

# Literature Review:

Chris Casey

4<sup>th</sup> Year D stream, BAI

20334271

[ccasey3@tcd.ie](mailto:ccasey3@tcd.ie)

02/02/25

Title: 'Compare censorship experienced in Ireland with another country'

Advisor: Stephen Farrell

SCSS

## Introduction

The purpose of this document is to establish an understanding of how internet censorship has and is being conducted. Emphasis will be given to Ireland and Israel as these are the countries to be compared in the thesis, as well as more egregious examples worldwide. In conducting background research, we hope to learn more about censorship methodology, circumvention techniques, points of control and the global situation regarding freedom of information, press and speech.

In collaboration with Griff Steinman, censorship in Ireland will be researched. Due to this overlap, work will be divided to avoid redundant efforts. Therefore, this literature review is less concerned with Ireland and focuses primarily on the historical context required to understand censorship methods and how it is conducted across the globe. A broad scope was deemed acceptable for now.

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 projects aimed at addressing this issue. Notable examples include the Tor project, OONI, Tails OS and others. However, it is coming to light that in some cases this technology is becoming deprecated. In 2022, German police were able to make an arrest after deanonymizing Tor traffic using timing analysis. [1]. This highlights the large dichotomy between what users believe governments are capable of, and reality.

## Abstract

Since its foundation, the internet has served a vast userbase that wishes to communicate with one another and seek out information. By design, the internet is a platform that should serve to

provide unfiltered information to users, inaccessible by more traditional media sources like radio. It is for this reason that the increasingly pervasive censorship done by governments around the world is so concerning. Now, more than ever, individuals rely on the internet for ground truth. The thesis looks to investigate this using online data collection tools (OONI probe) as well as virtual machines in the locale (Ireland & Israel).

It is important to make a distinction between censorship and surveillance. Though the two are inherently linked, the focus of the dissertation is on censorship and thus surveillance will only be touched on. This is largely due to surveillance going undetected for the most part, with historical cases having been researched to exhaustion.

### **Background [From my project plan]**

Internet users across the globe experience varying levels of censorship, reflecting cultural norms, local customs and tradition, and government policy. For this project our concern is focused on the suppression of information at a government level. The project is not concerned with CSAM or similar illegal content, but rather how, (and to what extent), a government influences the content consumed by individuals in the jurisdiction. The goal of the project is to compare the censorship situation faced in Ireland against another country.

Analysis of the censorship experienced in Ireland will be conducted in collaboration with another student assigned the same project, Griffin Steinman ([steinmag@tcd.ie](mailto:steinmag@tcd.ie)).

My supervisor and I have agreed that Israel would be a compelling comparison. Reasons for this include the country's complex ongoing international relations, an interesting overlap in cultural norms when compared to Ireland and a detailed history of conducting censorship on the internet. The country's uniqueness and distinct abundance of neighbouring adversaries have made national security an issue that Israel must always stay ahead of. Israel ranks quite poorly in the World Press Freedom Index (WPFI) at 88, further evidence that it would make for an interesting comparison. [2]

Though some censorship is widely considered appropriate, (for example explicit content), there are far reaching consequences on free speech and an individual's capacity to seek out 'undesirable' information when this is commonplace. In the worst of cases, information can be weaponised and used as propaganda. For reasons such as this, it is important to hold governments accountable to the internet experience given to their users.

The data collection will be done using the Open Observatory of Network Interference (OONI) primarily. The OONI probe, originally launched under the TOR project, is an open source community lead project aimed at quantifying censorship on the internet globally. Each probe runs a litany of internet connectivity tests to do this, and thus the project is community driven. [3] Once a large enough set of data has been collected, a comparative analysis will be conducted. This comparative analysis strives to highlight the different targets, methods, and extents of censorship in the two countries.

Ethical considerations will be paramount due to the sensitive nature of the thesis. Running these tests in certain regions could pose significant risk so care must be taken to adhere strictly to ethical and legal frameworks highlighted by my advisor or otherwise. GDPR and privacy considerations will also be critical to the project's successful completion.

## **Internet Censorship Historically**

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 cybercrime 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 all of the governments and entities that actively engage in the repression of online freedoms. This comes in the form of censorship and surveillance. As of 2014, there were 19 governments who fit this criterion but by now this number has likely increased. [5]

## **Internet Censorship Methods**

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.” [6]

## **Circumvention Methods**

### **State of the Art**

### **Cases of Interest**

Arguably, the most damning case of internet censorship can be seen in China. []

Project goals

## References

- [1] <https://securityaffairs.com/168667/security/tor-project-commented-on-deanonymizing-technique.html>
- [2] <https://rsf.org/en/2023-world-press-freedom-index-journalism-threatened-fake-content-industry>
- [3] <https://explorer.ooni.org/>
- [4] Zittrain, J., Faris, R., Noman, H., Clark, J., Tilton, C., & Morrison-Westphal, R. (2017). The Shifting Landscape of Global Internet Censorship. *Harvard Law School*.  
<https://doi.org/10.2139/ssrn.2993485>.
- [5] <https://rsf.org/sites/default/files/2014-rsf-rapport-enemies-of-the-internet.pdf>
- [6] Niaki, A., Cho, S., Weinberg, Z., Hoang, N., Razaghpanah, A., Christin, N., & Gill, P. (2019). ICLab: A Global, Longitudinal Internet Censorship Measurement Platform. *2020 IEEE Symposium on Security and Privacy (SP)*, 135-151.  
<https://doi.org/10.1109/SP40000.2020.00014>.
- [ ] Warf, B. (2011). Geographies of global Internet censorship. *GeoJournal*, 76, 1-23.  
<https://doi.org/10.1007/S10708-010-9393-3>.
- [ ] Liang, B., & Lu, H. (2010). Internet Development, Censorship, and Cyber Crimes in China. *Journal of Contemporary Criminal Justice*, 26, 103 - 120.  
<https://doi.org/10.1177/1043986209350437>.