CHILDLIGHT
Global Child Safety Institute

SEARCHLIGHT 2025

Technical Notes

Who benefits?

Shining a Light on the Business of Child Sexual Exploitation and Abuse

HUMAN
DIGNITY
FOUNDATION

THE UNIVERSITY
of EDINBURGH

This document has been designed to be accessible.
If you require this document in an alternative format,
such as large print or a coloured background,
please contact us at childlight@ed.ac.uk or write to us
at Childlight Global Child Safety Institute, University of
Edinburgh, Holyrood campus, Holyrood Road, EH8 8AQ.

SEARCHLIGHT 2025

Who benefits?

Shining a Light on the
Business of Child Sexual
Exploitation and Abuse

Study H: Access Denied: How Blocklists are Thwarting Attempts to View CSAM

Established by

HUMAN
DIGNITY
FOUNDATION

Hosted by

THE UNIVERSITY
of EDINBURGH

1. Background

Domain blocking technology has been available for more than 20 years. One of the earliest adopters of such methods of online safety for users was British Telecom (BT) through the Cleanfeed programme. Initially telecom companies like BT blocked content based on a list of child abuse websites provided and regularly updated by the Internet Watch Foundation (IWF) (Hunter, 2004). This was later made a regulatory principle of the Cospol Internet Related Child Abusive Material Project (CIRCAMP), a multi country effort that sought to block known child sexual abuse material (CSAM) domains globally. Since this time, other countries and companies around the world have adopted a similar approach, using law enforcement generated block lists including the INTERPOL 'Worst of' List (IWOL).

Keeping the block list current is key, as evidenced by a leak in 2010, which revealed many of the blocked sites had been terminated, were expired or no longer contained CSAM. As such, the IWF, as a part of their annual report, provide data concerning the activity of the block list including the number of additions and removed domains, to which on average 1,000 new URLs are added each day (IWF, 2024). What started out as a public monitoring system, bound to jurisdictional limitations has moved towards placing the impetus on the private sector. Internet service providers, like the domain answering service used in this study—a global brand in networking and domain answering—are responsible for managing their network activity and ensuring that they do not facilitate criminal activity. The specific service used in this study has not been named to highlight the broader relevance to similar companies (McIntyre, 2013). It is referred to as the DNS company throughout.

2. Rationale

This project sought to enhance knowledge about CSAM requests for users through the DNS company's web services, specifically in relation to understanding the prevalence and nature of attempted CSAM access on the DNS company network. This was accomplished by observing how CSAM DNS queries change over time, specifically in 2023, by observing trends in domains, time of request and numbers of requests over a given period.

The aims of the research were to examine the:

- Scale/magnitude and changes in blocked CSAM domain requests
- Scale/magnitude and changes in CSAM requests over time globally and per country
- Patterns of domain requests (where and when are requests occurring)
- The use of potential obfuscation techniques/anonymisation services following a blocked request

3. Research questions and aims

3.1 Research questions

Per country/region and globally (where data is collected) the following questions were asked:

- What are the total number of domain requests for CSAM webpages (over the time period 2–3 September 2024) on the DNS company networks identified within the data?
- How does the volume of requests change over a given period, when are the periods of greatest blocked request?
- Is there a correlation between blocked requests from an IP location and use of obfuscation techniques from that same property?
- What regions (UNICEF regions, countries) had the greatest number of users requesting to access known CSAM domains?

3.2 Objectives

The objectives of the study were to:

- Analyse DNS data from the reports generated by the DNS company and sent to Childlight
- Understand the current prevalence of the requests to access CSAM globally and per country (where country data is collected)
- Understand the association of blocking DNS of CSAM-sharing webpages with the use of known obfuscation techniques

4. Study design and methods of data collection and analysis

The data was found within the domain name service internal systems, which tracked the volume and nature of requests across their network daily. This data was prepared by the domain name service company for the purpose of this study and anonymised within the internal system. The redacted reports from the DNS company were sent in an encrypted Excel spreadsheet via an authorised file transfer (DataSync) from the DNS company to the University of Edinburgh research team.

The data was then converted into proportional measurements, rather than total volumes, using Microsoft Excel in preparation for further analysis. The IP addresses were redacted from the data source prior to receipt by the University of Edinburgh, with the data classified as case volumes, rather than individual IPs or users. For the country-level analysis of the DNS company data, the country acted as the parent-case. For data concerning unique IP access, the data was reported as volume of unique IPs associated with the larger dataset on the number of domain requests.

The data was prepared by the research team through the conversion of the raw volume of domain requests into proportions for each day of the study period. This meant that all the data included in the working Excel sheet was not replicable to the source data, as totals had been removed from the working data set. The data was sorted by the purpose of request, as either being for a known CSAM domain or any other request, which acted as the test and comparison group. The data was then assessed using descriptive analysis, e.g., univariate analysis, in which measures of central tendency such as the mean, mode and median per country and period were calculated to show how many attempts to access domains occurred, and any change over the two days. Relationships between the provided variables (CSAM request and non-CSAM request) were assessed to determine an association, e.g., the correlation between times of requests and specific anonymisation services used. The proportion of requests was calculated by measuring the total number of requests that employed any type of proxy, the use of virtual private networks and use of The Onion Router. Finally, the number of individual IPs that requested only CSAM domains/webpages over the two days were isolated from the rest of the IPs that requested more than just CSAM domains in the same period, and these were sorted by the countries in which the IP originated.

5. Study setting/information about the data source

The data on blocked domain requests for CSAM and associated queries was designed and run by a member of the DNS company staff on their internal system to ensure data privacy and security. The internal system tracks all domain request behaviour across the service, including approximate locations, individual IPs, associated IP owners where available, use of anonymisation services, time, date and any domain blocking with reason. These queries were narrowed by the study search parameters were concerned with IPs making requests for known CSAM domains. The queries were run based on the research questions and in consultation with the domain service provider concerning the data availability. All data from the system queries was reviewed by the DNS company staff prior to sending to ensure identifiable information was removed or aggregated to volumes and percentages. The data sets were exported from the DNS company systems in a .csv format and transferred through a secure link via DataSync, which was password protected.

The data was delivered and organised under the following headings: boolean label (csam & not csam), total_queries, proxy_queries, vpn_queries, darknet_queries, residential_vpn_queries, proxy_tor_queries, and ext_node_tor_queries. For all query headings, the data was represented numerically according to the count.

6. Sample and recruitment

6.1 Eligibility criteria – primary research studies

Data on domain requests was collected and included based on individual IPs using the domain answering service. These IPs were included provided they were using the DNS company network and made at least one request for a known and blocked domain displaying CSAM. The IP address was then removed from the dataset and the data was presented as volume of requests over the two days. The data was collected based on domain requests for 2–3 September 2024, Coordinated Universal Time (UTC).

6.1.1 Inclusion criteria – for both primary research and scoping/systematic and legislative reviews

IPs that had requested access to a domain on the blocked lists from the IWF and INTERPOL on 2–3 September 2024, while using the domain name service were included.

6.1.2 Exclusion criteria

All other IPs that did not make a request for a domain on the blocked lists from IWF and INTERPOL on 2–3 September 2024, while using the domain answering service were excluded.

6.2. Sampling

6.2.1 Size of sample

The data was based on a two-day sample of domain requests globally from the domain answering service. The data was derived from users/IPs which made requests for known CSAM domains. This made-up a significant volume of requests over the two days, on average more than 426,000 requests daily.

6.2.2. Sampling technique

The data was chosen based on the global nature of the domain answering service, which works with other internet service providers and telecommunication companies processing and connecting users to the internet. The data was sampled from this company's service based on the study variable of IPs requesting known CSAM domains over the two days. The sampling was chosen based on capturing data over a 48-hour period to account for a complete day according to the UTC for every time zone globally.

7. Ethical and regulatory considerations

All anonymous data has been securely shared and stored, and was used solely for the purposes of this study, according to the University of Edinburgh data protection and research data handling guidelines. Data privacy and security protocols have been implemented to ensure data integrity and confidentiality. The quantitative data from the DNS company will be kept for a maximum of one year after the project finishes, then destroyed, as recommended in the University’s research data retention policy. DataSync was used for files containing innocuous data between data partners.

The following measures were employed to reduce or eliminate any risks associated with the data:

- Data was anonymised prior to receipt by the University of Edinburgh to prevent data linkage.
- Data was presented in aggregate form, preventing the identification of individual participants due to small numbers.
- Data was transferred using secure methods such as encrypted formats and secure data transfer platforms and protocols.
- Strict controls were implemented to limit who can access the data.

In addition, Childlight and the domain naming service signed data transfer agreement which indicates the purpose of the data being transferred and its storage.

7.1 Safeguarding and researcher well-being

Childlight researchers completed the Sexual Violence Research Initiative's 4-module online course, 'Dare to Care: Wellness, self and collective care for those working in the VAW and VAC (Violence Against Children) fields'. Furthermore, Childlight hosted its own workshop with all global data fellows and researchers on vicarious trauma prior to fieldwork.

Regular check-ins and debriefing sessions were held with members of the research team to monitor their emotional wellbeing. Support sources and signposting provided to the research participants were also provided to the team.

7.2 Research approval

The project received ethics approval from the University of Edinburgh, Childlight Research Ethics Sub-committee on 16 July 2024. Reference: CATTU-JST-0060424CL.

A Data Transfer Agreement between the data source and Childlight was formalised ahead of the publication of the research on 7 March 2025.

7.3 Study advisory committee and peer review

An advisory committee was established, comprising professionals working in the technology and child sexual abuse prevention field. The committee includes a global regulator of online spaces and technology, a member of the domain answering service, and a representative of a domain management company.

The committee reviewed the protocol via email correspondence, and the research questions. The committee was provided with a copy of the full report, on which they gave their comments concerning accuracy and outcomes. This feedback was incorporated into the report and fed directly into the recommendations.

Further in-person consultations were held with individual members of the committee on 26 November 2024, 19 December 2025, and 15 January 2025.

7.4 Data management

All anonymous data was securely shared, stored, and used solely for the purposes of this study according to the University of Edinburgh's data protection and research data handling guidelines. Data privacy and security protocols have been implemented to ensure data integrity and confidentiality.

The data was transferred through authorised, authenticated and secure channels* and is stored in the DataSync at the University of Edinburgh.

The data was graded as Level 1 referring to the extracting and recoding of sensitive data and, as such, is required to be securely transferred and stored in a password protected environment only accessible to specific research staff.

7.5 Access to the final study dataset

The dataset will not be available due to permissions from the data source set out in the data transfer agreement, which prevents disclosure of the data beyond the employees of the data recipient, Childlight. The data also cannot be stored beyond the length of the agreement which lasts for one year.

8. References

Brown, I. (2013). *Research handbook on governance of the internet* (1st edition). Edward Elgar Publishing, pp. 1–499. https://doi.org/10.4337/9781849805049

Hunter, P. (2004). BT's bold pioneering child porn block wins plaudits amid Internet censorship concerns. *Computer Fraud & Security,* 2004(9), 4–5. https://doi.org/10.1016/S1361-3723(04)00109-5

Kantas, E., & Dekker, M. (2022). *Security and privacy of public DNS resolvers*. Publications Office

Parti, K., & Marin, L. (2013). Ensuring freedoms and protecting rights in the governance of the internet: A comparative analysis on blocking measures and internet providers' removal of illegal internet content. *Journal of Contemporary European Research*, 9(1), 138–159. https://doi.org/10.30950/jcer.v9i1.455

Sandeep Singh Grewal. (2011). New hotline on blocked websites. In: *McClatchy – Tribune Business News.* Tribune Content Agency LLC.

Varadharajan, V. (2010). Internet filtering – Issues and challenges. In: *IEEE Security & Privacy* (Vol. 8, Number 4, pp. 62–65). IEEE. https://doi.org/10.1109/MSP.2010.131