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

SCHOOL OF COMPUTER SCIENCE AND STATISTICS

COMPARING INTERNET CENSORSHIP IN IRELAND VS. ISRAEL

CHRIS CASEY

DR. STEPHEN FARRELL

MARCH 2, 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 Research Motivation

Since its inception, the Internet has served a vast user base that wishes to communicate with one another and spread information. By design, the Internet is a platform that should provide unfiltered content to users. In many cases this content may otherwise be inaccessible by traditional media outlets such as radio or TV. Originally designed to aid government researchers share information, its open and transparent foundation has since changed. Across the globe, governments and other entities are censoring the internet by network manipulation, legislative pressure or otherwise. This is a global threat to fundamental internet user rights and should be treated as such. It is for these reasons that this area ought to be investigated more thoroughly.

Although censorship of certain content (CSAM, pirated entertainment) is widely considered appropriate, normalising this has far reaching consequences on user privacy and free speech. The importance of establishing a quantitative approach to measuring internet censorship cannot be overstated as users are unaware of invisible content in most cases. As a result, the state has a large influence over what ideas can propagate within its borders. Various open-source and community led projects aimed at addressing this issue. Notable examples include the Tor project, OONI, Tails OS and others. However, it is coming to light that this technology is becoming deprecated. In 2022, German police were able to make an arrest after de anonymising

Tor traffic using timing analysis. [1]. This highlights the large dichotomy between what users believe governments are capable of and reality.

For the above reasons, the increasingly pervasive censorship done by governments and corporations around the world is concerning.

1.1.1 Practical Implications

1.1.2 Awareness & Transparency

1.1.3 Problem Statement

1.2 Background

1.2.1 Global Internet Censorship

Experts suggest that censorship on the internet is increasing at an alarming rate. “The majority of countries that censor content do so across all four themes, although the depth of the filtering varies. The study confirms that 40 percent of these 2,046 websites can only be reached by an encrypted connection (denoted by the "HTTPS" prefix on a web page, a voluntary upgrade from "HTTP").” [4] It is also clear that more and more countries are viewing this as a necessary solution to the unique problems they have. Whether this is appropriate or not, it is happening, and users should be aware of this.

Governments have a vested interest in maintaining control over telecommunications industries and public internet use. Whether protecting state secrets, preventing cyber crime piracy or acts of terrorism, insulating from perceived negative influence, aiding in the creation of propaganda or otherwise; a large majority of governments choose to exercise inordinate control over the information available to its public.

As more governments and entities began to engage in this, it became increasingly important to hold them accountable. As a result, the ‘Enemies of the Internet’ list was

devised. It contains the governments and entities that actively engage in the repression of online freedoms, in the form of censorship and surveillance. As of 2014, there were 19 governments that fit this criterion but by now this number has likely increased. [5] Traditionally, censorship involved monitoring a handful of media and cutting undesirable content, potentially replacing this with a message more in line with the agenda and norms of the locale. However, with the advent of the internet, this distribution of information became decentralised and thus allowed for more expression and freedom in the content consumed by a user. As a result, censorship has become more difficult to conduct, but potentially easier to get away with. Nowadays, governments leverage points of control, network-level filtering and many other techniques to block undesirable content.

1.2.2 User Privacy

1.2.3 Censorship vs. Surveillance

1.2.4 Legislation

Governments can enforce censorship directly through ISPs, tech companies and social media platforms by creating new legislation or simply mandating content be removed. This is used to deplatform individuals and movements during periods of unrest. This is also done in app stores, shutting down entire platforms that are deemed problematic.

1.3 Project Scope

1.3.1 Project Objectives

Below is an outline of the objectives completed during the duration of the project:

- To conduct a literature review to identify and evaluate existing censorship

measurement tools with a focus on OONI.

- To understand how and why censorship is conducted in these countries and how it can be measured.

- To collect data using OONI and other sources for both countries. Use historical datasets as well as rerunning tools for up to date data.

- To conduct a comparative analysis between the two countries' datasets.

- To consider ethical implications of the research early so as to ensure compliance.

- To set up VMs in Israel in order to establish ground truth.

- To present high-level findings about the two countries approach to censoring the experience of their internet users, make conclusions about the attitudes and values present in each locale based on the data collected.

- To understand more about the unique situations of both Ireland and Israel, and how censorship is used by the state considering this.

1.3.2 Core Research Questions

1.3.3 Data Collection & Analysis Tools

1.4 Ethical Considerations

1.4.1 GDPR and Data Privacy

1.4.2 Potential Risks

2 Literature Review

2.1 Introduction

Write an introduction outlining the reasons for lit review... Briefly elude to some high level differences between Ireland and Israel.

67.4

2.2 Literature Review Methodology

2.3 Findings of the Literature Review

2.3.1 Ireland Historically (Griff)

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 copyrighted 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.

2.3.2 Ireland Today (Griff)

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).

2.3.3 Israel Historically

2.3.4 Israel Today

2.4 Analysis: Ireland vs Israel

2.4.1 Similarities

2.4.2 Differences

2.5 Conclusions

3 State of the Art

3.1 Introduction

In order to quantify internet censorship conducted across the globe it is important to

3.1.1 Overt vs. Covert Censorship

ICLab, a censorship measurement tool very similar to OONI, released a paper in 2020 describing the need for their contribution. In this paper, the author highlights an important distinction between covert and overt censorship: 'In overt censorship, the censor sends the user a 'block page' instead of the material that was censored. In covert censorship, the censor causes a network error that could have occurred for other reasons, and thus avoids informing the user that the material was censored." (1) This is a concerning capability as it alludes to the potential for censorship to go unchecked.

3.2 Censorship Techniques and Mechanisms

3.2.1 Points of Control

Key control points are nodes in the Internet's architecture that connect a large user base to the wider network, making them attractive targets for censorship enforcement. Governments and institutions use leverage these points in order to

restrict user access. Some points of control include ISPs, IXPs, VPNs, national gateways and local networks. Institutions will typically use a combination of legislative pressure, technological and economic means to snuff out content. ISPs and VPNs face significant and constant pressure from legal arms to expose user data and manipulate the content available to a user.

These locations in the internet infrastructure are invaluable to those wishing to conduct internet censorship. Though security considerations such as HTTPS and TLS can protect users from MITM attacks, points of control are a physical reality which cannot be avoided. At some point, packets coming from the user will inevitably pass some point of control and thus will be prone to surveillance. In this way, points of control are a consideration for all internet users.

3.3 Network-Level Filtering

3.3.1 IP and DNS Blocking

Prevents access to certain websites by blocking their addresses. This was originally used to prevent email spam but is now used broadly as a censorship technique. DNS tampering falls into a similar category and involves rerouting requests to block domains.

3.3.2 Deep Packet Inspection

Deep packet inspection involves looking into payloads and data within packets, beyond its header. It is a sophisticated technique usually performed as part of a firewall defense and involves making real time decisions about the nature of each packet. DPI functions at the application level and can be used to identify both the sender and recipient of the packet by examining its payload. Compared to regular packet inspection which is only concerned with basic header information, it is considerably more costly.

Deep packet inspection is used in specific cases where a higher level of scrutiny is required. This includes packets carrying malware, content that has been blocked and intrusion efforts. DPI is usually performed by network middle boxes, devices that lie between end points. One of the these middle boxes is BlindBox, a system that accommodates DPI while preserving privacy and encryption. The creators of this system highlight the potential risks to user privacy with other black boxes. "To enable middlebox processing, some currently deployed middlebox systems support HTTPS in an insecure way: they mount a man-in-the-middle attack on SSL and decrypt the traffic at the middlebox." (2)

Though its deployment is limited, DPI represents a significant risk to user privacy. Not all middle box providers offer the protections and guarantees that BlindBox offer. Forecasts for the market show a troubling trend, with no guarantees of user privacy. "Global deep packet inspection (DPI) market size was anticipated to be worth USD 10.63 billion in 2024 and is expected to reach USD 79.26 billion by 2033 at a CAGR of 25% during the forecast period." (3)

3.4 Content Manipulation

3.4.1 Keyword Filtering

Keyword filtering involves detecting flagged words in messages and searches dealing with these as appropriate.

3.4.2 Search Engine Manipulation

Altering the ranking of websites or totally removing them from search results. This is done by companies like Google to incentivise paying for exposure, to censor content for compliance reasons, improve user experience and more.

3.4.3 MITM Attacks

A man-in-the-middle attack involves intercepting encrypted packets (potentially at a point of control), to potentially alter or block internet traffic. Governments have been seen to pressure VPNs into routing traffic through designated MITM servers. Inevitably this allows for selective content manipulation, deep packet inspection and surveillance. MITM attacks are particularly concerning due to their covert and intrusive nature.

3.4.4 DNS Hijacking/ Injection

As previously touched upon, DNS manipulation involves redirecting users by returning incorrect IP addresses. This is used to route users to controlled versions of websites or block access entirely.

3.4.5 Legal and Economic Pressure

Governments can enforce censorship directly through ISPs, tech companies and social media platforms by creating new legislation or simply mandating content be removed. This is used to de-platform individuals and movements during periods of unrest. This is also done in app stores, shutting down entire platforms that are deemed problematic.

3.5 Surveillance and Deanonymisation

In discussing internet user rights it is crucial to touch upon privacy and anonymity...

Efforts to identify users based on their traffic range from trivial to extremely complex based upon the protections employed by the user. Operational security, the collection of measures taken by an individual to protect their online anonymity, is often overlooked by internet users. Projects like Tor, Tails OS (an amnesiac Linux

distribution), and Briar (secure off-grid communication) as well as VPNs aim to protect users' identity. However, we have seen they are prone to failing. Though it is expected that a VPN service provider is vulnerable to the scrutiny of the jurisdiction they operate within, and thus it is likely they will comply with demands, issues within Tor's anonymity claim are significantly more impactful to user rights. See below section for more information on Tor.

Previously, it was touched on that German authorities managed to de anonymise Tor users by deploying timing attacks. This was a concerning development in 2022 as basic internet privacy was called into question. Users assume taking measures like using Tor would provide robust privacy guarantees; however, as of late this has been undermined by several tactics used by adversaries around the globe.

3.5.1 Timing Attacks

3.5.2 Side Channel Attacks

3.5.3 Machine Learning

It has been shown that deep learning models can be used to analyse network fingerprints to infer user identities.

4 | Circumvention Tools

Users who care about privacy and anonymity have options to increase their operational security. Some of these tools are outlined below.

4.1 Virtual Private Networks

INSERT general paragraph explaining commercial VPNs, logs policies etc.

Virtual Private Networks (VPNs) are one of the most commonly used circumvention tools. VPNs work by establishing a private tunnel in the public network through which users traffic is encrypted and routed. This allows users to mask their IP address and change their apparent geo - location. This grants both privacy and circumvention potential; VPNs can be used to avoid geo - restrictions by routing traffic through more lenient countries.

VPNs also protect users from cybercrime through their use of encryption and secure protocols...

The role of VPNs in personal privacy and censorship circumvention cannot be overstated due to how commonplace the technology has become. INSERT A STAT ABOUT VPN USAGE

4.1.1 Peer-to-Peer VPNs

4.2 TOR & Proxy Solutions

The Onion Router, originally developed by the US government, is an open-source network overlay that routes internet traffic through volunteer-operated relays. According to the founders "Onion Routing is a distributed overlay network designed to anonymize TCP-based applications like web browsing, secure shell, and instant messaging."[]

Requests travel through a relay passing three separate nodes. As a result, it is significantly more difficult to interpret the request's origin and destination. Tor is also commonly used as a censorship circumvention method. Tor was believed to be secure for a long time but recent developments would suggest otherwise. []

4.2.1 TOR Bridges

4.2.2 Mesh Networks

4.2.3 SSH Tunneling

4.3 Domain Name System

4.3.1 Domain Fronting

4.3.2

4.3.3

4.4 Privacy & Communication

4.4.1 Encrypted Communication

4.4.2 Email & Browsing

4.4.3 Tails OS

4.5

4.5.1

4.5.2

4.5.3

5 Methodology

5.1 Introduction

5.2 The OONI Probe

5.2.1 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 (4). The OONI organization openly publishes measurements and provides a public archive on network interference from across the world.

5.2.2 Data-Collection

5.3 Challenges & Limitations

6 Results

7 | Conclusions

Bibliography

[1] Arian Akhavan Niaki, Shinyoung Cho, Zachary Weinberg, Nguyen Phong Hoang, Abbas Razaghpanah, Nicolas Christin, and Phillipa Gill. Iclab: A global, longitudinal internet censorship measurement platform. pages 135–151, 2020. doi: 10.1109/SP40000.2020.00014.

[2] Justine Sherry, Chang Lan, Raluca Ada Popa, and Sylvia Ratnasamy. Blindbox: Deep packet inspection over encrypted traffic. In *Proceedings of the 2015 ACM conference on special interest group on data communication*, pages 213–226, 2015.

[3] Deep packet inspection (dpi) market size. *Business Research Insights*.

[4] 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.