Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

School of Computer Science and Statistics

Comparing Internet Censorship Between Ireland & Iraq

Griffin Steinman

Dr. Stephen Farrell
February 18, 2025

Submitted in partial fulfilment of the requirements for the degree of
B.A.I. Computer Engineering

Declaration

I hereby declare that this Thesis is entirely my own work and that it has not been submitted as an exercise for a degree at this or any other university.

I have read and I understand the plagiarism provisions in the General Regulations of the University Calendar for the current year, found at `http://www.tcd.ie/calendar`.

I have also completed the Online Tutorial on avoiding plagiarism 'Ready Steady Write', located at `http://tcd-ie.libguides.com/plagiarism/ready-steady-write`.

Signed: ____________________ Date: ____________________

Abstract

A short summary of the problem investigated, the approach taken and the key findings. This should not be more that around 400 words.

The must be on a separate page.

what's the title for our title abstract one page five paragraphs area and digital twin project research questions two paragraphs how to solve them paragraph to implement and evaluate main findings one paragraphs expanding the abstract

introduction literature review design implementation evaluation conclusion

Acknowledgements

Thanks Mum!

You should acknowledge any help that you have received (for example from technical staff), or input provided by, for example, a company.

Contents

1 Introduction

1.1 Internet Censorship and Privacy

The primary aim of this work is to identify and compare internet censorship methods between Ireland and Iraq.

1.1.1 Overt vs. Covert Censorship

Censorship can be implemented in many different ways, but there are two main categories: Overt and Covert Censorship. Overt censorship is openly implemented by governments, ISP's, or legal courts to block or restrict access to certain types of content, or specific websites. When the content a user is trying to access is blocked using overt censorship, it is made very clear to the user that it is blocked. An example of this is the 'Golden Shield Project', which is China's internet censorship project. This project blocks access to websites such as google and facebook, and the citizens of China are often aware that they websites have been blocked by the government (1).

Covert censorship is more often harder to detect. Search engine manipulation, throttling or slowness, and shadow banning are some of the primary methods of covert censorship. The goal of this type is to make censorship more difficult to detect by users, and is often disguised as technical issues.

1.1.2 Privacy

User Privacy across the internet is directly tied to censorship efforts from different regimes. Censorship often involves the state or corporate monitoring of internet users, and governments that impose censorship frequently justify it using security concerns while often violating privacy rights in the process. In countries where censorship is highly enforced, using anonymity tools to circumvent censorship can protect the right to free expression and access to information. For instance, the *Human Rights Watch* advises people in China to make use of the Tor Browser to avoid abuses by the state (2).

Based on a meta-analysis of studies related to internet privacy concerns, privacy literacy, and the adoption of privacy-protective measures, it was found that there is no strong correlation between national privacy laws and protective behaviors (3). This suggests that individuals do not rely on legal protections in their country, and more often take privacy into their own hands. It was also found that culture did not impact the use of privacy-protective behaviors in different countries.

While it may be easy to think censorship is only prevalent in non-western countries, such as China or Russia, it can also happen in democratic states. Weak privacy protections can lead to surveillance capitalism, where companies act as de facto censors by shaping information flows based on user data (4). For example, during the COVID-19 pandemic in the United States, it was recently revealed that Meta (formerly Facebook) was asked to censor certain information regarding COVID-19 (5). The United States Government and Meta actively engaged in the censorship of the people's right to free speech and expression, as humor and satire was also removed from the platform.

1.1.3 Background

This section will talk about internet censorship across the world and give a brief intro into the differences by general region

1.1.4 Global Censorship

1.2 Project Goals

The aim of this project is to ...

2 | State of the Art

2.1 Censorship Mechanisms

2.1.1 IP and DNS Blocking

2.1.2 Deep Packet Inspection (DPI)

2.1.3 Content Manipulation

2.2 Ireland

2.2.1 Censorship in the Past

According to a report from the United States Department of State in 2011, it was found that there were no government restrictions on access to the internet or that the government actively monitored email or internet chatrooms (6).

The Irish government engages in censoring or blocking the distribution of pirated copryrighted material. In 2009, the Irish Telecom Company, EIRCOM, blocked its customers from accessing the website *The Pirate Bay*. The Pirate Bay is a Swedish website which provides links to copyrighted material. The website was hit with a lawsuit from major record labels and many ISPs around the world agreed to block access to the website as part of the settlement. However, not all Irish ISPs complied. The cable TV operator UPC announced that it would not comply (7).

In alignment with international agreements, the Irish Government blocks access to websites that contain illegal content, such as Child Sexual Abuse Material (CSAM). The government has setup a hotline that allows citizens to anonymously report websites that they suspect contain illegal content, called hotline.ie (8).

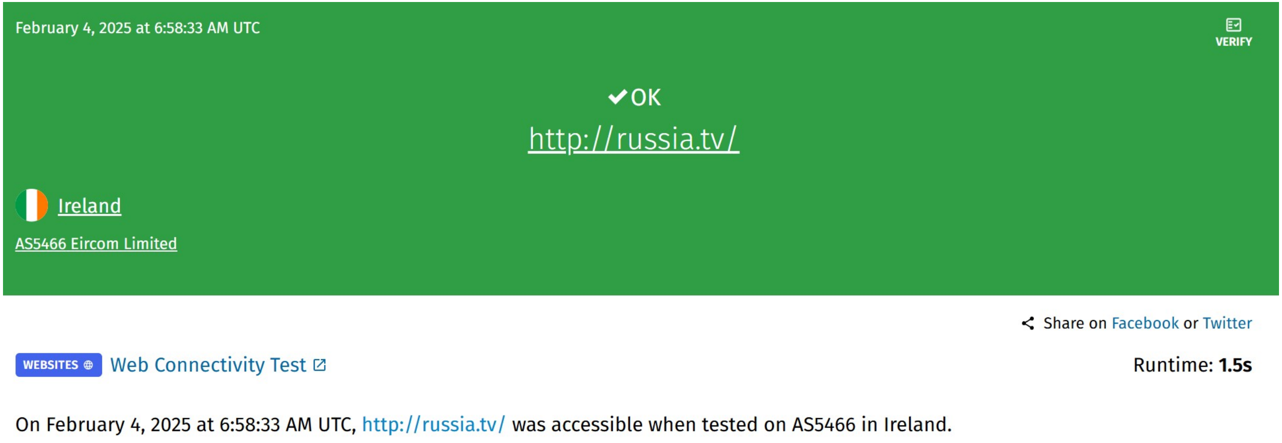
In contrast to other EU countries, Ireland does not have a broad government-mandated filtering system. They instead have the power through the Irish courts to mandate Irish ISPs to block certain websites. In addition, Irish ISPs may voluntarily enforce content filtering and website blocking in alignment with Irish content law.

Up until 2014, Ireland and other EU countries followed data retention laws, which required ISPs to store metadata for law enforcement purposes. In 2014, the European Court of Justice struck down the directive, which led to a change in this law in Ireland (9). After this change, Ireland enacted the *Communications (Retention of Data)(Amendment) Act 2022* (10). This legislation allows for the general and indiscriminate retention of communications traffic and location data on the grounds of national security, where approved by a judge.

2.2.2 Current Censorship

As a whole, Ireland's censorship efforts are limited and specific. The government and ISPs target mainly illegal and pirated content. Some specific websites that have been blocked include 1337x, Eztv, BMovies, GoMovies, Putlocker, Rarbg, WatchFree, and Yts (11). However, piracy websites are still widely accessible in Ireland.

It seems that Ireland has also rolled back blocks on some websites, such as Russian News outlets. Previously, the domain russia.tv, was blocked in Ireland. But as of 2025, it is able to be partially accessed. Based on data from the OONI project, there is evidence of TCP/IP blocking of this domain in Ireland. Based on the findings from OONI, this domain is able to be accessed when EIRCOM's root DNS server (AS5466, IP: 86.47.80.38) is used, but is blocked when accessed through Cloudflare's DNS server (AS14593, IP: 172.69.193.80).



February 4, 2025 at 6:58:33 AM UTC

VERIFY

✓OK

http://russia.tv/

Ireland

AS5466 Eircom Limited

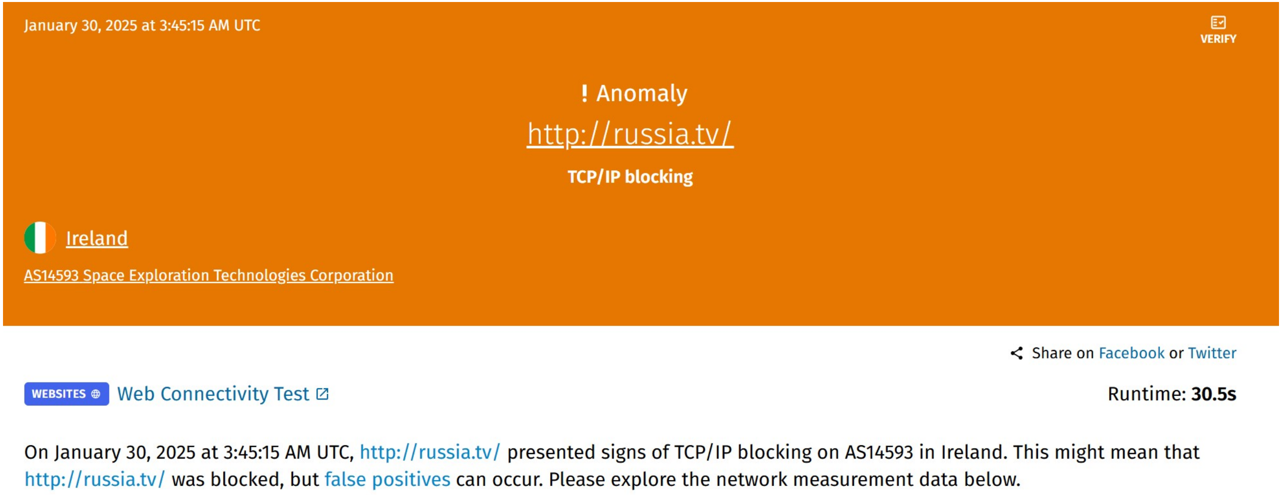
Share on Facebook or Twitter

WEBSITES Web Connectivity Test

Runtime: **1.5s**

On February 4, 2025 at 6:58:33 AM UTC, http://russia.tv/ was accessible when tested on AS5466 in Ireland.

Figure 1.1, EIRCOM DNS test for Russia.tv on OONI probe



January 30, 2025 at 3:45:15 AM UTC

VERIFY

! Anomaly

http://russia.tv/

TCP/IP blocking

Ireland

AS14593 Space Exploration Technologies Corporation

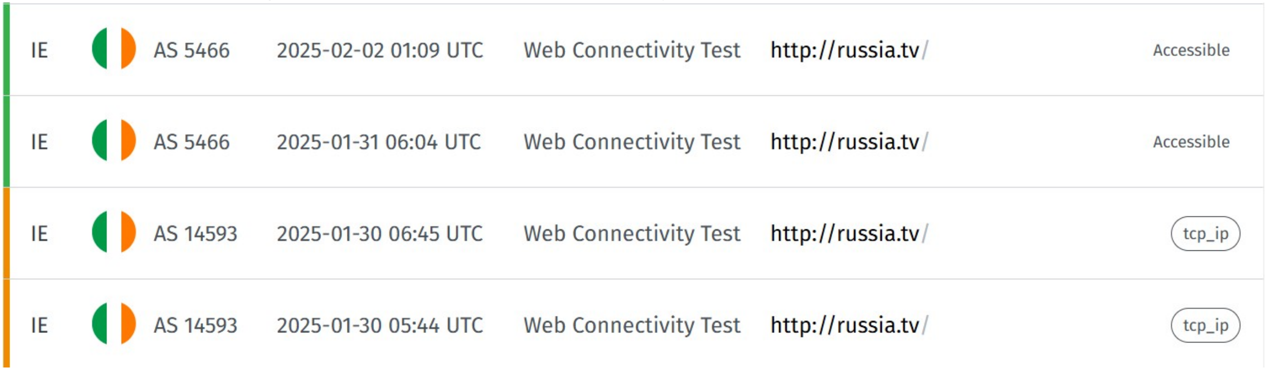
Share on Facebook or Twitter

WEBSITES Web Connectivity Test

Runtime: **30.5s**

On January 30, 2025 at 3:45:15 AM UTC, http://russia.tv/ presented signs of TCP/IP blocking on AS14593 in Ireland. This might mean that http://russia.tv/ was blocked, but false positives can occur. Please explore the network measurement data below.

Figure 1.2, CloudFlare DNS test for Russia.tv on OONI probe



IE	AS 5466	2025-02-02 01:09 UTC	Web Connectivity Test	http://russia.tv/	Accessible
IE	AS 5466	2025-01-31 06:04 UTC	Web Connectivity Test	http://russia.tv/	Accessible
IE	AS 14593	2025-01-30 06:45 UTC	Web Connectivity Test	http://russia.tv/	tcp_ip
IE	AS 14593	2025-01-30 05:44 UTC	Web Connectivity Test	http://russia.tv/	tcp_ip

Figure 1.3, Russia.tv domain search on OONI

2.3 Iraq

2.3.1 Censorship in the Past

Most people in Iraq did not have access to the internet until the mid 2010s. This section might be redundant as not much has changed.

2.3.2 Current Censorship

In a 2023 report from the United States Department of State, it was found that the government of Iraq restricted or disrupted access to the internet and censored online content, in conjunction with monitoring private online communications without appropriate legal authority (12). The Iraqi government and the Kurdistan Regional Government (KRG) consistently engage in implementing internet outages during protests or times of unrest (13). In 2023, Iraqi officials implemented 66 internet outages, more than any other country in the world. Most, if not all, internet infrastructure is controlled and managed by the government.

After the fall off Saddam Hussein's Regime in 2003, the internet became much more accessible and the information landscape was opened. However, the current-day Iraqi government occasionally blocks websites, and more often social media websites in order to maintain stability and control during times of unrest (13). During anti-government protests in 2019, the Iraqi government blocked access to Facebook, X (Formerly Twitter), WhatsApp, and Instagram. In protests in 2018, some users in Iraq found that they were unable to use VPNs to circumvent website blocking. The government routinely engages in the censoring and blocking of Pornography and Gambling websites on the guise of protecting their citizens from harmful content.

2.4 Censorship Circumvention Tools

2.4.1 The Tor Browser

The Tor Project Background

The Tor Browser is built on a concept called *Onion Routing*, which was developed in the 1990s by researchers at the United States Naval Research Laboratory. The goal of the project was to create a communication method where data is wrapped in multiple layers of encryption so that no point in the network could reveal the sender and receiver (14). Originally, the United States Government used the Tor network to access potentially illegal websites anonymously, and transmit data. But because only the US Government was using it at the time, it was easy to tell who the single anonymous user was, when viewing the site logs. It would also have made Tor a target for bad actors, as they could be sure that all data being sent over the network was related to the United States Government/Military.

To stop this from happening, the US Government released Tor to the public in the early 2000s, and later it became the Tor Project, a non-profit organization funded by the United States that develops and maintains the Tor software.

Technical & Circumvention Information

Internet traffic sent over the Tor network is encapsulated in multiple layers of encryption. Think of your data as a letter that is placed inside several envelopes. Each node in the network removes one envelope, revealing only the information necessary to pass the message along to the next node. To do this, the Tor browsers sends your data through at least three nodes, and the pathway of these nodes are randomly constructed and reconstructed during your session (15).

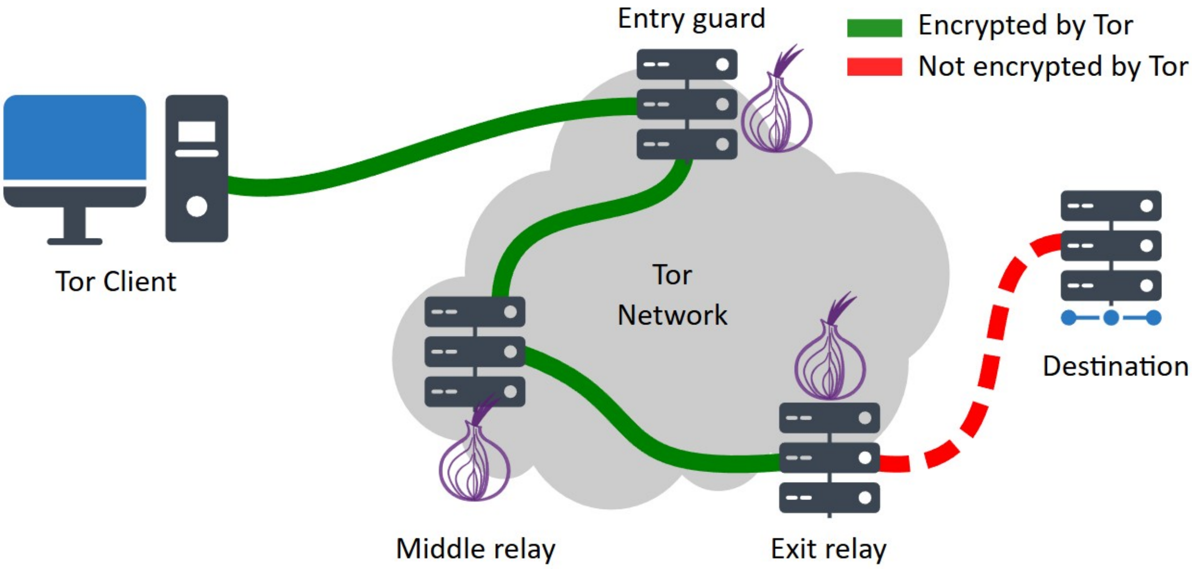


Figure 1.4, How the Tor Network Works

Tor is a great tool to combat censorship. Tor's distributed architecture of nodes makes it resilient against localized censorship efforts. In countries where the Tor network is blocked, users are able to use "Bridges", which are Tor nodes that are not listed publicly. Using a bridge address allows for the user to connect to the network covertly (16). Users can also avail of "Pluggable transports", which transforms Tor traffic to look like regular network traffic. This method can help circumvent censorship in regions that use *Deep Packet Inspection* (DPI) and other forms of advanced internet censorship (17).

2.4.2 VPNs

3 | Methodology

3.1 Introduction

3.2 The OONI Probe

3.2.1 Background of OONI

The Open Observatory of Network Interference (OONI) project was started in 2012 as a non-profit open-source software project aimed at identifying and documenting internet censorship around the world (18). The OONI organization openly publishes measurements and provides a public archive on network interference from across the world.

3.2.2 Data-Collection

3.3 Challenges & Limitations

4 | Results and Discussion

5 | Security Privacy

6 | Conclusions

Bibliography

[1] &xBB; The Great Firewall of China: Background Torfox — cs.stanford.edu. `https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html`, . [Accessed 18-02-2025].

[2] Eric Jardine. Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies. `https://journals.sagepub.com/doi/full/10.1177/1461444817733134`, 2017. [Accessed 29-01-2025].

[3] Lemi Baruh, Ekin Secinti, and Zeynep Cemalcilar. Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67(1): 26–53, 2017.

[4] Paul M Schwartz. Internet privacy and the state. *Conn. L. Rev.*, 32:815, 1999.

[5] Zuckerberg says the White House pressured Facebook to 'censor' some COVID-19 content during the pandemic — pbs.org. `https://www.pbs.org/newshour/politics/zuckerberg-says-the-white-house-pressured-facebook-to-censor-some-covid-19-conte` [Accessed 01-02-2025].

[6] Technical Difficulties — 2009-2017.state.gov. `https://2009-2017.state.gov/j/drl/rls/hrrpt/2011humanrightsreport/index.htm?dlid=186364#wrapper`, . [Accessed 04-02-2025].

[7] Eircom to block internet access to Pirate Bay as other firms refuse — irishtimes.com. https://www.irishtimes.com/news/eircom-to-block-internet-access-to-pirate-bay-as-other-firms-refuse-1.722015, . [Accessed 04-02-2025].

[8] About &x2013; Hotline — hotline.ie. https://hotline.ie/about/. [Accessed 04-02-2025].

[9] Practical Law IPIT. ECJ declares Data Retention Directive invalid. https://uk.practicallaw.thomsonreuters.com/5-564-2768?contextData=(sc.Default)&transitionType=Default&firstPage=true#:~:text=The%20ECJ%20has%20ruled%20that%20the%20Data%20Retention,%281%29%20of%20the%20EU%20Charter%20of%20Fundamental%20Rights. [Accessed 04-02-2025].

[10] Data retention law to be brought into effect — irishlegal.com. https://www.irishlegal.com/articles/data-retention-law-to-be-brought-into-effect, . [Accessed 04-02-2025].

[11] John Kennedy. Movie industry victory as eight piracy sites blocked in Ireland — siliconrepublic.com. https://www.siliconrepublic.com/enterprise/movie-piracy-ireland-legal-action-isps. [Accessed 04-02-2025].

[12] Technical Difficulties — state.gov. https://www.state.gov/wp-content/uploads/2024/03/528267_IRAQ-2023-HUMAN-RIGHTS-REPORT.pdf. [Accessed 08-02-2025].

[13] Iraq: Freedom on the Net 2024 Country Report | Freedom House — freedomhouse.org. https://freedomhouse.org/country/iraq/freedom-net/2024#footnote1_d8PVkoU73PsQqsV4AnRY-VMTJWntGAP2vv547rIRUA_vIch24iLQyPS. [Accessed 08-02-2025].

[14] The Tor Project | Privacy & Freedom Online — torproject.org. https://www.torproject.org/about/history/, . [Accessed 07-02-2025].

[15] Roger Dingledine, Nick Mathewson, Paul F Syverson, et al. Tor: The second-generation onion router. In *USENIX security symposium*, volume 4, pages 303–320, 2004.

[16] BRIDGES | Tor Project | Tor Browser Manual — torproject.github.io. https://torproject.github.io/manual/bridges/, . [Accessed 07-02-2025].

[17] CIRCUMVENTION | Tor Project | Tor Browser Manual — torproject.github.io. https://torproject.github.io/manual/circumvention/, . [Accessed 07-02-2025].

[18] About — ooni.org. https://ooni.org/about/. [Accessed 25-01-2025].

A1 | Appendix

You may use appendices to include relevant background information, such as calibration certificates, derivations of key equations or presentation of a particular data reduction method. You should not use the appendices to dump large amounts of additional results or data which are not properly discussed. If these results are really relevant, then they should appear in the main body of the report.

A1.1 Appendix numbering

Appendices are numbered sequentially, A1, A2, A3... The sections, figures and tables within appendices are numbered in the same way as in the main text. For example, the first figure in Appendix A1 would be Figure A1.1. Equations continue the numbering from the main text.