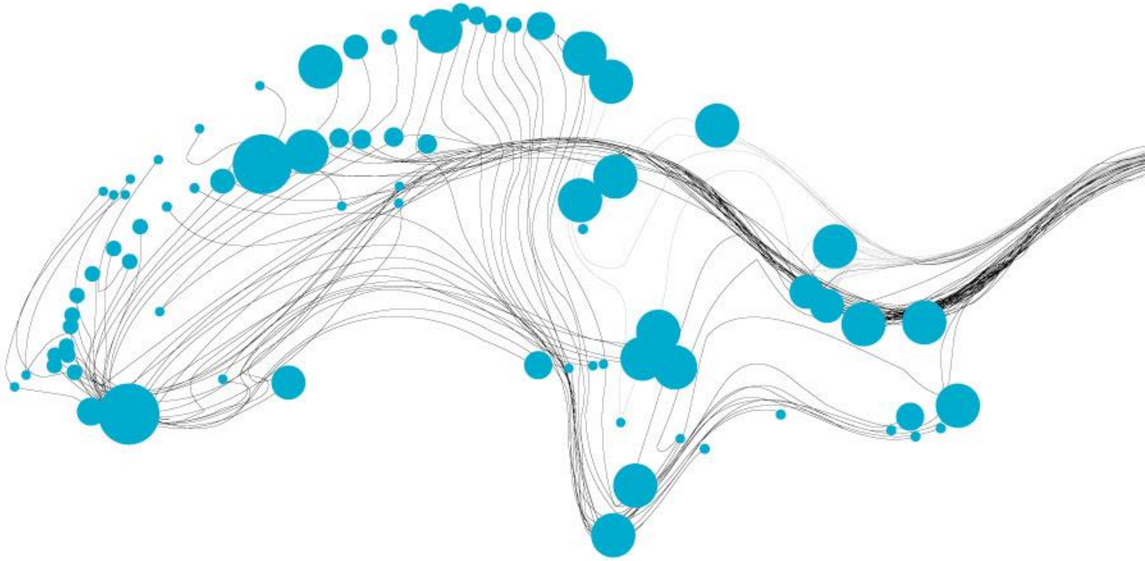
ISP Parental Controls:

Analyzing Domain Filtering and Online Safety Measures



Antonia Affinito, Anna Sperotto, Chiara Rizzato

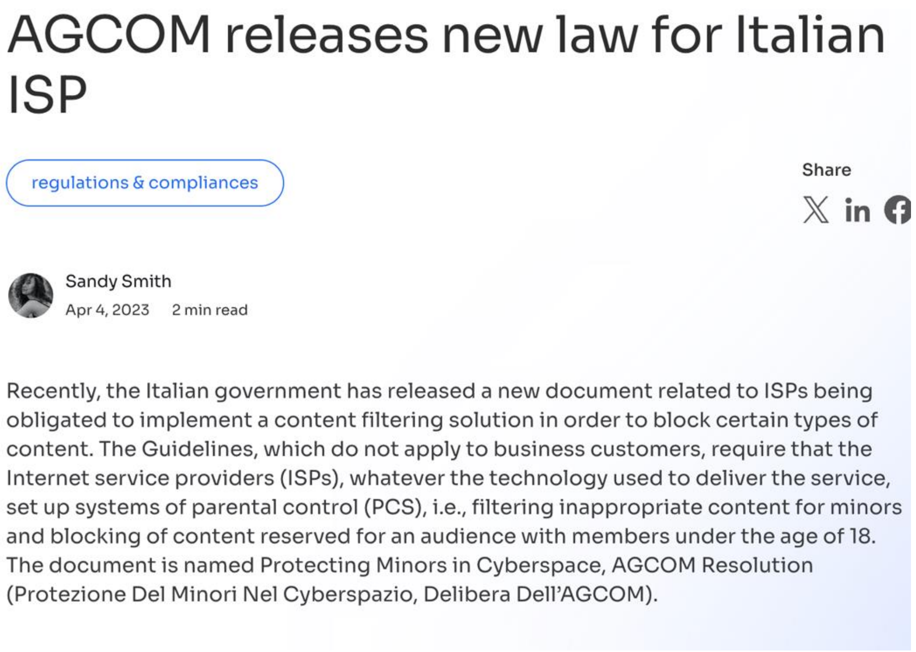
University of Twente, the Netherlands

UNIVERSITY
OF TWENTE.

Background

- The Internet provides access to vast information
  - But **not** all content is **suitable** for **children**
- Many governments **mandate ISPs** to offer **parental controls** to ensure child safety online

Background



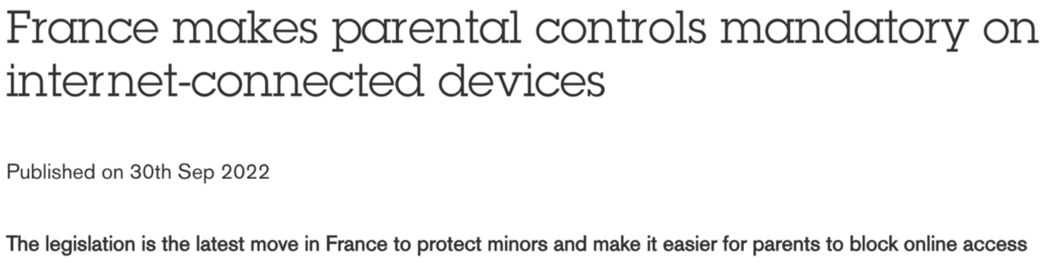
AGCOM releases new law for Italian ISP

regulations & compliances

Share

Sandy Smith
Apr 4, 2023 2 min read

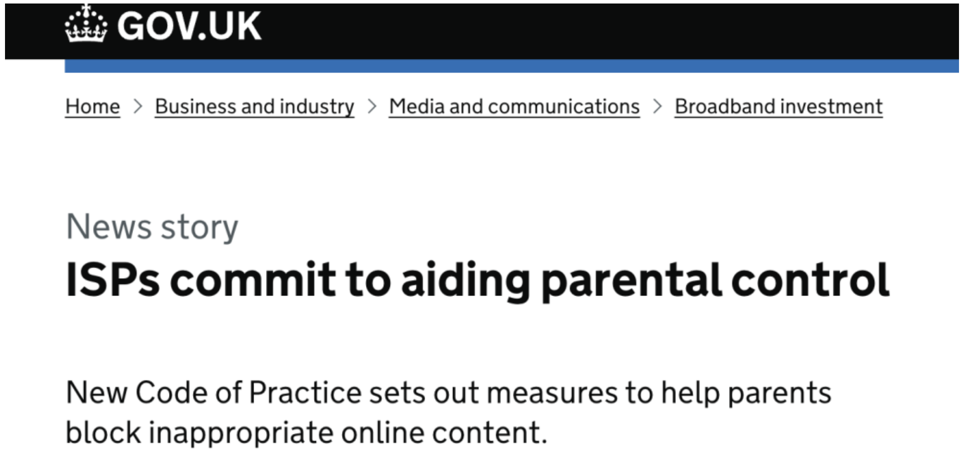
Recently, the Italian government has released a new document related to ISPs being obligated to implement a content filtering solution in order to block certain types of content. The Guidelines, which do not apply to business customers, require that the Internet service providers (ISPs), whatever the technology used to deliver the service, set up systems of parental control (PCS), i.e., filtering inappropriate content for minors and blocking of content reserved for an audience with members under the age of 18. The document is named Protecting Minors in Cyberspace, AGCOM Resolution (Protezione Del Minori Nel Cyberspazio, Delibera Dell'AGCOM).



France makes parental controls mandatory on internet-connected devices

Published on 30th Sep 2022

The legislation is the latest move in France to protect minors and make it easier for parents to block online access



GOV.UK

Home > Business and industry > Media and communications > Broadband investment

News story

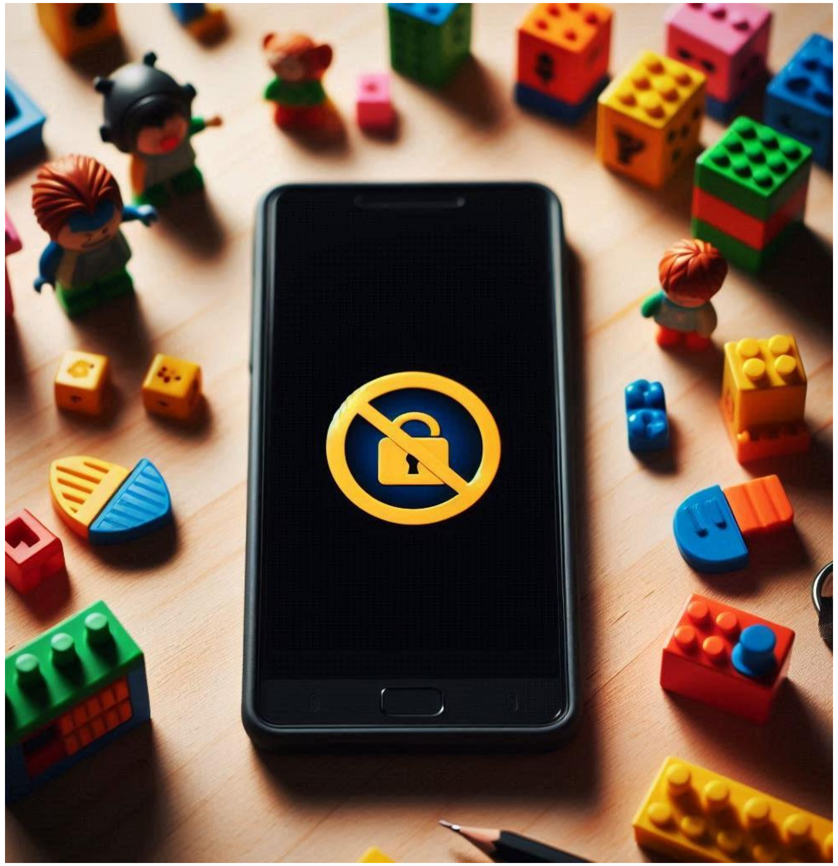
ISPs commit to aiding parental control

New Code of Practice sets out measures to help parents block inappropriate online content.

Background

Categories

- **Adult and Explicit Content** (Pornography, Nudity, Sex)
- **Gambling** (Online casinos, Lottery)
- **Violence and Extremism** (Hate speech, violence propaganda)
- **Drugs**



UNIVERSITY OF TWENTE.

Objectives

- **How** do ISPs classify and **block harmful** content?
- Is there evidence of **under-blocking**, where inappropriate content is not being filtered or blocked as intended?
- Can the blocking mechanisms be **bypassed**?

Methodology (1/2)

Data Sources

- **Tranco**: A list of popular domains based on traffic rankings
- **DNSForFamily**: A list of domains categorized for family-safe internet access
- **Cisco Umbrella Investigate**: Used to categorize and analyze domains to assess their relevance to children’s safety
  - Checked each domain's category to determine whether it falls under restricted content (e.g., gambling, adult content, violence)

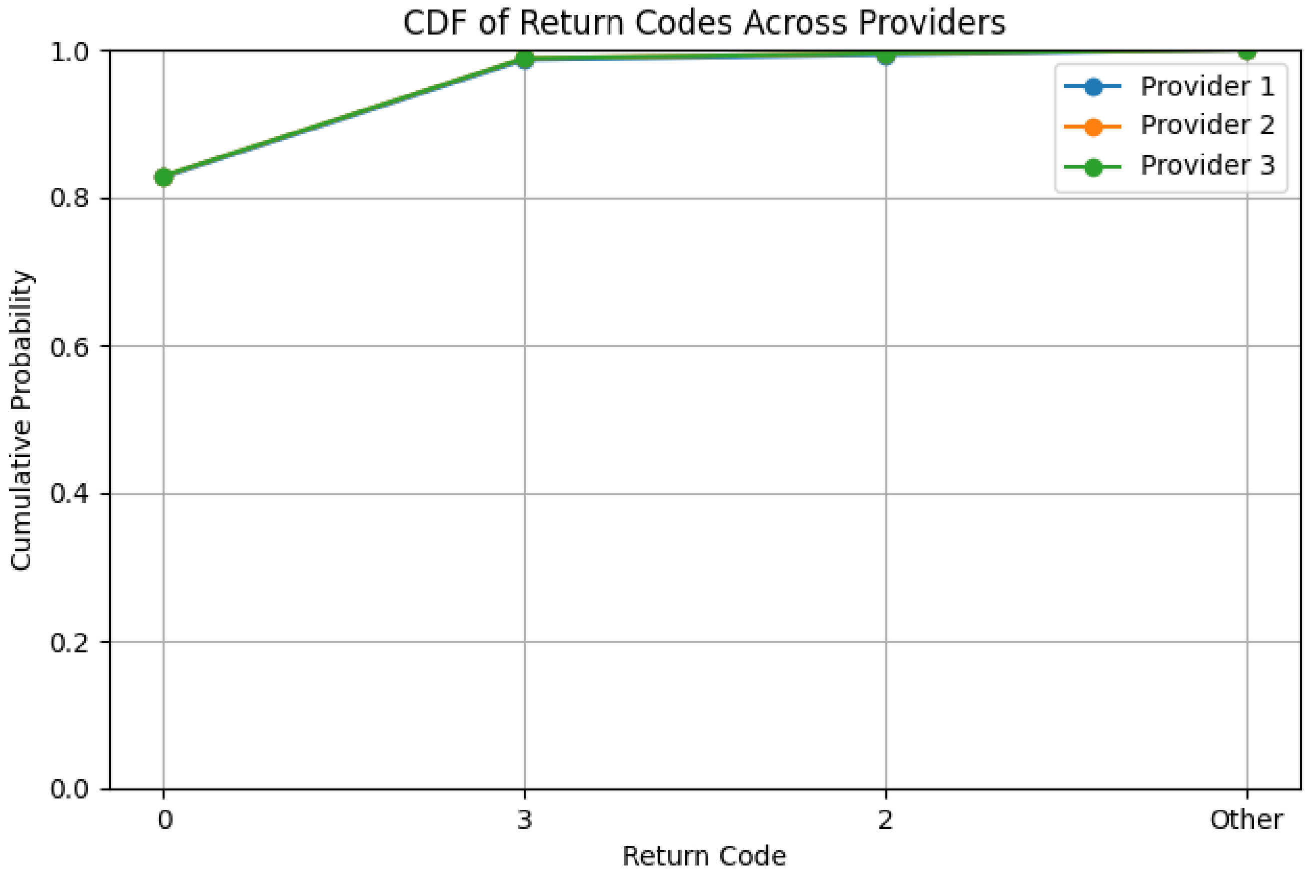
Methodology (2/2)

Analysis Process

- Queried the collected domains using **ISP DNS resolvers** with parental control **enabled** to observe filtering behavior.
  - Checked the **DNS response codes** (NXDOMAIN, SERVFAIL, REFUSED) to determine if access was restricted
- Performed **HTTPS requests** to analyze response status codes
  - Verified if the domains were inaccessible or if filtering only applied at the DNS level

Preliminary Results – DNS Response Codes

- ISPs can use **DNS resolvers** to implement content filtering by modifying the responses the resolver provides. “**Using DNS is an easy way to abide by the national regulations.”**

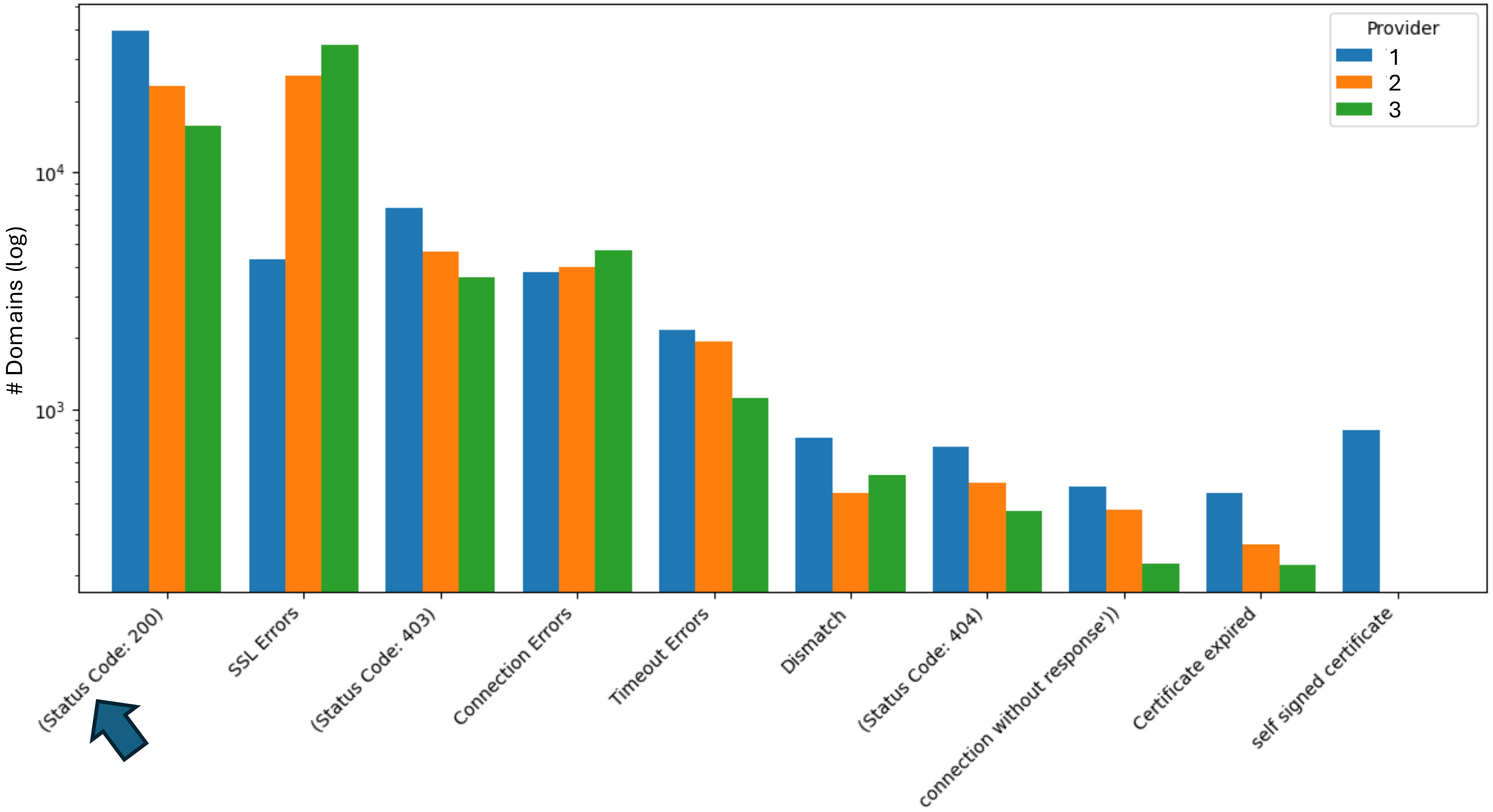


≈80% domains return a DNS response code of **“0”**

- **DNS filtering** is not being applied to these domains.

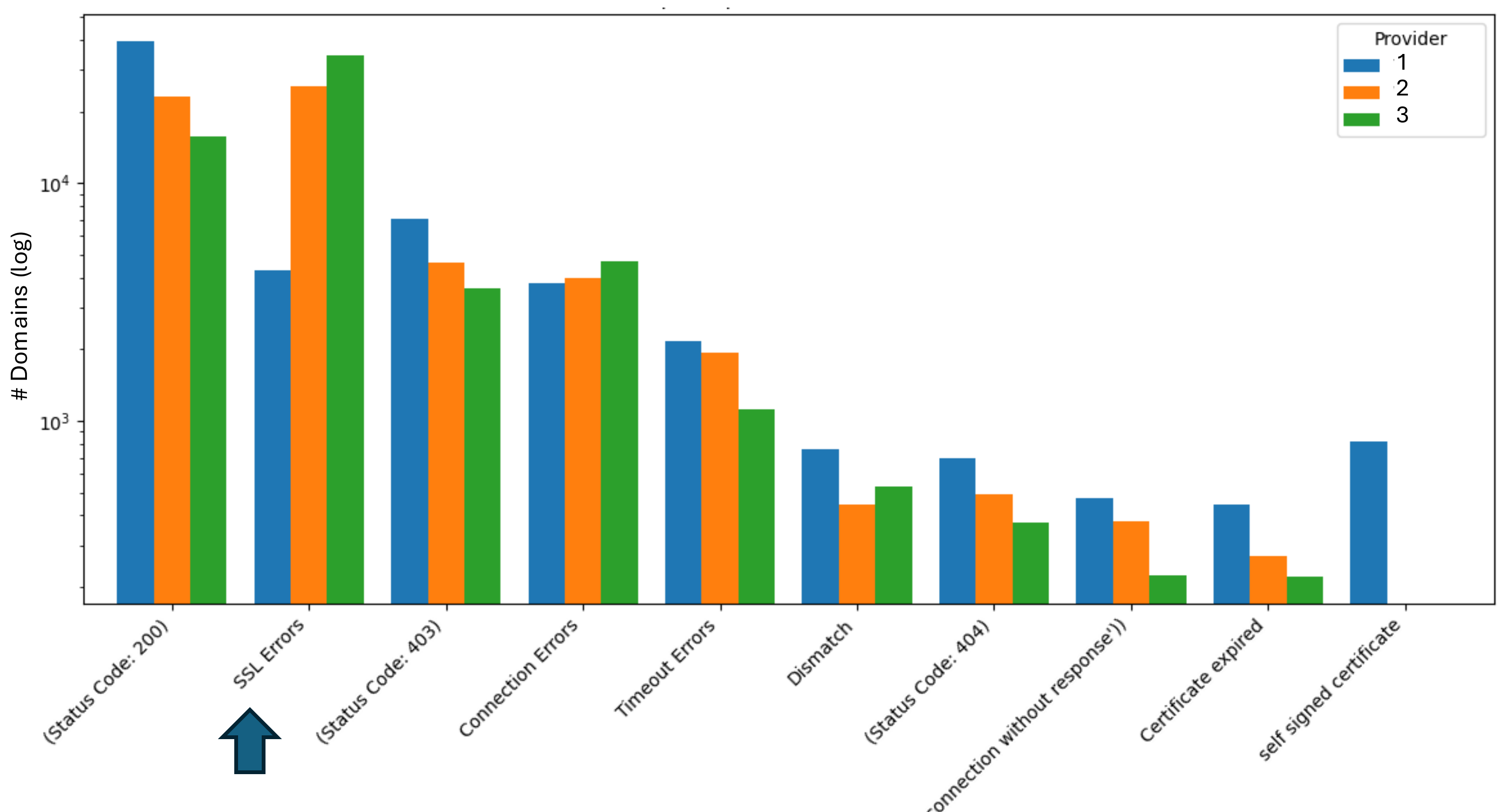
Preliminary Results – HTTP Response

- Domains are accessible
- **SSL/TLS interception**
  - SSL Errors: TLS handshake is over, and the client cannot verify the certificate provided by the server



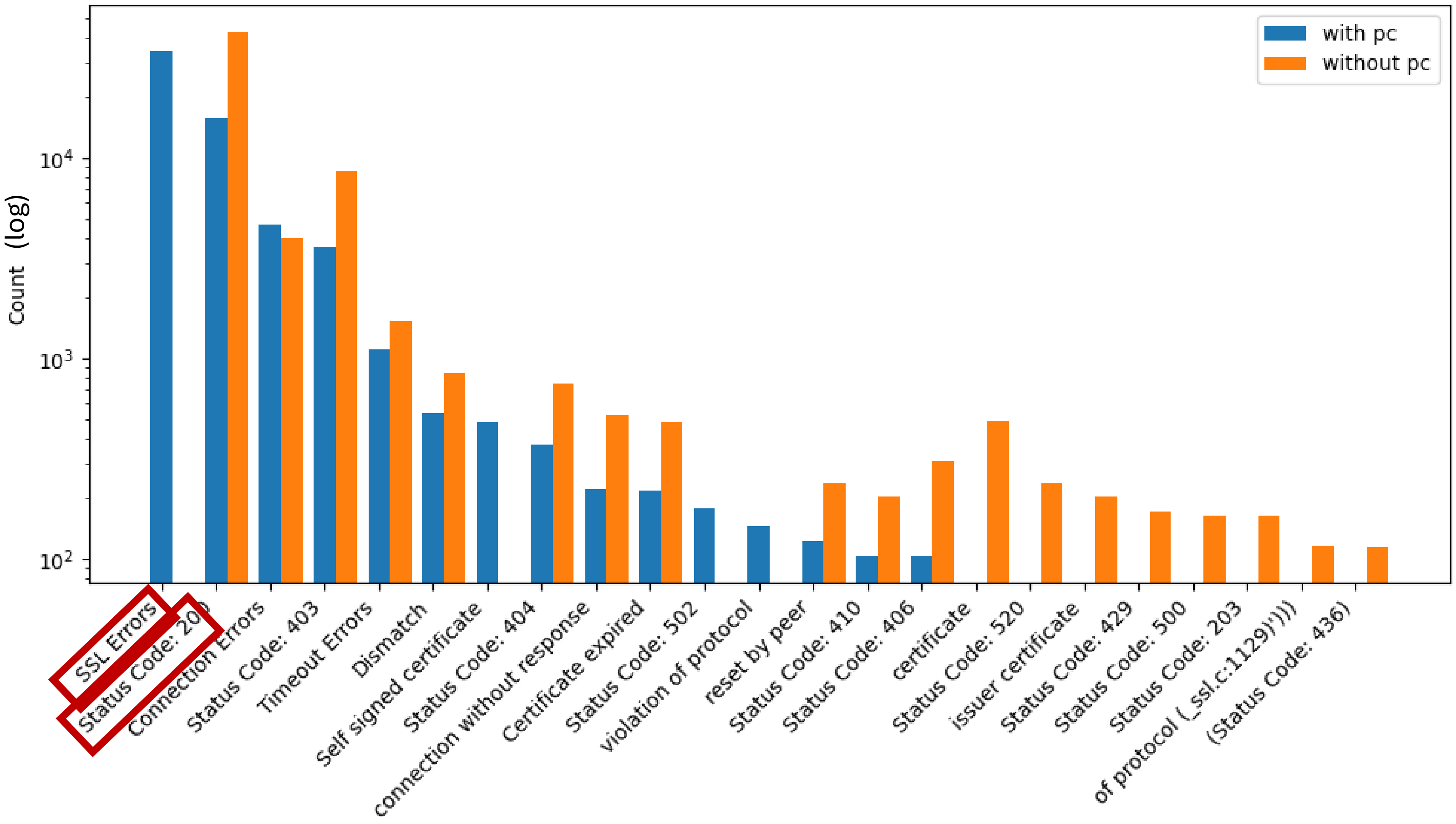
Preliminary Results – HTTP Response

- Domains are accessible
- **TLS interception**
  - SSL Errors: The client cannot verify the certificate provided by the server



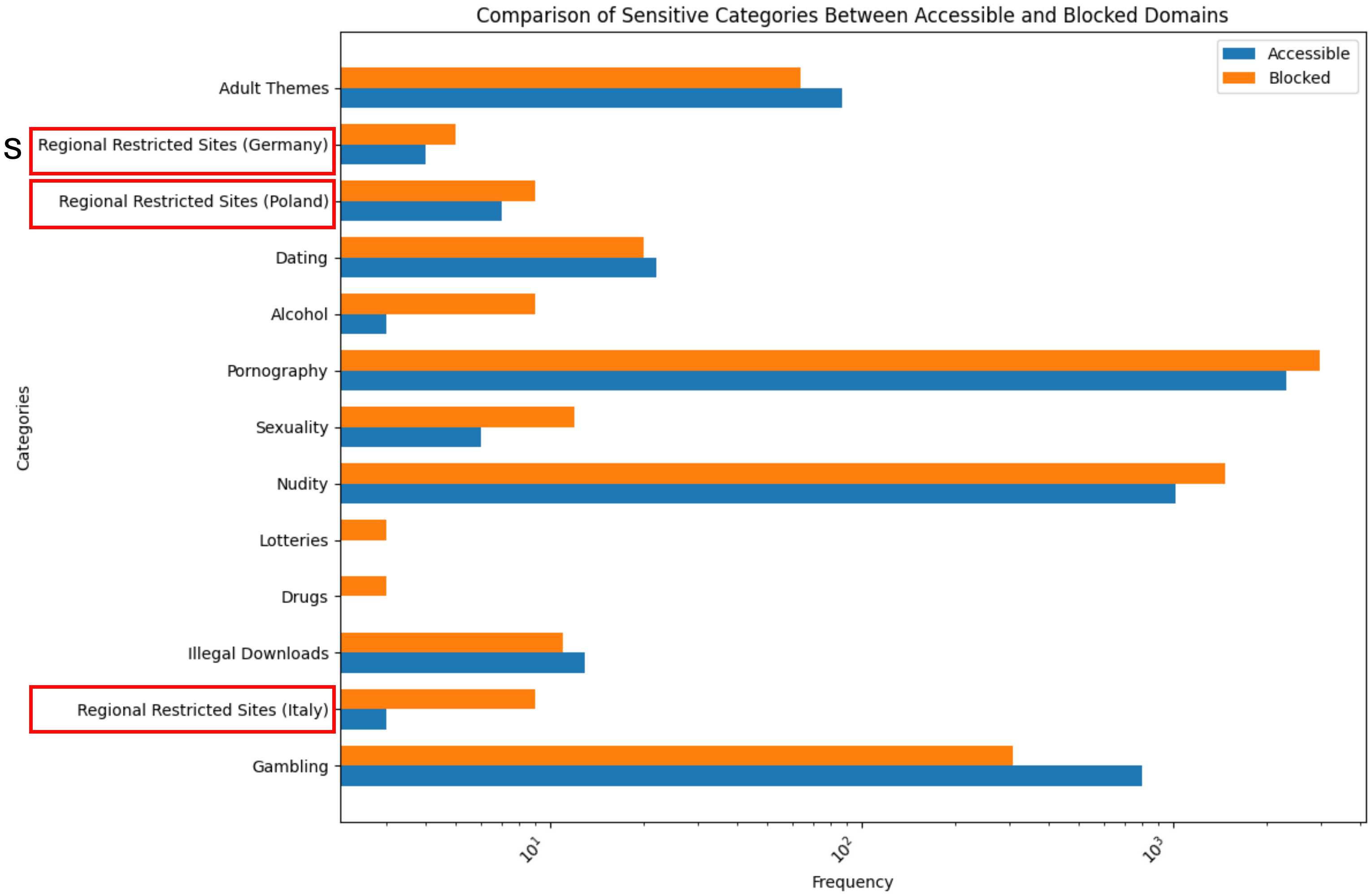
(Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: certificate has expired (_ssl.c:1129)')

Comparison With vs. Without Parental Controls



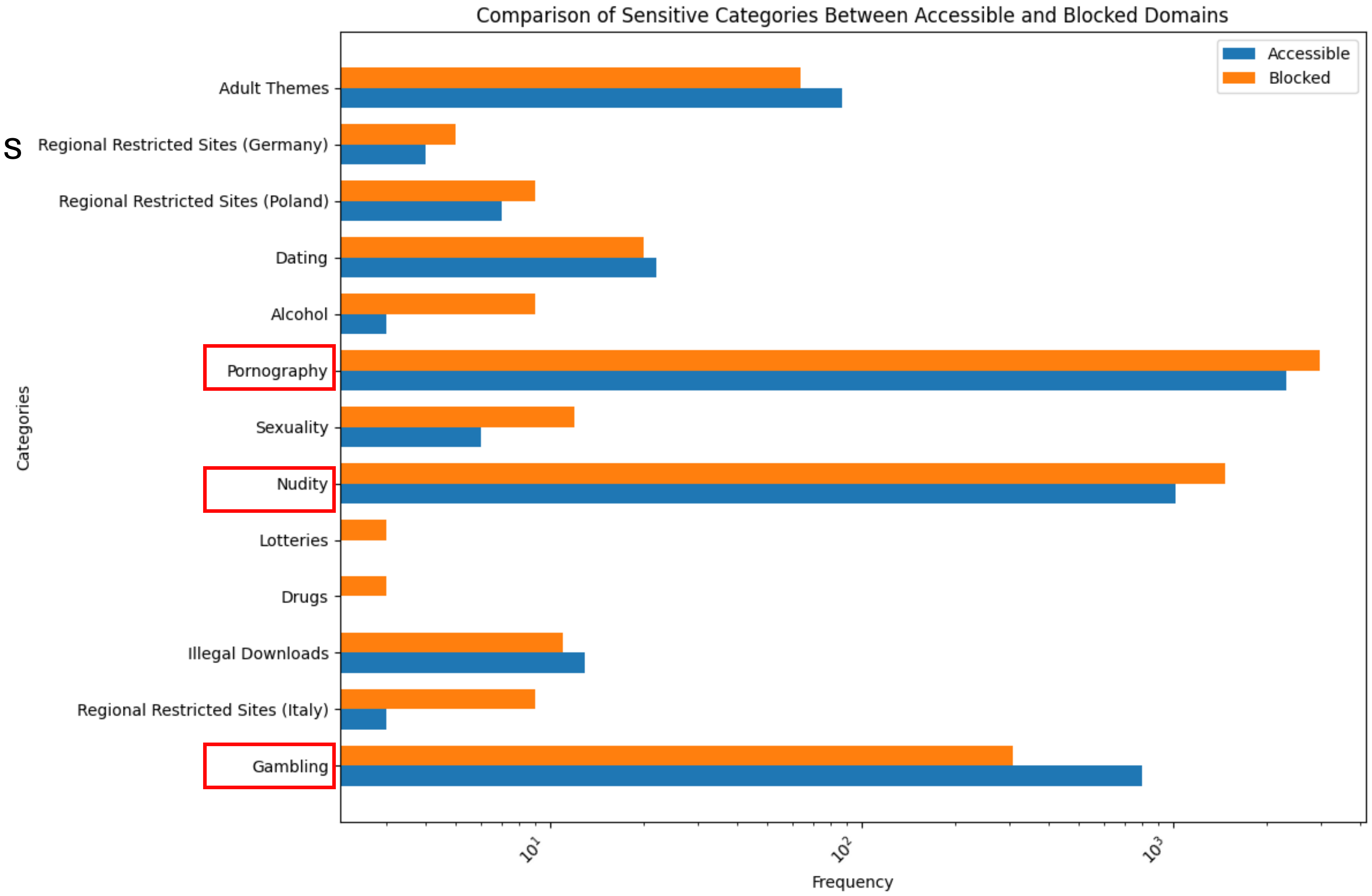
Categories

- Disparity between accessible and blocked content across different sensitive categories
  - A significant number of sensitive categories remain **accessible** despite blocking measures.
  - **Regional Restricted Sites** (Germany, Poland, Italy), accessible domains persist, showing that restrictions are region-specific and often bypassed or circumvented.



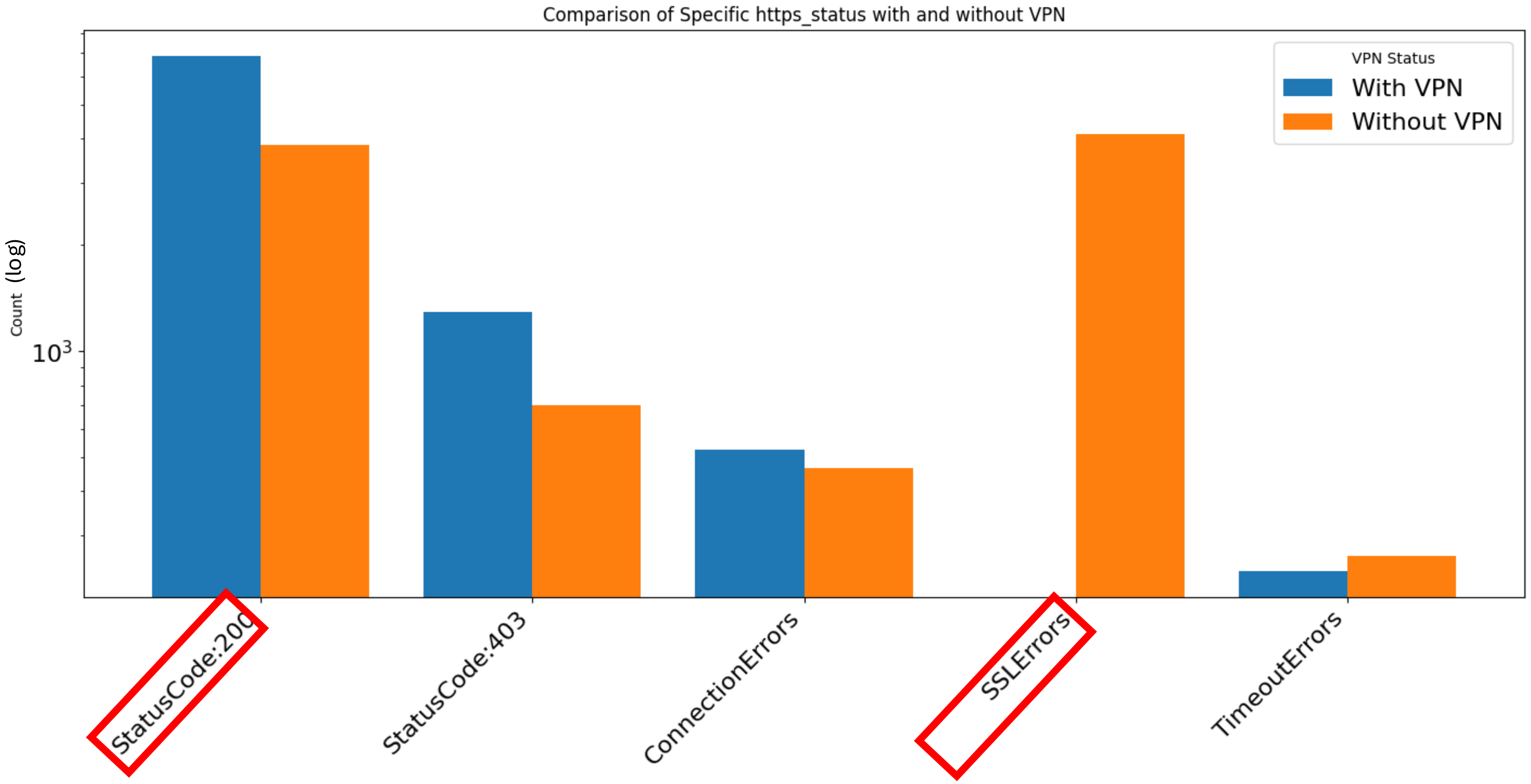
Categories

- Disparity between accessible and blocked content across different sensitive categories
  - A significant number of sensitive categories remain **accessible** despite blocking measures.
  - **Regional Restricted Sites** (Germany, Poland, Italy), accessible domains persist, showing that restrictions are region-specific and often bypassed or circumvented.



VPN Usage

DNS queries go through the **VPN server**



Conclusion/Future Work

- ~80% of domains returned DNS response code “0,” indicating that DNS filtering is not effectively applied to these domains.
- SSL/TLS interception issues, with certificate verification failures
- Despite blocking measures, several sensitive categories (e.g., gambling, adult content, violence) remain accessible.
- DNS queries going through VPN servers can bypass parental controls.

Thank you for your attention

Do you have any questions?

a.affinito@utwente.nl

UNIVERSITY OF TWENTE.