden on companies to administer and determine the validity of governmental and third-party requests; contributes to generating a standardized taxonomy for processing requests received
- **Tactical** – allows companies to track trends over time to strategize and react accordingly, while educating policymakers and raising awareness amongst consumers

In addition, publicizing data about governmental and third-party requests helps inform research and policy debates, identify systems that are inefficient or subject to abuse, and reduce misuse of executive power or government institutions.

Finally, we've generally seen strong pro-social competition on transparency reporting in the ICT sector, meaning that once influential companies start publishing reports on a particular segment of data, other companies will follow suit. The general guidance and reporting template that follow are intended to progress conversations and help internet infrastructure providers begin processing, recording, and reporting on government and third-party requests in a systematic and consistent way.

[1] See “Public Interest, Private Infrastructure: An Analysis of the Barriers and Drivers for Adopting Human Rights Standards in the Internet Infrastructure Industry” https://www.article19.org/wp-content/uploads/2018/06/HRIA-report-UNGP_5.6.pdf

PART II: GENERAL GUIDANCE

The most common types of requests received from companies operating in the DNS pertain to user data and content removals. Companies that collect and store personal data and/or have any level of content oversight should have a plan in place for handling these requests. A general baseline[2] is that requests must be made in writing, received from someone with the authority to make such a request, and made on the basis of an appropriate law in order to be honored. If a request does not meet legal requirements, the company should ask the requesting party to refine, limit, modify, or withdraw the request as appropriate.

While legal counsel should always be consulted to determine the validity of requests and appropriate response, the following considerations may be useful in devising a company's internal procedures for handling data and content requests:

- **Tracking Requests**: Ad-hoc processes such as forwarding requests or making decisions on the fly risk mistakes and inconsistencies. Companies are recommended to use a single, centralized process for tracking, tagging, and keeping tabs on requests from the moment they're received until a response is provided and the case closed.
- **Classifying Requests**: Requests must be correctly categorized by type and requesting authority in order to be handled appropriately. Sometimes this is easier said than done, as requests may be inaccurately labeled (either intentionally or on accident). Once more, companies should seek legal counsel to definitively determine the validity of a request; however, it is also recommended that all relevant staff members receive training on request categorizations.
- **Responding to Requests**: The most common requests received pertain to user data or web content. For data requests in particular, companies should have determined the kinds of data they keep, the grounds for keeping them, and the sufficient legal processes for accessing data *before* requests arrive. Governmental requests, particularly those made in emergencies, can be overwhelming for small businesses that aren't accustomed to being involved in such situations. Moreover, third-party requests may be fashioned to resemble law enforcement requests, posing a risk of data protection non-compliance to the company if they choose to disclose information. Companies should therefore work with their legal counsel[3] to define appropriate handling and responses ahead of time, and seek to minimize potential rights abuses by reacting proportionally and in direct and targeted response to requests (e.g., blocking an unlawful web page rather than blocking an entire domain).
- **Notifying Affected Users**: Barring legal restrictions, it should be company policy to inform respective users of requests, handling procedure, and action taken. Companies should have the process for contacting such users clearly defined ahead of time. In the case of legal restrictions, such as gag orders for ongoing criminal investigations, companies must decide whether they will challenge the order and give notice to the users once it has been lifted.
- **Keeping Data Secure**: Requests from governments, law enforcement agencies, and even third-parties often concern sensitive information. Companies must ensure that such data is kept secure by clearly defining processes for its handling, storage, backup, access, and deletion, even in jurisdictions where this isn't currently mandated by data protection legislation.

[2] See the Manila Principles on Intermediary Liability, https://www.manilaprinciples.org/
[3] Or subject-matter legal experts, such as EFF (https://www.eff.org/pages/legal-assistance)

Once defined, a company's internal procedures for receiving and acting upon requests should be made easily available for review by interested stakeholders. This can be done through a dedicated and easily accessible web page, which should include clear instructions to third parties about lawful requirements for access to user data, content removals, and any other processes that may have potential human rights implications. Any fast-track content removal agreements (e.g. with "trusted notifiers") should also be identified, as well as procedures for contesting disclosures / removals and recourse options for individuals who believe their rights have been infringed upon.

Additional Resources:

- .nz's Transparency Reporting Template (specific to New Zealand law)
- New America / Berkman Klein Center's Transparency Reporting Toolkit (great guide, largely specific to US law but with a section on international requests)
- Lumen database of legal complaints and requests for content removal

ANNEX: TRACKING TEMPLATE

Spreadsheet version available for download here: http://icannhumanrights.net/wp-content/uploads/2018/12/DNS-Transparency-Reporting-Template.xlsx

1. GENERAL INFORMATION

Means of receiving request — form, email, fax, mail, in person

Date received

Number of registrants targeted

Number of URLs concerned

Additional information

- Specified domains
- IP address(es)
- Number of copyright owners mentioned

2. REQUEST DETAILS – Citation of specific law must be included where relevant.

Data – What type of data was requested?

- Personal data
- Traffic data
- Anonymous data
- Other types of data: Pseudonymous, Controller, Processor, Consent

Content – On what grounds was the material deemed objectionable?

- Counterfeit pharmaceuticals
- Defamation
- Fraud
- Hate speech / discriminatory speech
- Intellectual property (copyright, trademark, etc)
- National security
- Online child abuse imagery
- Other (specify)

Infrastructure abuse – What type of abuse was identified?

- Malware
- Spam
- Phishing
- Other (specify)

Law Cited

3. REQUESTING ENTITY – Legal authority demanding action must be identified.

Country of Origin (jurisdiction)

Entity

Type

General governmental requests

- Subpoena
- Search warrant
- Court order
  - Criminal vs civil proceedings
- Other (specify)

Emergency governmental requests

- Emergency disclosure request
- Real-time monitoring requests (pen register / tap and trace)
- Other (specify)

Third-party requests

- Related to civil court proceedings
  - Subpoena duces tecum (for protection of evidence)
  - Criminal defense subpoena and/or court order
- No government connection
  - Intellectual property lawyers
  - Other (specify)

4. ACTION REQUESTED

Data – Production, preservation, other

Content – Blocking, removal, other

Infrastructure – Blocking, removing, other

5. RESPONSE

Status

Pending / In Progress – request still being processed

Full Response

- Responded to valid legal process by providing all of the user data information requested
- Responded to valid legal process by removing / blocking all content requested

Partial Response

- Responded to valid legal process by providing only some of the user data information requested
- Responded to valid legal process by removing some content requested

No Response

- Request did not meet legal requirements
- Request was for information that's publically unavailable
  - Requester was directed to source
  - No information given
- Request was for information that is unavailable / content neither hosted nor

accessible by company
- Request was withdrawn

Date completed

6. NOTIFICATION

Number of registrants notified when a request was made regarding their data / account

Date of notification

Delay between request being received and user being notified