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

APRIL 9, 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

This work presents a comparative study of internet censorship in Ireland and Iraq. This work is one of many in a series of such comparisons and was completed alongside Chris Casey. Ireland and Iraq have significantly different political structures, legal frameworks, and cultural norms. As a result, internet censorship is implemented differently in both countries. Ireland, as a member of the European Union, implements specifically targeted censorship that stems from legal and regulatory compliance. Iraq demonstrates a more decentralized, reactionary approach, often influenced by political instability and internal events. This work aims to research and analyze the technical methods, scope, and motivations behind censorship in each country. The work utilizes the Open Observatory of Network Interference (OONI) Probe to collect network data over a nine-day testing period in both countries. Network testing conducted in Ireland was conducted locally using the OONI Command Line Interface Probe, while network testing in Iraq was done through a Virtual Machine hosted in Baghdad. The data collected included testing for website accessibility, evidence of circumvention tools being blocked, instant messaging platform availability, and signs of network manipulation through middleboxes.

Results indicate that both countries exhibit instances of website blocking, with Iraq having a slightly higher block rate of 7% compared to Ireland's 2.5%. Blocking methods in both countries include TCP/IP and DNS interference, and evidence that TLS / SNI-based filtering may be present in some areas of Iraq. Most of Ireland's blocks are related to illegal content, legal cases, and EU compliance. Iraq's censorship extends

to political, religious, and most often communication platforms, as internet blackouts are common in the region during times of unrest or national exams. Both countries showed little evidence of systemic efforts to block circumvention tools, but some areas in Iraq showed significant evidence of Psiphon being blocked.

This work aids in the global effort to bring attention to internet censorship happening around the world. Contributing to projects like OONI is important, as it helps researchers identify internet censorship trends across certain countries, and brings awareness to network interference taking place. Protecting peopl's digital rights, privacy, and internet freedoms is growing increasingly more important, as governments and other entities expand their ability to monitor, restrict, and manipulate online information in ways that can undermine democratic values, personal privacy, and global access to information.

Acknowledgements

A special thank you to my mother and father for supporting me.

A special thank you to Eugene O'Rourke and Mark Linnane for their guidance and advice.

Contents

1 Introduction

1.1 Project Motivations

As the internet became available to more people across the world, access to digital information became a fundamental principle of democratic engagement and global communication. The concept of humans being able to know exactly what is happening at any time on any part of the globe is very new, and some countries and regimes have pushed back on this idea. This pushback has led to the censorship of information on the internet in some parts of the world. While countries such as China and Iran are known for having extensive censorship mechanisms in place, this work is motivated by the need to examine different types of regimes - those being Iraq and Ireland, and the comparison of the two.

Ireland, a member of the European Union, uses a censorship model based on limited and specific censorship. Most of Ireland's censorship is rooted in judicial and legal oversight. By contrast, Iraq demonstrates a relatively more reactive approach to censorship, characterized by intermittent shutdowns and varying regional enforcement. These two countries have large differences in government, culture, and social norms, which offers a unique perspective on how different regimes manage internet freedom.

This project is also motivated by the need for more publicly available empirical data in regards to internet interference. The Open Observatory of Netowrk Interference (OONI) Probe allows for real data to be published to further contribute to the

analysis of this work.

1.2 Project Goals

The aim of this project is to conduct a comparative analysis of internet censorship practices in Ireland and Iraq. By using tools such as the Open Observatory of Network Interference (OONI) Probe, this work aims to identify and document the presence, mechanisms, and the extent of internet censorship in both countries.

1.3 Internet Censorship and Privacy

1.3.1 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.

1.3.2 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.

1.3.3 Global Censorship (Chris)

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")" (6). 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 (7). 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.

2 State of the Art

2.1 Introduction

The purpose of this section is to give a high-level overview of common internet censorship mechanisms, the past and present landscapes of internet censorship in Ireland and Iraq, and a brief description of some circumvention tools. This review was conducted using publicly available information and data published on the internet.

2.2 Censorship Mechanisms

The following section is based primarily on information from the source *RFC 9505 A Survey of Worldwide Censorship Techniques* (8). Any other information sourced from elsewhere is identified as such.

2.2.1 IP Blocking

Shallow Packet Inspection

Shallow packet inspection refers to the action of looking at the transport layer segment (packet) headers to implement censorship based on the transparent source and destination IP addresses and port numbers. The information visible in the headers allows a censor to block content via IP blocklisting.

This method is easy to implement in some routers, but difficult to implement in

backbone or ISP routers at scale. It is usually implemented alongside Deep Packet Inspection using middleboxes.

Internet Protocol (IP) blocking is one of the most straightforward censorship techniques, but it is also very crude. To implement an IP blocklist, the censor will create a route in a router's flow table that instructs the router to drop any packets matching a set IP address. In IPv4, this is done as a /32 route, and in IPv6 as a /128. However, due to the limited amount of space in router flow tables, this means that only a limited number of IPs can be blocked at a time, making it difficult to scale.

IP blocking can also cause content over-blocking. Because many websites share the same IP address, blocking one IP address can lead to multiple websites getting blocked within a network. Censors also sometimes block a range of IP addresses, which can lead to more over-blocking.

IP blocking is often ineffective against Content Distribution Networks (CDNs) and services that are hosted using multiple load-balanced IP addresses. This is because when the server hosting the content being sent changes its IP addresses, the block list may not include this new IP address, and the packets are not dropped. VPNs are an excellent tool to circumvent IP blocking as it routes the packets through different servers, changing the source and destination IP addresses along the way. This makes it nearly impossible to stop IP blocked content from getting through, as the source and destination IP addresses can be different for every packet coming from the original blocked source.

IP blocking can either be implemented at a centralized level or at an ISP level. In Ireland, IP blocking is done at an ISP level to block certain illegal websites in accordance with court orders (see section 2.2 for more information). In Iraq, IP blocking is implemented at the ISP level under the directive of the Ministry of Communications (9) (see section 2.3 for more details).

2.2.2 DNS Interference

DNS interference refers to the altering of responses from the DNS to block or filter access to certain content. This is usually done by either blocking the response, replying with an error message, or responding with an incorrect address. *DNS Mangling* is a network-level technique of on-path interception where an incorrect IP address is returned in response to a DNS query to a censored destination.

DNS Cache Poisoning is an off-path technique in which a censor intercepts and replaces the legitimate response from an authoritative DNS name server with a spoofed IP address. Instead of allowing the real IP address of a site to reach the user, the censor replies faster than the real server, and that spoofed IP gets cached (perhaps by numerous recursive resolvers). Subsequent requests will then be redirected to an incorrect IP, normally leading to a warning page or a meaningless domain. In other cases, such as in Iran, the censor can merely block the response of the upstream resolver, so the accurate IP address is never transmitted.

DNS Lying is the most authoritative approach, where a censor mandates that the DNS responses provided are to be different from what would actually be returned by the DNS server (8).

The above DNS interference methods require the censor to traverse a controlled DNS hierarchy for this mechanism to be effective. This mechanism can be circumvented by using a different publicly known DNS resolver that is not controlled by the censor. This mechanism can also lead to unintentional blocking in area's not controlled by the censor. For example, sometimes a user outside of the censor's region will be directed through DNS servers controlled by the censor, causing the request to fail. Considering all of this, DNS interference is not a very effective censorship mechanism.

2.2.3 Deep Packet Inspection (DPI)

Deep Packet Inspection consists of any kind of packet analysis beyond IP address and port number. DPI reassembles network flows to examine the application data section, and is often implemented using Middleboxes. DPI is often used for keyword identification, but this method can also determine packet size and flow timings to detect other forms of content, such as the difference between text or video packets. Although DPI has difficulty with encrypted data and is the most expensive form of censorship to implement, it is still the most powerful identification method and is widely used in practice (8).

2.2.4 Transport Layer Security (TLS)

Transport Layer Security (TLS) is a protocol that secures most web traffic in our modern-day internet. As more internet traffic has become encrypted, the way censorship is implemented had to adapt. When users use circumvention tools such as VPN's or proxy solutions, more common censorship techniques (such as IP blocking or DNS interference) are often unable to sufficiently block undesired content. As a result, TLS-based censorship became more common as this mechanism is able to deny access to specific sites or services without decrypting the actual TLS content.

Server Name Indication (SNI) Filtering

SNI Filtering is a widely used form of TLS-based censorship. The SNI is a TLS extension in the client's handshake (ClientHello) that indicates the hostname of the server the client wants to reach. In instances of anything up to TLS version 1.3 (assuming no additional encryption extensions are used), the ClientHello is sent in unencrypted plaintext. This allows a censor to read the requested hostname and block the connection if it is on a blocklist (10). This technique is implemented by many countries, and since 2018, the governments of China, Egypt, Iran, Qatar, South

Korea, Turkey, Turkmenistan, and the United Arab Emirates have implemented widespread SNI filtering or blocking (11). The Great Firewall of China has *"Long been censoring HTTPS in this manner"* by blocking connections that match forbidden hostnames in the SNI field (12).

The obvious way to circumvent SNI filtering is to encrypt the SNI. In TLS 1.3, this is introduced as encrypted ClientHello (ECH). Before ECH, there was an extension that allowed for the SNI to be encrypted, aptly named Encrypted Server Name Indication (ESNI). But using ECH or ESNI has led to overclocking as censors simply block all traffic using them. An example of this can be found again in China, where all ESNI or ECH traffic is blocked.

TLS Fingerprinting

TLS Fingerprinting is used to identify and block tools or protocols that a censor might want to block. The way a TLS ClientHello is structured is like a digital fingerprint that is unique to an application or library. Censors will collect known fingerprints and deploy Deep Packet Inspection rules to block or flag those TLS connections (13). For example, a regime might recognize the unique CLientHello packet of Tor's TLS and configure the network to drop any matching packets. This technique, which is known to be used in China and Iran, prompted Tor to develop more mimicry in its TLS handshake. Many other circumvention tools followed this example, and have since tried to camouflage their TLS handshakes to look more like those of a common browser (13).

2.2.5 Network Blackouts

A very straightforward, holistic, and blunt form of censorship is network blackouts. This method involves a large governing body of an area or region completely shutting off Internet access for all content. This method is becoming more and more common across areas in the Middle East and Asia. According to a report from *Access Now*, there were a total of 296 different internet shutdowns across 54 countries. This

is a 35% increase from the previous high in 2022 (14). This form of censorship is very extreme and is often implemented in times of conflict, protest and instability, exams, and elections.

2.3 Ireland

2.3.1 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 (15).

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 (16).

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 (17).

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 (18). After this change, Ireland enacted the *Communications (Retention of Data)(Amendment) Act 2022* (19). 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 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 (20). 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).

Figure 1.1, Russia.tv domain search on OONI

2.3.3 EU Compliance (CHRIS)

Aside from Irish legislation, there are EU directives that run in conjuncture such as the Digital Services Act, GDPR and more. These will be discussed in detail in this

section. Let us first establish the primacy of EU law as echoed in the Irish Constitution. "As well as being superior to national law, some EU law has direct effect on its citizens." (21) The European Commission proposes laws that are sent to the European Commission and then the Council of the European Union to be approved by a qualified majority and passed, or rejected. (22) This procedure has lead to the passing of legislation that affects internet usage in Ireland.

The first law to be discussed is General Data Protection Regulation (GDPR). This legislation is designed to protect user privacy and bolster data integrity. It highlights the acceptable procedures for handling user data and is used to police organisations. Penalties come in the form of fines, up to 20 million euros. (23) The second law that is worth mentioning is the Digital Services Act, which came into EU law in November of 2022, and was followed by the Irish law of the same name in 2024. (24) (25) This act addresses illegal content, disinformation and transparent advertising and thus, is of particular relevance to the research being conducted. The final example of EU legislation that has undoubtedly shaped internet censorship seen in Ireland is the Copyright Directive (2019). This legislation solidifies intellectual copyright law within the EU, providing some edge cases of where free use applies. (26) These three important pieces of legislation guide Ireland's internet censorship.

It has been mentioned that compliance is a strong motivation for the Irish government to censor and due to EU law primacy. Now, let us focus on some notable real world examples of legislation being used to censor content online or otherwise reprimand nonconforming organisations. Four high profile cases of non compliance will be discussed as well as the outcomes in each case.

1. Google and the "Right to be Forgotten" (2014) In 2014, the Court of Justice of the European Union (CJEU) ruled in Google Spain SL v. Agencia Española de Protección de Datos. This salient case granted individuals the right to request the removal of outdated personal data from search engine results. (27) This landmark ruling was based on the EU's data protection laws. The ruling had a profound impact on how

search engines and online platforms handle personal data. Google, as the largest search engine, were forced to make stark changes in their browser's operation, reshaping online content management. The decision triggered similar discussions on privacy and free speech, creating a global precedent for data removal requests.

2. YouTube and the EU Copyright Directive (2019) Under the EU Copyright Directive, Article 17 requires platforms like YouTube to prevent the upload of copyrighted content without permission. (28) This change forced YouTube to implement automatic content filtering systems. This mandated more stringent controls over user-uploaded videos, significantly impacting how online platforms handle user-generated content. Though it aimed to protect copyright holders, it also raised concerns about excessive censorship. Automatic filters could lead to the removal of legitimate content, raising a significant challenge in balancing copyright protection and free speech.

3. Facebook and the GDPR Fines (2021-2024) In 2021, Meta (formerly Facebook) was fined €265 million by Ireland's Data Protection Commission (DPC) due to a data breach that exposed personal information of millions of users. (29) The breach was linked to the company's failure to adequately protect user data, violating GDPR standards. Meta has faced a litany of fines at the hands of the EU and other regulating bodies. Meta has received fines of over 2 billion euros in 2024 alone. (30) This exemplifies the European Union's stringent enforcement of GDPR which holds companies accountable for safeguarding personal data.

4. Twitter's Non-Compliance with the Digital Services Act (DSA) In 2023-2024, Twitter (now X) faced scrutiny under the EU Digital Services Act (DSA) for failing to implement required measures to combat illegal content and misinformation. (31) The platform was given deadlines to comply, including implementing more robust content moderation policies. This case highlighted the increasing regulatory pressure on tech firms to ensure their platforms are safe, free of illegal content, and accountable for user actions. Previously, X withdrew from a voluntary agreement to

combat disinformation online. Despite this protest in the face of the Digital Services Act, legislators were quick to point out that X will still have to comply with EU standards. (32)

2.4 Iraq

2.4.1 Censorship in the Past

Iraqi internet censorship has been radically reshaped over the years. Under Saddam Hussein's regime, only a very few Iraqis had access to the internet, leading to the state controlling all parts of the internet within the country. Post-2003, with more people accessing the internet and the country struggling with internal conflict and the threat of radicalization, censorship was decentralized and usually carried out with little transparency and regionally differentiated. While the constitution and laws of Iraq recognize free expression, actual enforcement is usually slow whenever security is at stake. As the internet began to take a greater role, both as a platform for political discourse and a vehicle for extremist messaging, the censorship and intrusions of the government increased correspondingly. Generally speaking, the policy of controlling the internet in Iraq has mirrored the broader political and security situation, tightening whenever Iraq is unstable (9).

Historically, most of Iraq's censorship was implemented via DNS interference and IP Blocking. In 2014, a Citizen Lab test found around 20 URLs that were blocked, likely by DNS interference, and displayed a government block page. In these tests, when a user tried to visit a banned site, they either got an incorrect DNS resolution or their HTTP request was outright blocked (33). In 2014 TLS usage was much lower so DNS and IP blocking was more effective.

2.4.2 Current Censorship

Iraq's internet growth has progressed from state-controlled limitations during Saddam Hussein's era, where limited citizens used the internet. After 2003, many private ISPs were formed, but primary fiber routes and gateways that link Iraq to international submarine cable networks via adjacent countries are still controlled by the Ministry of Communications (34). Baghdad, the country's capital and commercial center, is a hub of national connectivity, and other large cities (like Basra and Mosul) typically have local backbones that connect into the national fiber network. The Kurdistan Region of Iraq (KRI) also has standalone network configurations, with cross-border fiber routes—particularly to Turkey—creating a semi-independent internet ecosystem (9).

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 (35). The Iraqi government and the Kurdistan Regional Government (KRG) consistently engage in implementing internet outages during protests or times of unrest (9). In 2023, Iraqi officials implemented 66 internet outages, more than any other country in the world. It is worthy to note that another organization, *Access Now* (36), reports a different number for Iraq in this year, and their data often conflicts with the data from *FreedomHouse*.

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 (9). 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.

Based on a CloudFlare analysis of internet shutdowns in Iraq during national exams in 2022-2023, it was found that instead of full shutdowns, Iraq would instead employ IP Blocking, SNI/HTTP-based filtering, and DNS interference (37). This shows that Iraqi authorities have the ability to implement TLS or SNI based filtering. It is important to note that Iraq's censorship framework is not as technologically entrenched or constant as China's or Iran's is. A 2022 freedom house report states that *"advanced automated censorship is not used outside the banking sector in Iraq"* (9). So up until 2022, Iraq did not have an automated censorship system in place that monitors all traffic.

However, in recent years Iraq seems to be moving toward a more formal and structured censorship system. In 2023, the Iraqi government announced plans to block Google's public DNS (8.8.8.8) and instead force users to use state-run DNS resolvers (38). The stated reason was to block "immoral" websites by domain name lookups. But as it stands right now, it can be said that while Iraq engages in internet censorship, it is much more a reactive approach than a proactive one.

2.5 Censorship Circumvention Tools

2.5.1 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 (39). 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 (40).

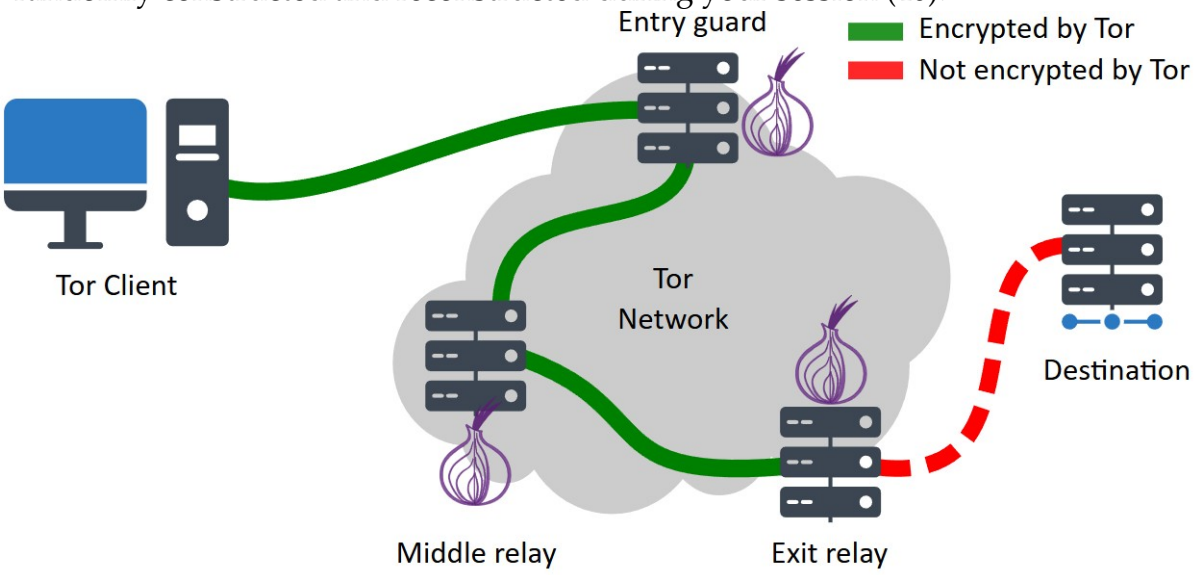

Figure 1.2, How the Tor Network Works

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 (41). 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 (42).

2.5.2 VPNs

Virtual Private Networks (VPNs) broadly speaking provide an end-to-end encrypted connection between your device and a VPN server. This method hides your IP address and grants the user anonymity while browsing over the network. This allows users to bypass censorship by connecting to servers outside of their location while masking their IP address (43).

2.5.3 Proxies

A proxy server is similar to a VPN as it fetches content on behalf of a user. When using a proxy, a user can request blocked content via a server in a non-censored region. From the perspective of the censor, the user is only connecting to the proxy server (which is ideally not blocked) and not the actual blocked content. For example, when *The Pirate Bay* was blocked by EIRCOM in Ireland in 2009 by court order, the website was still accessible via proxy servers (44).

2.5.4 Psiphon VPN

Psiphon is an open-source internet censorship circumvention tools developed at the Citizen Lab at the University of Toronto. Psiphon uses a combination of VPN, SSH, and Proxy techniques to gives users unfiltered access to the internet. The tool works by attempting to establish a secure tunnel though its distributed network of servers. Once a connection is established, internet traffic is routed through the Psiphon infrastructure. This method circumvents network-level censorship mechanisms such

as IP Blocking, DNS Interference, and some forms of Deep Packet Inspection.

The Open Observatory of Network Interference (OONI) Probe has a built in function to test if the Psiphon tool is blocked within a given network.

3 Methodology

3.1 The OONI Probe

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

3.1.2 Data-Collection

Web Connectivity Test

The Web Connectivity test determines if, and how, access to a specific website may be blocked. To do this, OONI Probe performs several checks from the network where the test is run and compares the results with measurements collected from a control network where censorship is not expected. If the measurements differ significantly, censorship techniques are likely used on the local network. This test is designed to perform the four different actions: Resolver Identification, DNS Lookup, TCP Connect, HTTP GET Request.

The Web Connectivity test begins by identifying the DNS resolver in use on the network. It achieves this by sending DNS queries to special domains, which disclose

the resolver's IP address. Once the resolver is identified, the test performs DNS lookups to determine which IP addresses (and potentially other host names) are mapped to the tested domain. After collecting that information, the test attempts to establish a TCP session on port 80 or port 443, depending on whether the URL uses HTTP or HTTPS. Finally, once the TCP connection is successful, the test sends an HTTP GET request to the server hosting the website; under normal circumstances, the server will respond with the requested webpage content (46).

Circumvention Test

The circumvention test is used to check weather Psiphon, Tor, or RiseupVPN are blocked on a given network. These are tools used to circumvent censorship by utilizing VPN, SSH, and HTTP proxy technologies.

The Psiphon VPN serves as a tunnel that enables you to circumvent censorship by connected you to an uncensored portion of the internet (47). The Psiphon test first uses Psiphon's own code to establish a Psiphon tunnel. After the tunnel is created, the test attempts to load a webpage to see if Psiphon actually works for accessing the internet. If the tunnel is successfully set up and the webpage loads, Psiphon is functioning on the tested network and can bypass censorship. If the tunnel is established but the webpage does not load, Psiphon is blocked in some way, preventing access to online resources. Finally, if the test cannot even create the Psiphon tunnel, it indicates that Psiphon is completely blocked on that network (48).

The Tor Test (49) automatically checks whether Tor is accessible in a given network by examining the reachability of core components such as Tor directory authorities, OR ports, and obfs4 bridges. It first attempts to retrieve the Tor consensus from directory authorities, then tries to connect to OR ports (including those of directory authorities) via a TLS handshake, and finally tests obfs4 bridges through an obfuscated handshake. If all of these steps succeed, Tor is likely usable in the tested network (unless it is blocked in ways not covered by the test). If any step fails, Tor

may be blocked and therefore unavailable on that network (50).

The RiseUpVPN test evaluates if the bootstrap servers used during the self-configuration of the VPN clients can be reached. The test also checks if RiseupVPN's gateways can be reached on different ports and transports (51). This test was contributed by the LEAP collective (52).

Instant Messaging Test

The Instant Messaging test is used to check weather WhatsApp, Facebook Messenger, Telegram, and Signal are blocked on a given network.

The Whatsapp test attempts to determine is there is any interference or blockage of it's App or Web Interface. To to this, the OONI probe attempts to perform an HTTP GET request TCP Connection, and DNS lookup to WhatsApp's enpoints. These include the endpoints used by the WhatsApp mobile app, the registration service, and the web interface (53). To conduct these tests, the OONI probe attempts to open TCP sockets towards WhatsApp endpoints on Ports 443 and 5222. If these connections fail or are rejected, it is seen as an indicator of blockage at the TCP level. The probe then verifies if the DNS resolution returned a valid IP address that is registered to WhatsApp. If the resolved IP address does not belong to WhatsApp, it can indicate DNS level blocking or tampering. And to check if the WhatsApp registration service is working correctly, an HTTP GET request is sent to the URL `https://v.whatsapp.net/v2/register`. The request is considered successful if there is no DNS, TCP connect, TLS (Transport Layer Security), or I/O error (54).

The Facebook Messenger Test is used to examine the reachability of the service within a tested network. The OONI probe begins by attempting to perform a TCP connect and DNS lookup to facebook's endpoints (55). The test verifies if Facebook Messenger endpoints resolve to consistently known IPs and if it's possible to establish TCP connections to them on port 443. For each endpoint tested, an A lookup for the domain name is performed and it is considered consistent if the IP is inside of

a netblock linked to the *Facebook Authonomous System Number* (AS32934) (56).

The Telegram Test is used to examine the reachability of Telegram's app and web version within a tested network. The telegram access points (DCs) are those used by the desktop client, and they have six unique IP addresses. The test establishes a TCP connection to all of the access point IP addresses and attempts to send a POST HTTP request to each of them. If all TCP connections on ports 80 and 443 fail, Telegram is considered to be blocked at the TCP level. Otherwise, Telegram is considered to be working as intended (57).

The Signal Test is used to measure the reachability of the Signal messaging app within a tested network. The test checks if it is possible to establish a TLS connection and send an HTTP GET request to the Signal server endpoints (58). A DNS query to `uptime.signal.org` is also performed to check if the backend servers are down (59).

Middlebox Test

A Middlebox is a computer networking device that transforms, filters, and manipulates traffic for purposes other than packet forwarding. These include network address translators, load balancers, and deep packet inspection (DPI) devices. The presence of Middleboxes can lead to evidence of censorship and/or traffic manipulation, but it can also be indicative of a less malicious intent, such as network caching.

The OONI Middlebox test consists of two main operations: HTTP Header Field Manipulation and HTTP Invalid Request Line. The HTTP header field manipulation test emulates an HTTP request towards a server, but sends HTTP headers that have variations in capitalization. These requests are sent to a backend control server which send back any data it receives, and if these requests return exactly as we sent them, it is assumed there is no middlebox present. If the alterations of the headers come back normalized, it can be assumed that there was packet manipulation of some kind,

leading to the confirmation of presence of Middleboxes It is worthy to note that false negatives can happen in this test, as some ISPs use highly sophisticated software that can disguise the presence of Middleboxes (60).

The HTTP Invalid request line test sends an invalid HTTP request to an echo service listening on the standard HTTP port, rather than a valid one. If the request is returned to the user exactly as it was sent, it can be concluded that there is no evidence of the presence of a Middlebox. However, it is possible that this invalid request can be intercepted by a Middlebox that triggers an error that is sent back to the probe. This is evidence that there is a Middlebox present in the network. It is worthy to note that false negatives are possible as some ISPs use highly sophisticated software that is designed not to trigger such errors (61).

3.1.3 Data Collection and Transparency

All results from OONI Probe tests are automatically sent to OONI's servers and published on the OONI explorer. This transparency ensures that anyone can explore the measurements for themselves. OONI aggregates measurements by country, time, and type of test. It highlights "confirmed" cases of blocking when there is strong enough certainty in the test result, but it also publishes anomalies that might be considered false positives.

The OONI team also work to release comparative analysis and real-time alerts for significant internet censorship related events. This would include events such as a sudden surge in social media blockage, or a complete drop off of internet traffic in certain areas. The OONI Mesaurement Aggregation Toolkit (MAT) can be used to visualize these events and potentially identify emerging trends.

3.2 Data Collection

Ireland

To collect network data in Ireland, the OONI CLI was installed on a MacBook Air M2 located in Ireland. The OONI probe was installed based on the CLI instructions found on the OONI website (62). The OONI probe by default does not run automatic tests on the Mac version of the CLI, and this was manually enabled during the installation process. All tests run in Ireland were using the providers HEAnet CLG (AS1213), and Liberty Global B.V. (AS6830).

Iraq

To collect network data in Iraq, a Virtual Machine was set up using the provider *LightNode* (63) on a cloud server located in Baghdad. The cloud server was running Linux Ubuntu version ...PUT VERSION HERE...The OONI probe was installed using the CLI instructions available on the OONI website (62). By default, the OONI probe runs censorship tests in the background once per day, and saves that data in a specific directory, as well as publishes the data publicly. All tests run in Iraq were using the provider Kaopu Cloud HK Limited (AS138915)

Overlapping Information

In addition to these automated tests, manual tests were conducted once per day to collect data. The OONI CLI user guide provided the specific commands to carry out these tests as well as how to run tests on specific files or test sets (64). The first and second day of data collection period used the comprehensive OONI test suite, which ran every test available, including 2200 websites. This broad test suite was used to identify blocked websites that could be added to a smaller test set of websites.

Following the initial testing, a set of 127 websites was collected. This test set included blocked websites from the broad OONI test set, some websites from the most known

blocked websites worldwide (65), the top 50 most visited websites in Ireland (66), and the top 50 most visited websites in Iraq (67). This test set was used in both countries for a span of 9 days.

Each website on the list was put into a category. The number of websites in each category can be found in the table below.

Table 3.1: Number of Websites in Each Category

Category	**Number of Websites**
Uncategorized	30
Piracy / Streaming / File Sharing	20
News / Media	20
Adult Content	20
Creative / Educational / Misc	15
General / National Services	9
Streaming / Social Media	9
Religious	4
VoIP / Communication	2
Gambling	2
Email/Privacy Tools	2
Adult / Alcohol	2
LGBTQ+	1
AI / Technology	1

To parse the OONI data, a python script was written that took in the raw bash/cmd output and organized the results of the test into a neatly formatted CSV file. This made data analysis much easier to complete. Each of the four main tests were recorded as raw bash/cmd output and parsed into CSV files for analysis. All results and OONI links are available on this project's public GitHub Repository, which can be found in the appendix of this report.

3.3 Challenges & Limitations

While the OONI probe and its tests give a good baseline of what internet censorship looks like in a country, it may be difficult to draw definitive conclusions based off of these tests alone. The list of websites used in this work, while tailored to fit these two

countries, still has massive gaps, and may not show the entire picture of what content is blocked in each country. As of 2024 there are about 200 million active websites on the internet (68). Testing every single one in both countries would provide a much more comprehensive view and potentially more concrete results, but this approach is not practical. Therefore, this work is limited in its actual data collection, but with the aid of past data and known censorship environments, conclusions can still be reached.

4 Results and Discussion

The data and discussion of results below come in a combination of data gathered using the OONI probe in Ireland and Iraq, as well as published OONI data from the OONI Measurement Aggregation Toolkit (MAT).

4.1 Test Results

4.1.1 Website Accessibility Results

Collected Data

The first part of this section is an analysis of the data collected by the OONI probe locally in Ireland and through the VM in Iraq.

The results below are an average of the number of websites blocked each day over the testing period of 9 days.

Table 4.1: Summary of Blocked vs. Unblocked Websites by Country

Country	Unblocked	Blocked
Ireland	105	32
Iraq	108	29

Table 4.2 shows the distribution of blocking methods in Ireland and Iraq.

Table 4.2: Distribution of Blocking Methods Detected in Iraq and Ireland

Blocking Method	Iraq Frequency	Ireland Frequency
TCP/IP	18	15
DNS	1	6
HTTP	3	1
Error/Failure	8	5

The table below shows the number of websites blocked in each category in both countries.

Table 4.3: Blocked Websites by Category and Country

Category	Total Websites Tested	Ireland	Iraq
Uncategorized	30	12	10
Piracy / Streaming / File Sharing	20	10	4
News / Media	20	2	2
Adult Content	20	0	0
Creative / Educational / Misc	15	0	0
General / National Services	9	1	2
Streaming / Social Media	9	1	1
Religious	4	2	3
VoIP / Communication	2	1	1
Gambling	2	2	2
Email/Privacy Tools	2	0	1
Adult / Alcohol	2	0	2
LGBTQ+	1	1	1
AI / Technology	1	0	0

Public OONI Data

This section is an analysis of publicly available OONI data over the previous 30 day period in Ireland and Iraq. The data in table 4.5 is the average over the 30-day period.

Table 4.4: Website Blocking based on Public OONI Data

	Ireland	**Iraq**
Number of Websites Tested	1695	3703
Number of Successful Connections	1628	3353
Number of Anomalies	43	262
Number of Failures	24	88
Percentage of Total Blocked	2.5%	7%

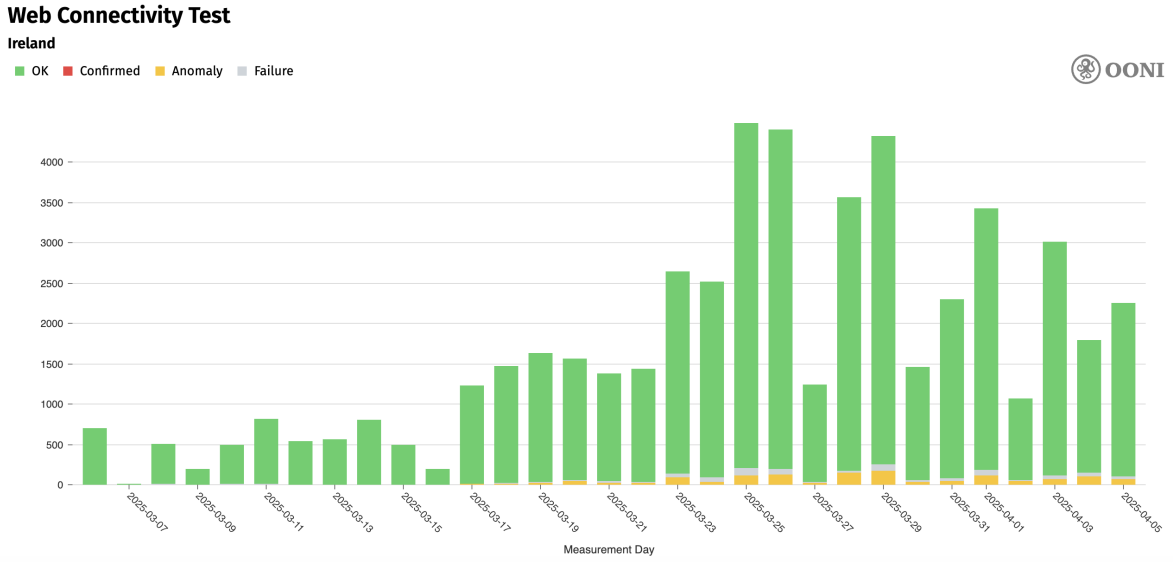

Figure 4.1: Ireland Web Connectivity Test: March 6, 2025 – April 6, 2025

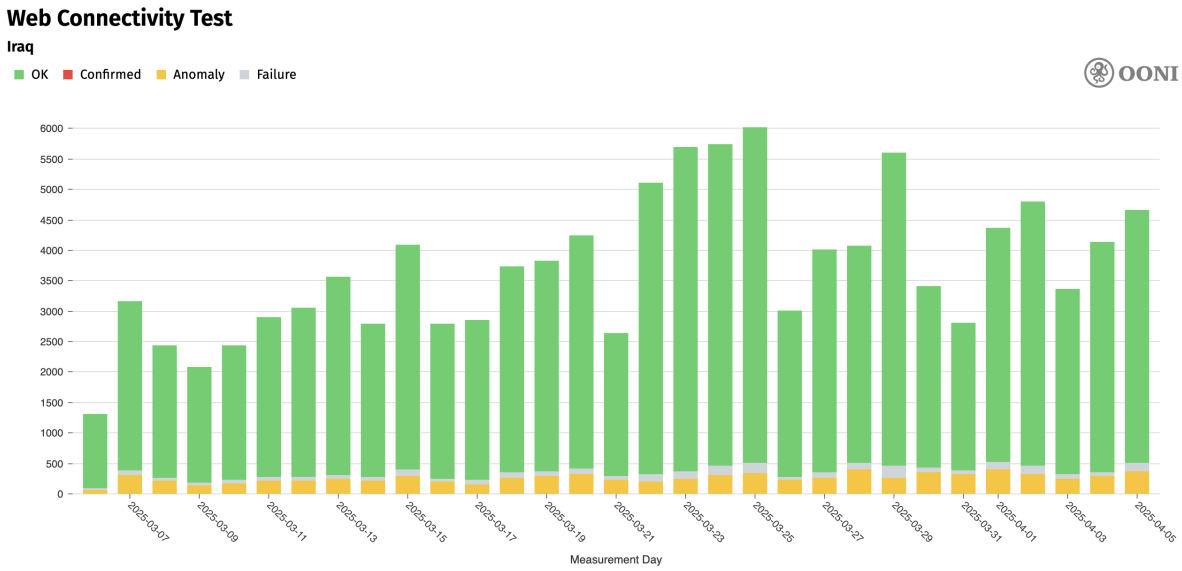

Figure 4.2: Iraq Web Connectivity Test: March 6, 2025 – April 6, 2025

4.1.2 Circumvention Test Results

Ireland

Ireland likely does not block Tor on any of its ASNs, as it is largely accessible outside of 2 anomalies.

March 18, 2025 - Magnet Networks Limited (AS34245) - Tor Test (1 anomaly out of 78 measurements)

March 31, 2025 - Liberty Global B.V. (AS6830) - Tor Test (1 anomaly out of 191 measurements)

Outside of these two anomalies, there is no evidence that Tor is being blocked in Ireland.

Psiphon on the other hand yielded different results. While Psiphon was largely able to be accessed on most ASNs, there were a few where access is likely blocked.

Table 4.5: ASN's with Evidence of Psiphon being Blocked in Ireland

ASN	Anomaly	Total Measurement Count	Percentage
AS1213	33	35	94%
AS6830	16	215	7.4%
AS8075	1	1	100%
AS13280	8	12	66%
AS15751	1	9	11%
Totals	60	494	12.1%

Iraq

Similar to Ireland, Iraq largely does not block access to Tor outside of a few outliers.

March 20, 2025 - Super Cell Network for Internet Services LTD (AS209193) - Tor Test (1 anomaly out of 92 measurements)

March 30, 2025 - Hulum Almustakbal Company for Communication Engineering and Services Ltd (AS203214) - Tor Test (2 anomalies out of 160 measurements)

March 30, 2025 - Valin Company for General Trading and Communications LTD (AS205254) - Tor Test (1 anomaly out of 17 measurements)

Outside of these anomalies, there is no significant evidence that Tor is being blocked in Iraq.

There is also little evidence of Psiphon being blocked in Iraq at a significant scale. Aside of a few outliers, Psiphon only seemed to be blocked on one ASN.

Table 4.6: ASN's with Evidence of Psiphon being Blocked in Iraq

ASN	Anomaly	Total Measurement Count	Percentage
AS203214	127	165	77%
AS51684	4	23	17%
AS199739	1	352	0.2%
AS205254	1	30	3.3%
AS208324	1	3	33%
Totals	134	1107	12.1%

Based on this data, Psiphon is widely accessible in Iraq outside of AS203214.

4.1.3 Instant Messaging Test Results

The results of the Instant Messaging tests were very similar in Ireland and Iraq. Both tests showed no signs of interference or blocking of Facebook Messenger, Telegram, Whatsapp, or Signal. However, looking outside of the tested ASNs reveals a significant difference between the two countries. The tested data in Ireand is consistent with public OONI data, and shows no blocking of instant messaging platforms. The Iraq data is also consistent with tests run on the same ASN, but in Iraq there are other ASNs that show signs of blocking.

Ireland

In the past 30-day period, there were only 2 anomalies found that shows any kind of instant messaging blocking:

March 24, 2025 - Packethub S.A. (AS136787) - Facebook Messenger Test (1 anomaly out of 3 measurements)

March 24, 2025 - HEAnetCLG (AS1213) - Signal Test (1 anomaly out of 37 measurements)

Outside of these anomalies, there was no evidence of instant messaging blocking.

Iraq

Iraq had significant evidence of instant messaging platforms being blocked in certain ASNs. The table below shows each ASN, and the percentage of tests where there was an anomaly found.

Table 4.7: ASN's with Evidence of Instant Message Platform Blocking in Iraq

ASN	Facebook	Telegram	WhatsApp	Signal
AS203214	27%	7.8%	25%	44%
AS205254	26%	3.8%	7.6%	7.6%
AS199739	1%	0.5%	0.2%	0.8%
AS13335	47%	0%	0%	0%
AS50710	33%	0%	0%	0%
AS206206	60%	0%	0%	0%
AS212330	100%	0%	0%	0%
AS210022	0%	0%	0%	82%
AS51020	0%	0%	0%	32%
AS202651	0%	0%	0%	23%
AS59588	0%	0%	1.9%	1.9%
AS209193	0%	0%	0.7%	0%
Total Percentage Blocked	6.2%	1.4%	4.1%	6.2%

Instant Messaging platforms are essentially widely available in Iraq, but there are some areas where blocking does occur.

4.1.4 Middlebox Test Results

The results of the Middlebox Test were the same for both countries. Both the HTTP Header Field Manipulation and HTTP Invalid Request Line tests resulted in no

Middleboxes being detected in either country. However, while there was no evidence of Middleboxes being found using the providers tested, it is possible that other providers in both countries have Middleboxes present in the network.

Using publicly available OONI data for Ireland and Iraq, it was found that there were cases of Middleboxes being detected in both countries over the past 30 days (March 6, 2025 - April 6, 2025).

Ireland

There is very little evidence of Middleboxes being present in Ireland. Over the past 30-day period, there are only two anomalies present. Both of these anomalies are from the HTTP Invalid Request Line test.

March 25, 2025 - Meteor Mobile Communications Ireland (AS15751) (1 anomaly out of 9 measurements)

April 1, 2025 - Vodafone Ireland Limited (AS15502) (1 anomaly out of 79 measurements)

These results are likely outliers, as there are very little Middlebox tests for Meteor Mobile Communications Ireland in this time span and no other anomalies for Vodafone Ireland Limited.

Iraq

There is considerably more evidence of Middleboxes being present in Iraq. Over the past 30 day period, there were 125 anomalies in the HTTP Invalid request line Test and 19 anomalies in the HTTP Header Field Manipulation Test.

The table below lists the ASNs that were suspected to have Middleboxes present using the HTTP Invalid Request Line test. It then shows the number of anomalies, the total measurement count, and what percentage of the total count were anomalies. Note that any ASN that had less than 0.5% anomalies was ignored.

Table 4.8: ASN's with Evidence of Middleboxes (HTTP Invalid Request Line Test) in Iraq

ASN	Anomaly	Total Measurement Count	Percentage
AS198589	68	70	97%
AS203214	32	158	20.25%
AS59588	13	53	24.5%
AS13335	8	10	80%
AS48492	2	4	50%
AS50710	1	1	100%
Total Percentage	125	1071	11.6%

The table below lists the ASNs that were suspected to have Middleboxes present using the HTTP Header Field Manipulation test. It then shows the number of anomalies, the total measurement count, and what percentage of the total count were anomalies. Note that any ASN that had less than 0.5% anomalies was ignored.

Table 4.9: ASN's with Evidence of Middleboxes (HTTP Header Field Manipulation Test) in Iraq

ASN	Anomaly	Total Measurement Count	Percentage
AS13335	8	10	80%
AS48492	2	4	50%
AS50710	1	1	100%
Total Percentage	19	1074	1.7%

Note: All CSV files gathered from the public OONI database can be found on the public GitHub for this work; see Appendix A1.2.

4.2 Comparative Analysis: Ireland v. Iraq

The combined results of OONI probe testing and public OONI data reveal differences in censorship between Ireland and Iraq. While both countries implement content restrictions and other blocks, there are significant differences in the scale and motivations behind these blocks.

Website Accessability

(waiting on some final data from OONI)

Circumvention Tools

The accessibility of Tor and Psiphon were largely the same in Ireland and Iraq outside of a few exceptions. Tor was widely accessible in both countries, indicating that both Ireland and Iraq have no significant mechanisms in place to block this tool, and if they do there is no evidence that it is effective. There is evidence that Psiphon is blocked on specific ASNs in both countries, with public OONI data backing this up. Over the same 30-day period, both Ireland and Iraq blocked Psiphon 12.1% of the time. As a result, there is little evidence that there are systemic efforts to block access to Psiphon, similar to Tor.

Instant Messaging Platforms

In Ireland, there is essentially no evidence that instant messaging services are blocked in any meaningful manner. This is inline with Ireland's stance on censorship, and was expected. In Iraq however, there is some evidence that instant messaging services are blocked in some areas, but according to public OONI data they are widely accessible. There are ASNs that had implemented blocks on all four services tested to some capacity, which can indication regional blocking in response to certain events. This is aligned with Iraq's more reactionary censoring practice.

Presence of Middleboxes

The use of Middleboxes was almost non-existant, as there were only two anomalies over the 30-day time period, which were likely false-positives. This data indicates that Ireland does not implement TLS or SNI-based filtering in any systematic or widespread manner. By contrast, Iraq showed significant evidence of Middleboxes being present. AS198589 showed significant signs of Middleboxes being present, and there are other ASNs with significant anomalies. This indicates that Iraq may

implmelent TLS or SNI-based filtering in some areas of the country, which makes sense as we know that much of Iraq's current censorship efforts are decentralized.

4.2.1 Summary of Comparative Observations

Table 4.10: Comparative Summary of Internet Censorship: Ireland vs. Iraq

Metric	**Ireland**	**Iraq**
Block Rate (OONI)	2.5%	7%
Blocking Methods	–	–
Tool Blocking	Rare, selective	Targeted, ASN-specific
Messaging Blocking	Negligible	Present on some ASNs
Middleboxes Detected	Minimal	Present on some ASNs
Motivations	Legal, EU compliance	Political, cultural control

These findings support the initial research, showing that Ireland and Iraq have quite different approaches to censorship. Ireland maintains a limited, legal-centric censorship model, which is transparent and aligned with most other Western nations. Iraq's approach, while less centralized, is more reactive and inconsistent, with it often being tied to internal events.

5 | Security and Privacy

The following section contains information regarding the privacy and security concerns associated with the completion of the dissertation. This was completed in conjunction with an assignment given in the CSU44302 Security and Privacy module. In writing a dissertation, it is crucial to consider the potential impacts of the research. This document discusses the security and privacy concerns associated with researching internet censorship.

This section addresses security and privacy concerns involved with operating the OONI probe in relation to this work while considering both the technical aspects and the broader legal or regulatory aspects. The comparison of censorship between Ireland and Iraq is significant. While using the OONI probe within both countries comes with its own risk, the use of the probe in Iraq carries much more concern when it comes to security and privacy. The environment in Iraq is significantly more dangerous with ongoing government surveillance, frequent shutting down of social media sites, and the risk of authorities considering unauthorized data-gathering activities as suspicious. All these factors indicate the need to carefully plan where, how, and why measurements are taken, as well as how resulting data will be stored.

5.1 OONI

Although OONI strives to minimize the collection of personal data, its measurements are published openly, which may inadvertently disclose approximate locations and

times when tests occurred (69). If the individual running OONI is tied to a VM in Iraq with an IP address, local authorities or ISPs might link test activity back to the source. This risk is particularly heightened if the probe is frequently connecting to or testing politically sensitive, banned, or controversial websites. In a high-censorship environment, repeated network tests can attract attention and might be interpreted as an intentional challenge to government policies.

(Chris paragraph below)

Their positive track record is emphasized by the claim: "To our knowledge, no OONI Probe user has ever faced consequences as a result of using our software."(**?**). The success of OONI is critically dependent on users conducting tests without repercussions. However, OONI outlines several scenarios in which running their probe may be unwise. This includes users residing in countries with a history of prosecuting similar activities, surveillance concerns, or legal restrictions on accessing content. Users who fall into one or more of these categories should be wary of the potential risks. In this context, operating in Ireland with no reason to believe I am under surveillance, I am considered a low-risk user.

5.2 Iraq Virtual Machine

When deploying a VM in Iraq, the potential security and privacy risk increases due to the possibility that authorities or other outside sources might attempt to compromise the server. The government of Iraq might be motivated to confiscate or check the contents of the VM in order to identify individuals who are actively monitoring sensitive network interference. It is also possible that the hosting provider itself can be forced to give logs, user connections, or site testing targets, which removes all privacy the user has. To avoid this, one should ensure that no personal data is used on this VM, and tools for circumvention are used to encrypt the origin of the user accessing the VM.

Even beyond direct government intervention, there is the risk of third-party hacks or

malware injection. A public and well known measurement platform like OONI will attract hackers looking to disrupt users of this tool or introduce malware that will capture all incoming and outgoing traffic. In Iraq, the network infrastructure might already contain middleboxes or deep packet inspection systems that are actively filtering or manipulating data. These devices sometimes disrupt the traffic generated by the OONI probe measurements, leading to manipulated data to be collected.

6 | Conclusions

This work set out to research and compare internet censorship practices in Ireland and Iraq. These two nations have significantly different governments and cultures. By using both direct network testing using the OONI Probe and published OONI data, this work has identified the distinct methods and motivations behind censorship in each country.

Ireland as a member of the European Union implements a limited and legally rooted censorship model. Ireland mainly blocks illegal and pirated content, and these blocks are implemented through the country's legal system or through EU compliance. The OONI data shows that there is little evidence of widespread censorship of non-illegal content, no use of advanced censorship methods like TLS / SNI-based filtering, and no efforts to block circumvention tools.

Iraq implements a more decentralized and reactionary censorship model, where a wider range of content is blocked when compared to Ireland. The Iraqi government is known to shut off internet access in parts of the country during times of unrest or national exams. The OONI data shows that there is evidence TLS/ SNI-based filters in specific parts of the country, but there is no evidence to support that there is widespread implementation of these advanced mechanisms. Additionally there is some evidence of some circumvention tools, such as Psiphon, being blocked in some areas, but there is nothing to support widespread efforts to block these tools. These findings point to regional and situational censorship, driven by political or cultural events rather than being rooted in a legal basis.

This comparative analysis contributes to the growing importance of digital rights and government accountability by using empirical data and structured analysis. The importance of projects like OONI allows for people to learn about the presence and nature of internet censorship in their own countries, and gives researchers the ability to identify global trends and document network interference. As the internet continues to grow in importance to civil discourse, education, and access to information, vigilance against censorship becomes foundational.

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] Jonathan L Zittrain, Robert Faris, Helmi Noman, Justin Clark, Casey Tilton, and Ryan Morrison-Westphal. The shifting landscape of global internet censorship. *Berkman Klein Center Research Publication*, (2017-4):17–38, 2017.

[7] Information on RFC 9505 &xBB; RFC Editor — rfc-editor.org. https://www.rfc-editor.org/info/rfc9505. [Accessed 15-03-2025].

[8] Mallory Knodel. RFC 9505: A Survey of Worldwide Censorship Techniques — rfc-editor.org. https://www.rfc-editor.org/rfc/rfc9505.html#name-technical-identification,. [Accessed 04-03-2025].

[9] 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].

[10] Encrypt it or lose it: how encrypted SNI works — blog.cloudflare.com. https://blog.cloudflare.com/encrypted-sni/. [Accessed 31-03-2025].

[11] Mallory Knodel. RFC 9505: A Survey of Worldwide Censorship Techniques — rfc-editor.org. https://www.rfc-editor.org/rfc/rfc9505.html#name-transport-layer-security-tl,. [Accessed 10-03-2025].

[12] Exposing and Circumventing China's Censorship of ESNI — gfw.report. https://gfw.report/blog/gfw_esni_blocking/en/. [Accessed 31-03-2025].

[13] The use of TLS in Censorship Circumvention - NDSS Symposium — ndss-symposium.org. https://www.ndss-symposium.org/ndss-paper/the-use-of-tls-in-censorship-circumvention/. [Accessed 31-03-2025].

[14] Carolyn Tackett Méabh Maguire Zach Rosson, Felicia Anthonio. Lives on hold: internet shutdowns in 2024 - Access Now — accessnow.org. https://www.accessnow.org/internet-shutdowns-2024/. [Accessed 15-03-2025].

[15] 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].

[16] 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].

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

[18] 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].

[19] 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].

[20] 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].

[21] Citizens Information. How eu law works, 2025. URL https://www.citizensinformation.ie/en/government-in-ireland/european-government/eu-law/how-eu-law-works/#4022f6.

[22] European Union. How eu policy is decided, 2025. URL https://european-union.europa.eu/institutions-law-budget/law/how-eu-policy-decided_en.

[23] GDPR-Info. General data protection regulation (gdpr), 2025. URL https://gdpr-info.eu/.

[24] Trade Department of Enterprise and Employment. Digital services act, 2025. URL https://enterprise.gov.ie/en/what-we-do/the-business-environment/digital-single-market/eu-digital-single-market-aspects/digital-services-act/.

[25] Irish Statute Book. Act 2 of 2024 (enacted), 2024. URL https://www.irishstatutebook.ie/eli/2024/act/2/enacted/en/html.

[26] Trade Department of Enterprise and Employment. Summary of articles of directive (eu) 2019/790, 2019. URL https://enterprise.gov.ie/en/consultations/consultations-files/summary-articles-of-directive-eu-2019-790.pdf. Accessed: 2025-03-28.

[27] Court of Justice of the European Union. Google spain sl v. agencia española de protección de datos (2014), 2014. URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131.

[28] European Union. Directive (eu) 2019/790 on copyright in the digital single market, 2019. URL https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790.

[29] European Data Protection Board. €2.6 billion euro fine for facebook due to gdpr breach, 2023. URL https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en.

[30] Statista. Meta fines from eu and dpc, 2023. URL https://www.statista.com/statistics/1192794/meta-fines-from-eu-and-dpc/.

[31] European Commission. Eu digital services act: Twitter under scrutiny, 2023. URL https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709.

[32] Business Human Rights Resource Centre. Eu: Twitter could face legal consequences if it fails to comply with eu regulations, 2023. URL https://www.business-humanrights.org/en/latest-news/eu-twitter-could-face-legal-consequences-if-it-fails-to-comply-with-eu-regulatio

[33] Iraq Information Controls Update: Analyzing Internet Filtering and Mobile Apps — citizenlab.ca. https://citizenlab.ca/2014/07/iraq-information-controls-update-analyzing-internet-filtering-mobile-apps/. [Accessed 31-03-2025].

[34] The Role of Government in Telecommunication &x2013; National Investment Commission — investpromo.gov.iq. https://investpromo.gov.iq/?page_id=1526. [Accessed 10-03-2025].

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

[36] Violence & internet shutdowns in 2023: the worst year on record - Access Now — accessnow.org. https://www.accessnow.org/press-release/keepiton-internet-shutdowns-2023/#:~:text=By%20almost%20every%20measure%2C%202023,rights%20of%20millions%20of%20people. [Accessed 15-03-2025].

[37] Exam-ining recent Internet shutdowns in Syria, Iraq, and Algeria — blog.cloudflare.com. https://blog.cloudflare.com/en-us/syria-iraq-algeria-exam-internet-shutdown/. [Accessed 31-03-2025].

[38] Yasmina Zein. Google's DNS Ban in Iraq Restricts Internet Freedom - SMEX — smex.org. https://smex.org/googles-dns-ban-in-iraq-restricts-internet-freedom/. [Accessed 31-03-2025].

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

[40] 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.

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

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

[43] How does a VPN work? — tomsguide.com. https://www.tomsguide.com/features/how-does-a-vpn-work. [Accessed 05-03-2025].

[44] Eircom to block Pirate Bay access — irishexaminer.com. https://www.irishexaminer.com/news/arid-30423241.html. [Accessed 01-04-2025].

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

[46] Web Connectivity — ooni.org. https://ooni.org/nettest/web-connectivity/,. [Accessed 02-03-2025].

[47] Psiphon — ooni.org. https://ooni.org/nettest/psiphon/,. [Accessed 02-03-2025].

[48] spec/nettests/ts-015-psiphon.md at master · ooni/spec — github.com. https://github.com/ooni/spec/blob/master/nettests/ts-015-psiphon.md. [Accessed 02-03-2025].

[49] Tor — ooni.org. https://ooni.org/nettest/tor/,. [Accessed 02-03-2025].

[50] spec/nettests/ts-023-tor.md at master · ooni/spec — github.com. https://github.com/ooni/spec/blob/master/nettests/ts-023-tor.md,. [Accessed 02-03-2025].

[51] spec/nettests/ts-026-riseupvpn.md at master · ooni/spec — github.com. https://github.com/ooni/spec/blob/master/nettests/ts-026-riseupvpn.md. [Accessed 02-03-2025].

[52] LEAP Encryption Access Project — leap.se. https://leap.se/. [Accessed 02-03-2025].

[53] WhatsApp test — ooni.org. https://ooni.org/nettest/whatsapp/,. [Accessed 02-03-2025].

[54] spec/nettests/ts-018-whatsapp.md at master · ooni/spec — github.com. https://github.com/ooni/spec/blob/master/nettests/ts-018-whatsapp.md. [Accessed 02-03-2025].

[55] Facebook Messenger test — ooni.org. https://ooni.org/nettest/facebook-messenger/,. [Accessed 02-03-2025].

[56] spec/nettests/ts-019-facebook-messenger.md at master · ooni/spec — github.com. https://github.com/ooni/spec/blob/master/nettests/ts-019-facebook-messenger.md. [Accessed 02-03-2025].

[57] spec/nettests/ts-020-telegram.md at master · ooni/spec — github.com. https://github.com/ooni/spec/blob/master/nettests/ts-020-telegram.md. [Accessed 02-03-2025].

[58] Signal test — ooni.org. https://ooni.org/nettest/signal,. [Accessed 02-03-2025].

[59] spec/nettests/ts-029-signal.md at master · ooni/spec — github.com. https://github.com/ooni/spec/blob/master/nettests/ts-029-signal.md. [Accessed 02-03-2025].

[60] HTTP Header Field Manipulation — ooni.org. https://ooni.org/nettest/http-header-field-manipulation/,. [Accessed 02-03-2025].

[61] HTTP Invalid Request Line — ooni.org. https://ooni.org/nettest/http-invalid-request-line/,. [Accessed 02-03-2025].

[62] ://ooni.org/install/cli/ubuntu-debian/. [Accessed 24-03-2025].

[63] LightNode - Global NVMe SSD VPS Hosting in Over 40+ Locations — lightnode.com. https://www.lightnode.com/. [Accessed 24-03-2025].

[64] User Guide: OONI Probe Command Line Interface (CLI) — ooni.org. https://ooni.org/support/ooni-probe-cli/,. [Accessed 02-04-2025].

[65] Blocksite. The Most Blocked Websites of 2023 | BlockSite — blocksite.co. https://blocksite.co/blog/digital-mindfulness/most-blocked-sites. [Accessed 29-03-2025].

[66] Top Websites Ranking In Ireland In February 2025 | Similarweb — similarweb.com. https://www.similarweb.com/top-websites/ireland/,. [Accessed 29-03-2025].

[67] Most Visited Websites in Iraq 2025 | Open .Trends — semrush.com. https://www.semrush.com/trending-websites/iq/all,. [Accessed 29-03-2025].

[68] Matt. How Many Websites Are There? — digitalsilk.com. https://www.digitalsilk.com/digital-trends/how-many-websites-are-there/. [Accessed 05-04-2025].

[69] | OONI — ooni.org. https://ooni.org/about/risks/,. [Accessed 14-03-2025].

A1 Appendix

To aid in the writing of this work, additional tools were used to ensure clarity, presentation, correctness, and structure.

ChatGPT ChatGPT was used to assist in structuring the content of this thesis, and in the naming of chapters and sections. It was also used to help generate tables in Latex, and check for spelling and grammar mistakes. ChatGPT also assisted in parsing data collected by the OONI Probe.

Grammarly Grammarly was used to check for spelling and grammar mistakes throughout the entire thesis.

Overleaf Overleaf was used to write and generate the final thesis.

GitHub GitHub was used to store all data related to this project. The public link to this GitHub is `https://github.com/ccasey300/censorship_project`.

This work was completed alongside Chris Casey, and some sections of this report were authored by him. These sections include, 1.3.3 and 2.3.3.

A1.1 List of Websites

The list of websites used to test the OONI probe in Ireland and Iraq can be found at the following link on this project's public GibHub: `https://github.com/ccasey300/censorship_project/blob/main/Griff/Files/WebsitesLive.txt`

A1.2 OONI Data

All OONI data collected during this work can be found at the following link on this project's public GitHub: `https://github.com/ccasey300/censorship_project/tree/main/Griff/OONIData`

A1.3 OONI Data Parsing File

The python script used to parse the OONI data into CSV files can be found at the following link on this project's public GitHub: `https://github.com/ccasey300/censorship_project/blob/main/Griff/Files/OONIDataParse.py`