Internet Censorship Capabilities in Cyprus: An Investigation of Online Gambling Blocklisting

Vasilis Ververis[1,5](✉), Marios Isaakidis[2], Chrystalleni Loizidou[3], and Benjamin Fabian[4]

[1] Humboldt University, Berlin, Germany
ververis@kth.se
[2] University College London, London, UK
[3] University of Nicosia, Nicosia, Cyprus
[4] Hochschule für Telekommunikation, Leipzig, Germany
[5] Universidade Estadual do Piauí, Teresina, Brazil

Abstract. This paper presents the initial findings of an open and collective effort towards a cross comparison study of web-content blocking regulations and practices, in different parts of Cyprus. Our analysis is based on network measurement data collected by volunteers in Cyprus, using a custom OONI probe and open DNS resolvers, from five residential ISPs; Callsat (AS 24672), Cablenet (AS 35432), Cyta (AS 6866), MTN (AS 15805) and Multimax (AS 197792). We were able to identify a number of unreported Internet censorship cases, non-transparently implemented blocking regulations, and collateral damage due to blocking of email delivery to the regulated domains by the National Betting Authority of the Republic of Cyprus. These results indicate the presence of at least two distinct regimes on the island.

Keywords: Internet censorship · Cyprus · Internet policy · Network measurements · Blocklists · Network filtering · Freedom of expression · Information policy

1 Introduction

This paper describes the initial findings of an open and collective effort to gather data, using OONI (Open Observatory of Network Interference) and open DNS (Domain Name System) resolvers in Cyprus, towards a cross comparison study of web content blocking regulations and practices between Cyprus and other countries in terms of implementation techniques. We suggest there is a need for a closer study of how censorship (the blocking of content, the top-down imposition of restrictions on information) is legislated and justified in political terms on the one hand, and on the other hand the actual extent and the procedural technicalities of its implementation as experienced by the citizen, in this case the Internet user or the ISP (Internet Service Provider) client. This investigation

S.K. Katsikas and V. Zorkadis (Eds.): E-Democracy 2017, CCIS 792, pp. 136–149, 2017.
https://doi.org/10.1007/978-3-319-71117-1_10

of *how* blocking is legislated and implemented on a local level contributes to discussions around transparency, accountability, and freedom of expression more broadly. The island of Cyprus presents an interesting geopolitical case study because it allows for the collection of data on what we have come to think of as more than two distinct regimes in terms of information policy: the one followed in the RoC (Republic of Cyprus) in the south of the island, which largely adopts EU (European Union) policy, and the one followed in the area occupied by Turkey in the north of the island. The landscape regarding policy over Internet blocking may prove to be even more complex, considering the existence of two British sovereign military bases on the island, although our study does not yet include data from these areas. Our initial measurements are biased towards Internet blocking by ISPs following RoC protocols, with fewer observations revealing the policy of Internet blocking in the north (only one north Cyprus ISP, Multimax, is measured).

Our intention is to gather data on the capabilities of ISPs to perform censorship, or more specifically their capabilities to block access to specific information in Cyprus, and to provide comparable data about how the application of technologies for censorship, or control over information, is developing internationally.

The rest of the article is structured as follows. First we introduce the case of Cyprus and the specific legal circumstances around online gambling that allow us to investigate Internet blocking on the level of the ISP. We then briefly indicate similar research done in other countries, and present our methodology, the infrastructure and the tools we used. Following, we provide an analysis of the collected data set per blocking method and ISP and analyze the blocklist used to conduct blocking, its effects and collateral damage. We conclude with an outlook on how this kind of research might be used in the future.

2 The Case of Cyprus

For the case of Cyprus we collected measurements from end-user connections located on various ISPs on both sides of the island. Cyprus has a population of 1,1 million. In comparison to other countries, access to Internet services is very good, as shown by the 2016 statistics of the ITU information society report: 71.2% penetration of Internet access in Cyprus. The share of fixed-broadband subscriptions of residents lies at 22.3%, with an additional 54.8% having active mobile broadband subscriptions. The average Internet bandwidth per Internet user is measured at 89,791 Bit/s in 2016 [36]. This gives us a better understanding about user experience and allows for evaluating how each ISP has implemented the updated betting act directives. We investigate the extent to which ISPs may have over-blocked or under-blocked any entries included or deduced in the blocklist, and we analyze any collateral damages to unregulated websites. In recent years, ISPs in the RoC have implemented an Internet filtering infrastructure to comply with the laws and regulations imposed by the National Betting Authority (NBA). Our starting point was to find out how the technical infrastructure to block or filter unregulated web resources (the ones implied by the NBA) has taken place and discover cases of under or over blocking and to find collateral damage caused by blocking Internet resources that were not meant to be blocked (such as email).

3 Previous Research

The RoC is considered a safe haven for freedom of speech. It is important to note that Freedom House reports that mention and catalog Internet censorship related events in the years 2006 [27], 2007 [28], 2008 [29], 2011 [30], 2012 [31], 2013 [32], 2014 [33] document that citizens are able to access the Internet on a regular basis and are not subject to any known government restrictions, although they do report a difference between the years 2012 and 2013. However, Freedom House numerical rating reports for Cyprus are based on conditions on the south of the island only. Worth mentioning is research on media pluralism that considers risks to freedom of expression and right to information in Cyprus as low risk [4]. We have not been able to find any previous work that discusses Internet censorship in Cyprus, and there has been no attempt to compare information across the island's divisions.

This case study on Cyprus is related to two previous OONI case studies. In the first instance we refer to previous research on large scale content blocking in Greece [43]. Similarly with the NBA in Cyprus, in Greece this kind of blocking is initiated by the Greek gaming commission (EEEP), an independent administrative authority that acts as the public body, responsible for the control and supervision of gambling services. The Greek case-study analyzed the techniques and policies used to block content of gambling websites in Greece and presented the implications of under-blocking, over-blocking, and collateral damage by blocked email communication. It also highlighted issues of transparency in Internet filtering and unfair competition between ISPs. In the second instance we refer to a case study in Turkey that attempted to track changes to Internet traffic during the coup d'etat of July 2016. The study brings up the technical aspects of potential Internet blocking in Turkey and highlights the importance of a grassroots understanding of ISP blocking capabilities [23].

4 Detecting Network Interference and the Republic of Cyprus Gambling Law of 2012

Identifying signs or conclusive results of network interference that can be caused by Internet filtering or surveillance is a challenging process that requires adequate knowledge of the underlying network infrastructure on the side of the ISPs or their upstream providers. In this article, we focus on censorship by content regulation policies, and particularly the gambling law of 2012, L. 106(I)/2012 [8]. The law implies that the ISPs are obliged to apply a *blocking system* that will prevent users and ISP clients from accessing gambling services providers who are not licensed (do not hold a Class B license) or service providers who possess, operate infrastructure or provide online casino services in Cyprus. According to the NBA, a *blocking system* is defined as:

> A system installed by the Internet service provider which prevents the routing and the movement from the terminal equipment of the Internet user to particular Internet website addresses URL (Uniform Resource Locator).

According to the RoC gamling law of 2012, non compliance is punishable with a term of imprisonment not exceeding five years or a fine not exceeding three hundred thousand Euro or to both such sentences. Upon notification from the NBA, ISPs are obliged to block URLs of gamling services that do not follow regulations within seventy two hours. Although the law does not specify the way in which URLs should be submitted to the ISPs for blocking, the current means seem to be a publicly available blocklist; a file with a list of URL entries named as *Blocking List* [19], located on the official website of the RoC NBA [20].

4.1 Analysis of the Republic of Cyprus NBA Blocklist

NBA publishes a blocklist usually in a text file format that contains a number of URL entries of websites with complete file paths, not just domain names (such as http://m.downloadatoz.com/apps/com.microgenius.casino777,482188.html) that offer non-licensed gamling services in Cyprus. NBA was established in 2012 as an independent authority, consisting of a president and six members. One of the authority's duties is to notify ISPs in an electronic manner on every Internet URL through which gamling services are offered that are not covered by a class A or B licensed bookmaker, or anyone offering services prohibited in the present gamling law [8]. Although the law was issued in 2012, the first public release of the blocklist (that we were able to detect from the online archives) was in February, 2013 [9]. NBA does not provide a blocklist versioning system similar to other countries [43]. We assume 10 blocklist versions from February 2013 to May 2017 [9–18], though we cannot with certainty confirm the existence of additional blocklists in the past. Our findings are derived from Internet archives [1,2] that provide historical snapshots of websites. Starting in February 2013, the NBA publishes a blocklist containing 95 entries of URLs [9] that increases to a total of 2563 (in April 2017) URL entries [18], approximately 27 times more than the initial size of the blocklist. Figure 1 illustrates a timeline with the date and URL entries of the blocklist published by the NBA.

During our analysis of the blocklist, we identified a number of malformed entries (mainly URLs and domain names) such as *1xbet.??* as well as duplicate entries and at least one entry that does not seem to host gambling related content; https://www.commission.bz, an advertisement affiliate program. The malformed URL entries of the blocklist may introduce technical issues to the filtering implementation of the blocklist as URLs that contain malformed characters (such as *??*) may not be parsed correctly. Additionally, a number of domain names in the blocklist were found to be expired or not registered, meaning that these domain names are not hosting any gambling related content (actually not hosting any content since they are not registered) but are still blocked by many ISPs in the Republic of Cyprus.

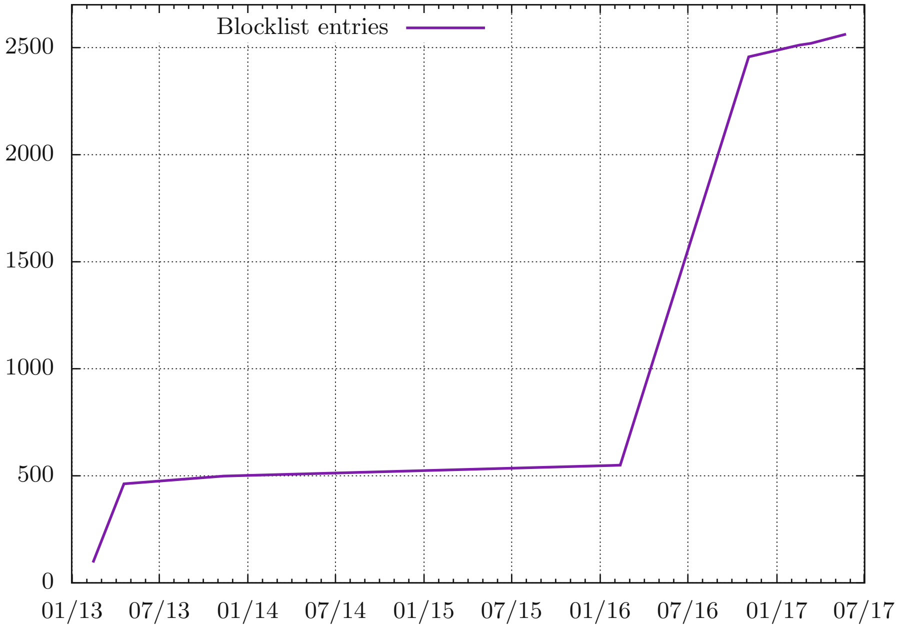


Fig. 1. Timeline of the NBA blocklist publication

The NBA list implies that ISPs should do URL blocking as the entries of the blocklist contain URLs. ISPs would only be able to block them if they had previously deployed a blocking mechanism that would give the technical capability to ISPs to look inside the payload of the network packets, and more specifically at the layer 7 contents where the actual URL of an HTTP request is referenced, that technology is named as a Deep Packet Inspection (DPI). In order to be able to filter HTTPS URLs the ISP needs to intercept the connection between the client (user of the ISP) to the server and perform an active man-in-the-middle attack on every HTTPS connection in order to decrypt the SSL/TLS, layer it and look at the unencrypted payload. Currently the SSL/TLS connections (HTTPS URLs) destined to the ISPs censorship infrastructure are not being handled (port 443 is unreachable). The connection times out and the user is not receiving any notification about the blocking in place apart from a connection error (error: couldn't connect to host).

5 Methodology for Data Collection and Analysis

We are using a variety of common free and open source software networking tools for gathering, categorizing, distributing, analyzing data and comparing the results. Acquiring results from a number of different ISPs is crucial to form a representative sample. We have conducted network measurements and used publicly available data based on OONI reports [41] submitted by volunteers. We were able to collect and process network measurement data from the following residential landlines and cellular ASes (Autonomous Systems): AS15805 (MTN Cyprus Limited), AS24672 (CallSat International Telecommunications Ltd.), AS35432 (Cablenet Communication Systems Ltd.), AS6866 (Cyprus Telecommunications Authority), AS8544 (Primetel) and AS197792 (Multimax Iletisim Limited). Even so, this remains a limited sample and the findings presented here are tentative and preliminary.

5.1 Data Set Used for the Tests

First, we compiled a list of all URLs that are reported to be blocked in Cyprus as published and curated by the RoC NBA [19], the Greek gamling authority's blocklist [7] the Lumen database [35] for Turkey, and the community-collected global test list maintained by Citizenlab [37]. Additionally, we have used the public open DNS servers list provided by Digineo GmbH [25].

5.2 Collection of Network Measurements

The collection of the network measurements took place during the months of March to May 2017, though we were able to process relevant data submitted by volunteers from the months January and February earlier in 2017. Volunteers collected and submitted network measurements by using a custom set of tools and test lists [40] populated from the data sets enumerated in Sect. 5.1. For our censorship research we used ooniprobe, an application developed by the OONI project [24] and used by volunteers and organizations to probe their network for signs of network tampering, surveillance or censorship. Developed with the idea of ensuring the detection of any interference to network communications, it aims to collect and provide high quality reports by using open and transparent data methodologies freely available to anyone that would like to process and analyze.

Ooniprobe is the application that was used to conduct the measurements on the ISP networks (both landline and cellular networks) where we detected network tampering and content blocking. Ooniprobe provides a variety of test cases and classes that could be used to probe the networks. More analytically, in our research we have deployed and analyzed a number of network measurements tests, precisely instant messaging, HTTP header fields manipulation and invalid request line tests, Tor and pluggable transports reachability tests as well as the web connectivity test. We were not able to identify any certain case of network interference in all of the tests apart from the web connectivity test. However this does not necessarily mean that there is no other sort of network interference happening on the network during different date periods or from different vantage points.

Web connectivity is an ooniprobe test methodology where we were able to identify and detect if a website is reachable and the reason or cause in case a website is not reachable. This test reaches a non censored control measurement endpoint (test helper) to assist with the comparison of the measurements for a given website. At first, the test performs an *A* DNS lookup to a special domain name service in our experiments; *whoami.akamai.com* that will respond to the *A* DNS lookup request with the resolver of the probe. Upon DNS resolver identification, the test will perform a DNS lookup querying the *A* record of the default resolver for the hostname of the URL tested. Following the test will try to establish a TCP session on port 80 or port 443 if the URL in question begins with the prefix *http* or *https* accordingly for the list of all IPs returned by the previous DNS query. Finally, the test performs a HTTP GET request for the path specified in the uniform resource identifier using the most widely used web browser user agent; *Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.106 Safari/537.36* [42] as the HTTP header. Upon completion of the test, the gathered data are compared with the ones of the control measurement test helper.

6 Preliminary Findings

We were able to perform measurements on the following ISPs: Cytanet (AS 6866), Cablenet (AS 35432) and Multimax (AS 197792). Additionally, we were able to identify block pages based on reports contributed by volunteers to the OONI data repository [41] on ISPs Callsat (AS 24672) and MTN (AS AS15805).

The most common identified method of content blocking on Cypriot ISPs is DNS hijacking. Since ISPs are in control of the DNS servers used by their users in residential broadband or cellular connections, they can manipulate the DNS servers' responses and can redirect the requesting users to anywhere they want. Taking advantage of this privilege, ISPs modify their resolvers to override censored domains' legitimate DNS replies by creating local zone entries [3]. These entries usually point to a server that they control where they run a web server that displays a webpage with the warning message to users or block page.

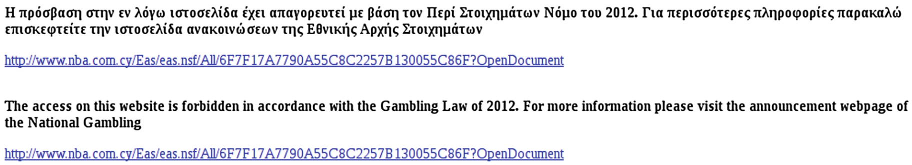
6.1 Differences Between ISPs

All ISPs, with the exception of Multimax in the north of the island, were using DNS hijacking as the blocking to control the access of the entries in NBA's list. Comparing the network measurements from all ISPs we found multiple cases of websites (entries of the blocklist) not being blocked, providing error messages (specifically HTTP status codes 403 and 404) or were unable to connect (connection failed) to HTTPS entries instead of the blocking page or the reason (legislation) why a user cannot access the specific website in question. Additionally, we were able to detect instances where email communication to the specific websites was also blocked although the law does not imply blocking email communication but only restricting access to the website that is included in the blocklist.

Additionally, at least one ISP was found redirecting the user to the website of NBA [20], leaking the IP addresses and possible the web browser's specific user metadata.

6.2 Callsat ISP

Network measurements analyzed from Callsat ISP [6] (AS 24672) on the entries of the NBA blocklist revealed an outdated *landing* block page with a URL that points to a non-existent web resource (HTTP status code 404). The blockpage is illustrated in Fig. 2.



Η πρόσβαση στην εν λόγω ιστοσελίδα έχει απαγορευτεί με βάση τον Περί Στοιχημάτων Νόμο του 2012. Για περισσότερες πληροφορίες παρακαλώ επισκεφτείτε την ιστοσελίδα ανακοινώσεων της Εθνικής Αρχής Στοιχημάτων

http://www.nba.com.cy/Eas/eas.nsf/All/6F7F17A7790A55C8C2257B130055C86F?OpenDocument

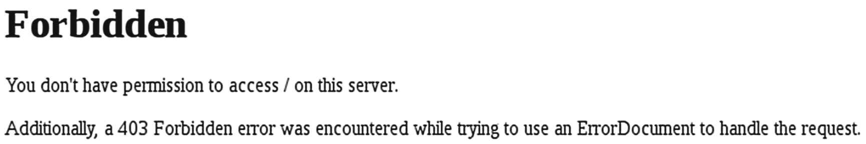
The access on this website is forbidden in accordance with the Gambling Law of 2012. For more information please visit the announcement webpage of the National Gambling

http://www.nba.com.cy/Eas/eas.nsf/All/6F7F17A7790A55C8C2257B130055C86F?OpenDocument

Fig. 2. Callsat ISP NBA regulation landing page

6.3 Cablenet ISP

Our findings from the network measurements reveal that the Cablenet ISP [5] (AS 35432) was directing users trying to access the entries of the blocklist to a generic error webpage (HTTP status code 403) without providing any justification of the blocking. The user may falsely assume that the website in question experiences technical issues. The blockpage is illustrated in Fig. 3.



Forbidden

You don't have permission to access / on this server.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

Fig. 3. Cablenet ISP NBA regulation landing page

6.4 Cyta ISP

Cyta ISP [21] (AS 6866) does not point the users to a blockpage but rather redirects the users trying to access the blocked entries from the blocklist to the NBA website. The excerpt from the HTML markup code is illustrated in Listing 1.1.

```
<!doctype html>
<html class="no-js">
<head>

<meta http-equiv="content-type" content="text/html; charset=
    utf-8">
<meta name="copyright" content="copyright 2013">
<meta name="author" content="Designed & Developed by Cyta">
<meta name="distribution" content="global">
<meta http-equiv="refresh" content="0; url=http://www.nba.gov.
    cy/" />

</head>
</html>
```

Listing 1.1. Cyta ISP's HTML markup landing page

6.5 MTN ISP

Network measurements collected from MTN ISP [38] (AS 15805) on one day (02/04/2017) show no evidence of blocking.

6.6 Multimax ISP

Multimax [39] (AS 197792) is one of the ISPs that operates in the north of Cyprus. We have not identified any block pages, however, upon closer analysis, we found many similarities to the Turkish ISPs and specifically the blocking of web resources using IP blocking. We can conclude that the websites in Table 1 have not been accessible for the period of time during our network measurements. Note that the list of websites in Table 1 is not exhaustive and there could more websites or service that may be potentially blocked by this ISP.

Table 1. Multimax ISP: List of blocked websites

https://www.wikipedia.org
https://www.torproject.org
http://www.islamdoor.com
http://www.fepproject.org
http://www.no-ip.com
https://wikileaks.org
https://psiphon.ca

6.7 Collateral Damage

In our research we identified that the Mail Exchange (MX) records are absent, and do not contain the relevant DNS records that point to the email server of the domain name in question. That is rendering email delivery to the specific domain name impossible.

```
; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> MX williamhill.com @82
    .102.93.140
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19519
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1,
    ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;williamhill.com.          IN   MX

;; AUTHORITY SECTION:
williamhill.com.    3600    IN   SOA ns1.cablenet-as.net. noc.
    wavespeed.net.
1483803163 10800 3600 604800 3600

;; Query time: 97 msec
;; SERVER: 82.102.93.140#53(82.102.93.140)
;; WHEN: Tue Apr 04 02:35:07 CEST 2017
;; MSG SIZE  rcvd: 113
```

Listing 1.2. Empty (no answer) DNS MX records for williamhill.com (dig output)

In the Listing 1.2 we have requested the MX records of the domain name williamhill.com from the DNS server *82.102.93.140* (DNS resolver in Cyprus operated by Cablenet) compared to the Google's DNS resolver *8.8.8.8* as illustrated in Listing 1.3. Google's DNS resolver answered with 2 entries in the query (*ANSWER: 2*) for the domain name in question whereas Cablenet's DNS resolver sent no answers (*ANSWER: 0*). The DNS queries took place on 4 April, 2017.

```
; <<>> DiG 9.9.5-9+deb8u10-Debian <<>> MX williamhill.com @8
    .8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16093
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0,
    ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;williamhill.com.                IN      MX

;; ANSWER SECTION:
williamhill.com.         605     IN      MX      10
mxb-0010e301.gslb.pphosted.com.
williamhill.com.         605     IN      MX      10
mxa-0010e301.gslb.pphosted.com.

;; Query time: 40 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Apr 04 02:43:51 CEST 2017
;; MSG SIZE  rcvd: 116
```

Listing 1.3. Google DNS MX records for williamhill.com (dig output)

6.8 Circumventing Blocking

Using a block-list/allow-list model (sort of an ON/OFF model) is not granular enough and tends to fail; it will have negative impact on users and customers of the ISPs that may or may not find routes around the blocking. Furthermore, creating such an ineffective blocking gives a false sense of security as the entities that enforced such blocking would assume that the content is being blocked although blocking is easily circumvented.

6.9 Using Alternative DNS Resolver

Circumventing the blocking enforced by the ISPs is just a tweak in the network configuration and requires no technical expertise by using a different DNS resolver such as Google DNS [22] (*8.8.8.8*) or OpenDNS [34] (*208.67.222.222*).

7 Conclusions and Future Work

Although this case study initially focused on the blocking of gamling websites specifically, it brings up interesting data regarding more general blocking practices in the north of the island, which need to be further investigated. One example is our finding that the RoC block list isn't blocked in the north of

Cyprus, but that a number of other websites have been blocked there, matching the list of websites blocked in Turkey (see Table 1). This opens up a discussion of more than one regime of freedom of expression on the island, and also raises the question of whether there may be a third point of difference with blocking practices implemented in the British sovereign bases. Furthermore, our intention is to confirm with ISPs regarding the technical infrastructure used to implement blocking.

As explained in the introduction, this is only the beginning of an effort to more closely study how online content-blocking is legislated and implemented, in an effort to understand the political extensions of these practices and their related dangers to internet freedom and freedom of information. For example, beyond issues of content-blocking and connected debates around censorship, the data collected here also implicate issues of privacy and personal data protection (with regard to ISP redirection practices), as well as issues of transparency (with regard to how content-blocking is implemented). We hope that the evidence this research begins to produce will come to feature in further discussion, leading to a better understanding of the dangers as well as alternative and safer technical options. More ambitiously, we hope that this research will promote a more sensitive approach guiding policy and national legal provisions that will more effectively safeguard the aforementioned freedoms.

Acknowledgements. We are grateful to Greg Andreou, observer, Costas Tsangarides, savvas, members of the Lefkoşa Hackerspace, and other anonymous contributors in Cyprus for running the measurement tests and their overall support. This project is an initiative of hack66/observatory [26], a Cyprus-based Internet observatory that aims to collect and analyze data, and routes of data, through Europe, Middle East and Africa in order to promote evidence-based policy making. It has been possible thanks to the long-running efforts of the OONI team.

References

1. Internet Archive. The Wayback Machinve. http://web.archive.org/. Accessed 05 Jun 2015
2. Archive.is. Webpage Capture. http://archive.is. Accessed 04 Jun 2015
3. Atkins, D., Austein, R.: Threat analysis of the domain name system (DNS). http://web.archive.org/web/20140826081656/http://www.ietf.org/rfc/rfc3833.txt. Accessed 26 Aug 2014
4. Christophorou, C.: Cyprus: Media Pluralism Monitor 2015 [European Uni versity Institute, Robert Schuman Centre for Advanced Studies]. https://web.archive.org/web/20170606205318/http://monitor.cmpf.eui.eu/mpm2015/results/cyprus/. Accessed 06 Jun 2017
5. Cablenet. Cablenet ISP official website. http://archive.is/UBxqc. Accessed 05 Jun 2017
6. Callsat. Callsat ISP official website. http://archive.is/CAuFL. Accessed 04 Jun 2015
7. EEEP Greek Gaming Commission. https://www.gamingcommission.gov.gr/images/Anakoinoseis/BlackListVersion4_11072014.pdf. Accessed 11 Jul 2015

8. National Betting Authority of Cyprus. Betting Law 2012. http://web.archive.org/web/20170605132235/http://nba.gov.cy/wp-content/uploads/TheBettingLawof2012.pdf. Accessed 05 Jun 2015
9. National Betting Authority of Cyprus. National Betting Authority of Cyprus Blocklist. 14 February 2013. https://web.archive.org/web/20130217021102/http://blocking.nba.com.cy:80/. Accessed 17 Feb 2013
10. National Betting Authority of Cyprus. National Betting Authority of Cyprus Blocklist, 19 April 2013. https://web.archive.org/web/20130906231633/http://blocking.nba.com.cy:80/. Accessed 06 Sept 2013
11. National Betting Authority of Cyprus. National Betting Authority of Cyprus Blocklist, 12 November 2013. https://web.archive.org/web/20131124123355/http://blocking.nba.com.cy:80/. Accessed 24 Nov 2013
12. National Betting Authority of Cyprus. National Betting Authority of Cyprus Blocklist, 29 January 2016. https://web.archive.org/web/20160201084135/http://blocking.nba.com.cy:80/. Accessed 20 Feb 2016
13. National Betting Authority of Cyprus. National Betting Authority of Cyprus Blocklist, 15 February 2016. https://web.archive.org/web/20160303044805/http://blocking.nba.com.cy:80/. Accessed 03 Mar 2016
14. National Betting Authority of Cyprus. National Betting Authority of Cyprus Blocklist, 4 November 2016. https://web.archive.org/web/20161106114742/http://blocking.nba.com.cy:80/. Accessed 06 Dec 2016
15. National Betting Authority of Cyprus. National Betting Authority of Cyprus Blocklist, 17 February 2016. https://archive.fo/Wdb9n. Accessed 24 Feb 2017
16. National Betting Authority of Cyprus. National Betting Authority of Cyprus Blocklist, 13 March 2017. https://archive.fo/Z7WtK. Accessed 19 Mar 2017
17. National Betting Authority of Cyprus. National Betting Authority of Cyprus Blocklist. As it appeared in Google cache on 27 April 2017 05:09:03 GMT, 27 April 2017
18. National Betting Authority of Cyprus. National Betting Authority of Cyprus Blocklist, 25 May 2017. https://web.archive.org/web/20170526021718/http://blocking.nba.com.cy. Accessed 26 May 2017
19. National Betting Authority of Cyprus. National Betting Authority of Cyprus Blocklist website. https://web.archive.org/web/20170605133936/http://blocking.nba.com.cy. Accessed 05 Jun 2015
20. National Betting Authority of Cyprus. National Betting Authority of Cyprus official website. https://web.archive.org/web/20170605132348/http://nba.gov.cy. Accessed 05 Jun 2015
21. Cyta. Cyta ISP official website. http://archive.is/NBDpH. Accessed 05 Jun 2017
22. Google Developers. Using Google Public DNS. http://web.archive.org/web/20140829223153/https://developers.google.com/speed/public-dns/docs/using. Accessed 29 Aug 2014
23. Aben, E., Evdokimov, L., Xynou, M.: Internet Access Disruption in Turkey (2016). https://web.archive.org/web/20170606190316/http://ooni.torproject.org/post/turkey-internet-access-disruption/. Accessed 06 Jun 2017
24. Filastó, A., Appelbaum, J.: ONI: open observatory of network interference. In: Free and Open Communications on the Internet. USENIX (2012). https://www.usenix.org/system/files/conference/foci12/foci12-final12.pdf
25. Digineo GmbH. Public DNS Server List. https://web.archive.org/web/20170606195759/https://public-dns.info/. Accessed 06 Jun 2017
26. Hack66. Hack66 Observatory. https://web.archive.org/web/20170606204802/http://hack66.info/observatory. Accessed 06 Jun 2017

27. Freedom of House. Freedom of the Press, Cyprus Country report (2006). https://web.archive.org/web/20170605134525/https://freedomhouse.org/report/freedom-press/2006/cyprus. Accessed 05 Jun 2015
28. Freedom of House. Freedom of the Press, Cyprus Country report (2007). https://web.archive.org/web/20170605134610/https://freedomhouse.org/report/freedom-press/2007/cyprus. Accessed 05 Jun 2015
29. Freedom of House. Freedom of the Press, Cyprus Country report (2008). https://web.archive.org/web/20170605134650/https://freedomhouse.org/report/freedom-press/2008/cyprus. Accessed 05 Jun 2015
30. Freedom of House. Freedom of the Press, Cyprus Country report (2011). https://web.archive.org/web/20170605134800/https://freedomhouse.org/report/freedom-press/2011/cyprus. Accessed 05 Jun 2015
31. Freedom of House. Freedom of the Press, Cyprus Country report (2012). https://web.archive.org/web/20170605134838/https://freedomhouse.org/report/freedom-press/2012/cyprus. Accessed 05 Jun 2015
32. Freedom of House. Freedom of the Press, Cyprus Country report (2013). https://web.archive.org/web/20170605134916/https://freedomhouse.org/report/freedom-press/2013/cyprus. Accessed 05 Jun 2015
33. Freedom of House. Freedom of the Press, Cyprus Country report (2014). https://web.archive.org/web/20170605135021/https://freedomhouse.org/report/freedom-press/2014/cyprus. Accessed 05 Jun 2015
34. OpenDNS Inc., OpenDNS IP Addresses. http://web.archive.org/web/20140829223158/http://www.opendns.com/opendns-ip-addresses/. Accessed 29 Sept 2014
35. Berkman Klein Center for Internet and Society at Harvard University, Lumen. http://archive.is/BwyBv. Accessed 05 Jun 2015
36. ITY. I. T. U. 2016. Measuring the Information Society Report. https://web.archive.org/web/20170605134129/http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf. Accessed 05 Jun 2015
37. Citizen Lab and Others. URL testing lists intended for discovering website censorship. https://github.com/citizenlab/test-lists.2014
38. MTN. MTN ISP official website. http://web.archive.org/web/20170605020143/http://www.mtn.com.cy/. Accessed 05 Jun 2017
39. Multimax. Multimax ISP official website. http://web.archive.org/web/20170605015656/http://www.mmcyp.com. Accessed 05 Jun 2017
40. Hack66 Observatory. A custom set of tools to perform ooniprobe network measurements (2017). https://github.com/hack66/bet2512
41. OONI. OONI measurements files repository. https://web.archive.org/web/20170606210652/https://measurements.ooni.torproject.org/. Accessed 06 Jun 2017
42. Statcounter. StatCounter GlobalStats. http://gs.statcounter.com/. Accessed 05 Jun 2015
43. Ververis, V., et al.: Internet censorship policy: the case of Greece. In: Free and Open Communications on the Internet. USENIX (2015). https://www.usenix.org/system/files/conference/foci15/foci15-paper-ververis-updated-2.pdf