Opening Digital Borders Cautiously yet Decisively: Digital Filtering in Saudi Arabia

Fatemah Alharbi
Taibah University, Yanbu

Michalis Faloutsos
University of California, Riverside

Nael Abu-Ghazaleh
University of California, Riverside

Abstract

Our study makes a rare positive observation: Saudi Arabia has been opening its digital borders since 2017 in a deliberate new era towards openness. In this paper, we present a comprehensive longitudinal study of *digital filtering*, which we define to include both mobile apps and website access, in Saudi Arabia over a period of three years. Our results show that Saudi Arabia has indeed made significant progress towards opening its digital borders: (a) the use of mobile applications has been significantly permitted; and (2) web access is becoming more open. We use: (a) 18 social media and communications mobile apps such as WhatsApp, Facetime, and Skype; and (b) Alexa's top 500 websites in 18 different categories. For mobile app access, our mobile app group was completely blocked in 2017, but access was permitted to 67% in 2018, 93% in 2019, and all, except WeChat, in 2020. For web access, we find that Internet filtering decreased by 3.4% and 2.2% in *Adult* and *Shopping*, respectively, which are the most two blocked categories. Finally, we examine how digital filtering reflects the wider geopolitical events, such as the blocking of ISIS-friendly sites in 2020 and news sites from Qatar, Iran, and Turkey in 2017, 2018, and 2020, respectively, due to diplomatic tensions.

1 Introduction

The Kingdom of Saudi Arabia is often considered to be one of the most conservative countries in the world. The government manages Internet access with a filtering system to restrict content it deems unacceptable or inappropriate. These filtering decisions are motivated by the government's desire to protect the values of the Saudi society (which center around Islam, the official religion of the country), in addition to implementing national security and public safety policies [8].

In the last years, Saudi Arabia has undergone significant sociopolitical changes, combined with significant political events in the region, which seem to have brought forward a more progressive approach regarding access to information.

To investigate this impact on Internet filtering, we present the, arguably, first systematic longitudinal study of *digital filtering* in Saudi Arabia. We use this term to include both: (a) traditional Internet filtering on websites; and (b) access to mobile applications. The study spans the period from March 2018 to April 2020, with three separate measurements, one in each calendar year. Our goal is to answer the three questions: (a) "what content is filtered?", (b) "how is filtering implemented?", and (c) "how does filtering evolve over time in response to geopolitical conditions?"

We pursue a mutli-pronged strategy as follows.

1. Quantification: What is filtered? We provide a fairly extensive study on the accessibility of both mobile apps and websites from within Saudi Arabia and its evolution over time. Our results show significant progress towards the opening of the country's digital borders.

a. Mobile applications accessibility: We conduct systematic measurements on 18 of the most popular mobile social network applications worldwide and in the Middle East, including Facetime, Tango, Viber, Line, SOMA, and WeChat. As shown in Figure 1, all of the selected apps were blocked over the period 2013-2017, while 67% and 93% of them were accessible in 2018 and 2019, respectively. In 2020, all these apps are accessible, except WeChat. These results point to a significant relaxing of the filtering rules for mobile apps.

b. Network accessibility: We assess web access filtering by considering the top 500 most popular websites in 18 different categories according to Alexa [7] for a total of 9000 websites. In Figure 1, we plot the evolution for the three most blocked categories: *Adult*, *Shopping*, and *Games*. We observe a moderate trend across the categories towards more openness. For example, the number of accessible websites in the *Shopping* category increased from 90.4% in 2018 to 93% in 2020.

2. Understanding: filtering implementation: We identify the mechanisms in the communication interaction, where the filtering takes place. Inspired by earlier efforts [18], we develop a significantly more detailed tool for assessing digital filtering. The key capability is that we detect the specific techniques used for filtering. In more detail, we identify four types of filtering: (a) DNS level filtering, (b) IP address filtering, (c) HTTP filtering, and (d) TLS filtering, all of which we will detail in the full paper. Our results show that Internet filtering in Saudi Arabia is based on HTTP filtering augmented with TLS filtering for connections using HTTPS:

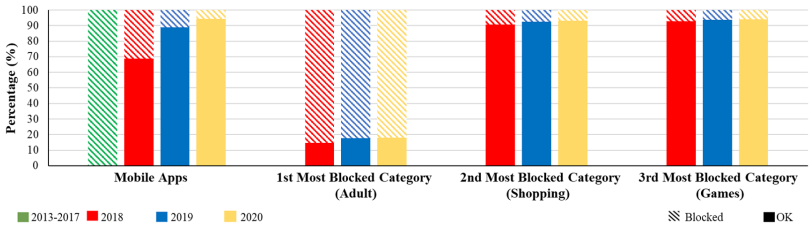

Figure 1: Overview of the extent of filtering over time per category. We observe a significant relaxing of the filtering rules for both Internet and mobile apps. Note that we did not measure the period 2013-2017, but rely instead on personal use and public sources (*e.g.,* Twitter and Saudi news sites). The bars for mobile apps represent the percentage of the apps that were tested at that time period.: we added two new apps in 2019.

- HTTP filtering: By comparing the filtering results between 2018 and 2020, we see that HTTP filtering decreased by 3.4%, 2.2%, and 1.2% in *Adult*, *Shopping*, and *Games* categories, respectively.
- TLS filtering: We also see the reflection of digital border openness in the TLS filtering results. For instance, we observe that the number of websites from the *Shopping* category that are filtered by TLS-level filtering decreased from 9.6% to 6.6% during the time of the study.

3. Interpreting: filtering and political events: We finally go at the political and policy level and examine the manifestation of real-world events on filtering. We find that ISIS-friendly sites are blocked due to the fact that ISIS supports terrorism and destabilization to the region. We also find that more news sites got blocked. For instance, some Qatari, Iranian, and Turkish news sites got blocked in 2017, 2018 and 2020, respectively, amid continued political tensions with these countries.

To increase the confidence in our observations, we performed network measurements inside Saudi Arabia from *four* major cities spread across the country (Riyadh, Jeddah, Makkah, and Al-Khobar) and spanning *three* major Internet Service Providers (ISPs) in the country. This methodology differs from prior studies of filtering in other countries, which overwhelmingly rely on VPNs or PlanetLab nodes [17,25,26].

2 Methodology

In this section, we explain the tools, measurement methodology and the data collected in our experiments. We start by presenting some ethical considerations that we contemplated as we undertook this study.

2.1 Ethical Considerations

While it is out of the scope of this paper to further discuss the debate about Internet filtering, we acknowledge that our study may be beneficial to entities on either side of the filtering. Indeed, our analysis helps understand the technical aspects of the actual filtering ecosystem in Saudi Arabia.

To avoid legal complications, we discussed the scope of our study with a Saudi high-ranking government official, who is an expert in Saudi Arabian law, and he confirmed that the study does not violate the Saudi Arabian law. Clearly, Internet filtering is a sensitive topic, and we had to consider whether the experiments would violate not only ethical considerations, but also any laws or regulations in Saudi Arabia. Article 6 in the Anti-Cyber Crime Law of the country [9] states that the production of any artifacts that would undermine public order is strictly illegal. In the context of our work, we had to verify that our measurement study does not present mechanisms to bypass the filtering which would make it illegal under article 6.

We took precautions to ensure that our study would not jeopardize any individual within or outside Saudi Arabia. We never disclosed the personal information of our anonymous volunteers, nor did we re-distribute or otherwise share the detailed experimental logs data (now or in the future). We only analyze aggregated information that neither exposes details of the network or any identifiable information with respect to our measurement points. Additionally, since Internet filtering in Saudi Arabia is evident and explicit, the act of probing blocked sites is legal.

2.2 Measurement Methodology

To identify the scope of Internet filtering inside Saudi Arabia, we tested the reachability of the most popular websites worldwide according to the Top Sites lists overall and by category published by Alexa [6]. We collected the top 500 websites in 18 different categories [7].The experiments were conducted three times, roughly one year apart between March 2018 and April 2020. For each iteration of the measurements, we got the updated lists of the top 500 websites ending up with three lists for each category corresponding to the three measurements. We found that the lists remained almost identical (less than 3% of change) across the three years and the changes were typically at the very bottom of the list. We also found that if a site is blocked in the previous year (*e.g.,* in 2018) is either still blocked in the following years (*e.g.,* in 2019 and 2020) or turned to be accessible. In other words, we have not encountered a case where a website is blocked in the previous year and no longer on the list in the following years.

In addition, we tested the availability of 18 mobile applications, including Line, Skype, and Facetime, as we discuss later.

2.3 Tool Overview

To conduct our experiments, we developed a tool which was inspired by an earlier filtering tool, Samizdat [18]. Samizdat was used in a study of Internet filtering in Pakistan in 2013. Despite the functionality of the tool, we needed to develop significant new capabilities to go to the level of granularity that wanted in our study.

For each website in our lists, we carry out the following measurements.

1. DNS Filtering: First, the tool performs a DNS lookup using UDP and records the IP address in the response packet; otherwise, the retrieved error code (*e.g.,* `Timeout`, `SERVFAIL`, `REFUSED`, `NXDOMAIN`, etc) is recorded. It then performs the same test using TCP and records the results.

2. IP Address Filtering: If the website is successfully resolved in the first test, the tool initiates a TCP connection using a stream socket to the IP address and port `80`. If the connection is established, the test is recorded as successful; otherwise, it is recorded as a failure.

3. HTTP Filtering: This experiment is divided into two phases. In the first phase, we check if there is direct HTTP filtering of the FQDN in the `GET` request. Specifically, the tool tries to establish an HTTP connection and sends a `GET` request to the website. Both the response and returned code are recorded. In the second phase, using a non-blocked website (*e.g.,* `www.google.com.sa`), the tool appends the URL of the website we want to test (*e.g.,* `www.aljazeera.com`) to Google's URL (*e.g.,* `http://www.google.com.sa/www.aljazeera.com`). The normal behavior is to see the well-known `Page Not Found` HTTP `404` error code. If a different error code (*e.g.,* `403`) is returned, this means HTTP-URL-Keyword filtering is enabled.

4. TLS Filtering: Separately, we extended the tool to try to establish a TLS connection with the web server of the site we want to test to check if there is filtering on the HTTPS protocol.

Our methodology and tool include the following steps and measurements in order to enhance and strengthen the results of our study.

First, we wanted to ensure that network issues (e.g., temporary unreachability, packet losses and other networking pathologies) do not affect the measured results. For this reason, for each year, we randomly selected and re-probed 10% of sites per category 100 times each and discovered no errors in the initial measurement for these websites. We also modified the set of open DNS servers used by Samizdat.

Second, in addition to the default DNS servers used by our vantage points (which belong to the respective ISP DNS service), we measured the Internet filtering on the following public servers: Google (8.8.8.8), Quad9 (9.9.9.9), OpenDNS (208.67.222.222), Norton (199.85.126.10), Comodo (8.26.56.26), and Level3 (209.244.0.3).

Third, to get more precise results, we performed DNS lookups using both UDP and TCP protocols. We tested site accessibility over both HTTP and HTTPS protocols since HTTPS is not amenable to keyword based filtering.

Finally, we also conducted a number of Wireshark measurements to capture and analyze the detailed network behaviors and to verify the subtleties of the filtering mechanisms.

ID	City	ISP
N1	Riyadh	STC
N2	Jeddah	STC
N3	Al-Khobar	STC
N4	Makkah	STC
N5	Makkah	Zain
N6	Makkah	Mobily

Table 1: Vantage Points

2.4 Filtering at the Mobile App Level

In what is arguably, a relatively novel dimension in filtering, we want to assess if mobile applications are affected by filtering. For that, we conduct a systematic measurement study with two smartphones one in USA and one in Saudi Arabia and we compared the differences in terms of downloading and using apps.

2.5 Measurement Vantage Points

We conducted measurements from six different vantage points distributed across four major cities in Saudi Arabia using the three major ISPs in the country. The four cities are: (1) Riyadh, which is the capital and the largest city of Saudi Arabia (population 6.5 million). Riyadh is centrally located; (2) Jeddah, which is located on the west coast and is the second largest city in the country (population 4 million); (3) Makkah, which is the birthplace of Islam and the spiritual center of the kingdom (population 2 million); and (4) Al-Khobar which is one of the major cities in the eastern region of the country (population 1 million). We selected these cities because of their different nature, roles they play in the kingdom, as well as for geographical distribution. Table 1 shows the details of each network. We chose vantage points connecting to different major Internet Service Providers (ISPs)—which are STC, Zain, and Mobily—to understand whether there is ISP level filtering, or other variation in the experienced filtering based on the ISP. All machines are connected to their default gateways, or routers, with a 1GB Ethernet cable. All machines run Windows 10 Professional Edition.

We conducted the measurements multiple times to eliminate the effect of transient phenomena, such as short lived outages. In addition, to establish a baseline external reference point, we also executed the same measurements on our lab machine in the United States (US), which also runs Windows 10 Professional Edition and is connected to the university network. We used these measurements to better understand the results from our machines in Saudi Arabia. For example, to confirm that an unreachable website is indeed blocked inside Saudi Arabia, we checked if it is accessible from the US. If the website returned the same error code (*e.g.,* HTTP codes

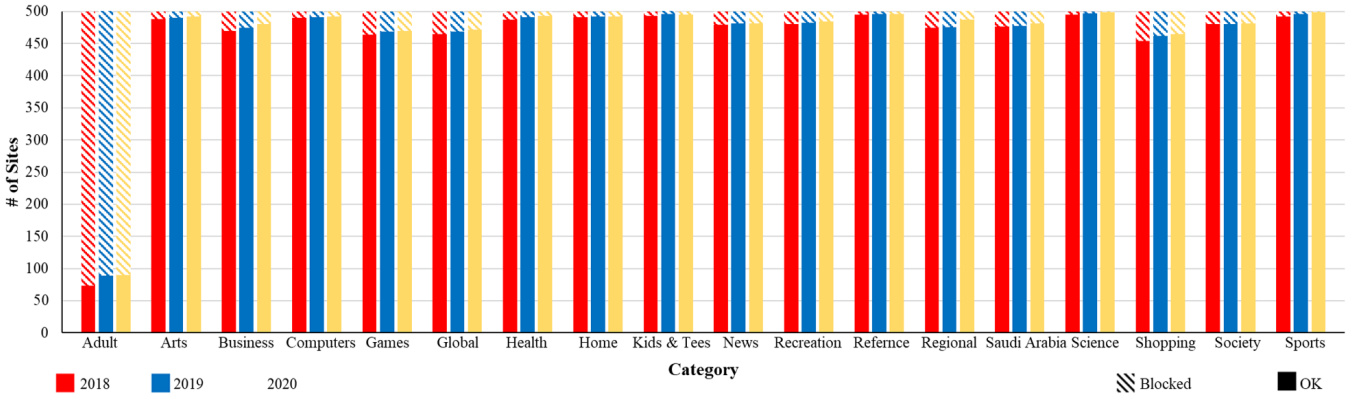

Figure 2: The scope of Internet filtering in Saudi Arabia

503 or 301 indicating that the server is unavailable or moved permanently, respectively) in both countries, we consider that the lack of accessibility is not due to filtering.

3 Results

Overall, we observe that the filtering rules are relaxed over the time for both websites and mobile apps, promising evidence that Saudi Arabia is cautiously opening its digital borders. We summarize the results of our study in Figure 2.

Adult. Unsurprisingly, we see that the most blocked category is *Adult* where 85.4%, 82.2%, and 82% of the websites are blocked in 2018, 2019, and 2020, respectively. The content of the sites in this list is usually related to pornography, gambling, drugs, violence, and similar content inappropriate for young audience. We spot-checked the content of some of the *Adult* sites that were not blocked and found that most are related to art work including comics and caricatures (we did not find any that are pornographic, gambling, or drug-related for example). We note that the increase is minimal on the other categories that are **least** blocked; however, we observe the opposite on the sites from the **most** blocked categories (*e.g.,* Adult and Shopping). We see that the largest additive difference in blocking is in the most blocked categories. The observed drop was due to websites that used to be blocked and later turned to be accessible. In addition, if we consider the top 200 sites sampled from the three lists for the Adult category corresponding to the three measurements (since they are almost identical), we find that 98.5% and 94% were blocked in 2018 and 2020, respectively.

Shopping. The second most blocked category is *Shopping*. We believe the main reason behind blocking is that these sites sell products that are considered illegal (*e.g.,* alcohol and guns).

We also found that for a blocked website, the filtering system blocks the whole domain. For example, we tried to access the accounts of a number of blocked news sites (*e.g.,* www.aljazeera.com) on other social media applications (*e.g.,* Twitter and Instagram). Since these applications use HTTPS, and hence, HTTP-URL-keyword filtering is not applied, we found that they can be accessed and viewed from inside the country.

In addition, we found that some sites are not reachable in Saudi Arabia due to server-side blocking [23]. For instance, we conducted an empirical experiment on www.sce.com which belongs to Southern California Edison (SCE), a US company that provides energy and electricity to the Southern California region. While the site is accessible in US, HTTP code 502 is returned when trying to access it in Saudi Arabia indicating that the server blocked the connection.

With respect to the operation of the filtering mechanism, we found that Internet filtering rules applied uniformly across the different vantage points and ISPs we tested: thus, we suspect that there is no additional ISP-level filtering. After verifying this observation, we show results only from one of the vantage points in the remainder of the paper (N6).

With regards to mobile apps measurements, our results show that all apps were blocked in 2017, but access was permitted to 67% in 2018 and 93% in 2019. We repeated the experiment in 2020 and found that all apps, except WeChat, were accessible. This perhaps reflects that the kingdom is moving towards moderating regulations on Internet filtering.

3.1 Filtering Mechanism

We present the key results of each filtering level:

DNS and IP Filtering. As shown in Table 2, our system could not perform DNS resolutions or establish TCP connections for a small number of websites. We believe this is resulted from transient network failures and not from purposeful filtering.

HTTP Filtering. As shown in Table 2, a large number of websites were filtered based on the HTTP URL string, (either FQDNs or special keywords): 82.2%, 7.6%, and 6.2% of the *Adult*, *Shopping*, and *Games* websites were blocked in 2019, respectively.

TLS Filtering. HTTPS disables keyword based filtering since it is not possible for the filtering system to access the encrypted contents of the TCP packet holding the GET request. Therefore, we tested the accessibility of the websites with HTTPS. We discovered that if the website being contacted

Category	DNS						IP			HTTP			TLS/HTTPS		
	UDP			TCP											
Adult	5	7	3	7	9	5	2	8	8	427	411	410	4	1	1
Arts	2	5	6	5	6	4	9	11	10	12	10	8	10	7	7
Business	3	10	11	3	8	5	6	13	14	30	26	20	38	29	15
Computers	0	0	0	0	0	0	1	0	0	10	9	8	8	6	3
Games	0	0	1	0	0	0	0	0	0	36	31	30	13	11	11
Global	6	7	7	6	7	7	12	12	12	35	31	28	9	8	6
Health	4	3	5	4	3	2	7	6	5	13	9	7	17	8	2
Home	1	2	0	1	2	1	4	5	4	9	8	8	16	10	7
Kids& Teens	2	1	1	2	1	1	3	1	0	7	6	5	12	6	5
News	0	0	0	0	0	1	1	0	0	21	19	19	20	17	13
Recreation	0	0	0	0	0	0	6	2	1	20	18	16	18	15	11
Reference	0	1	1	0	0	0	0	2	1	5	4	4	6	6	6
Regional	1	1	0	1	1	1	1	3	2	26	25	22	21	20	20
Saudi Arabia	12	12	12	11	12	13	18	18	18	24	23	19	15	15	14
Science	3	0	1	3	0	0	3	1	1	5	3	1	6	5	5
Shopping	1	1	0	1	1	1	1	1	1	46	38	35	48	36	33
Society	0	0	0	0	0	0	4	1	2	20	20	19	18	17	17
Sports	0	0	0	0	0	0	1	0	0	8	4	1	11	9	8

Table 2: Breakdown of Internet filtering results against Alexa top 500 websites in 18 categories. The table shows the number of pages that failed at a level for every attempt to load that page in a year. Numbers in blue, green, and red denote results in 2018, 2019, and 2020, respectively. The HTTP and TLS/HTTPS results are for status code `403`.

is blocked, it remains blocked under HTTPS. When examining the traces, we discovered that this is due to TLS level filtering.

3.2 Mobile Application Filtering

In this section, we report our results in regards to mobile application filtering, and we start by providing some context regarding the policies of Saudi Arabia.

Historical context regarding mobile app usage. In 2013, CITC blocked the Voice over Internet Protocol (VoIP) call services on Viber, a popular mobile application that offers free video/voice calls [24]. VoIP calls on similar applications were slowly being blocked including FaceTime, Skype, Line, Tango, Facebook Messenger, WhatsApp and Snapchat. We believe the main reason behind blocking is economic, since these applications provide free alternatives to services that otherwise generate revenue to the ISPs. CITC received requests from service providers such as Mobily and STC to block the free or low-cost VoIP calls on these applications to protect their competitiveness and rights [13, 14]. However, in 2017, CITC responded to citizens demands and announced its intent to lift the ban on all applications that provide voice and video communications over the Internet that meet the regulatory requirements of the country [10]. We conjecture that this decision was also driven by the Vision 2030 and National Transformation 2020 programs published with the aim of modernizing society: one of the stated goals is to provide transparency and clarity with respect to policies especially in the telecommunications and information technology sectors.

We conduct three measurements for mobile apps whose results we summarize in Table 3. We attempt to install and use them on two iPhones, one in Saudi Arabia and the other in USA. We tested the text, audio, and video communication services. Based on personal use, our mobile app group was completely blocked in 2013-2017, the period before CITC lifted the ban on all applications that provide voice and video communications over the Internet that meet the regulatory requirements of the country [10]. In March 2018, five applications failed to establish at least one of the text, audio, and video communication services. In October 2019, we repeated the experiment and added two more applications: Houseparty and WeChat. We found that both audio and video calls are still blocked on WhatsApp, which was corroborated by a CITC statement [4]. We could not install the application WeChat on our Saudi iPhone. Although the vice president of Tencent announced back in 2013 that WeChat is available in Saudi Arabia [1], this is not fully accurate. Currently, we are not sure if the installation failure is caused by Tencent or the Internet filtering system. Finally, in April 2020, we repeated the experiment and found that nearly all previously-blocked messaging applications were accessible, including WhatsApp, with the only exception being WeChat.

3.3 Relation Between Geopolitical Events and Internet Filtering

Over the past years, the Middle East experienced several major political events that affected societies internally and externally. Consequently, these events affected Saudi Arabian policies regarding access to information, and our measurements capture the effect of such events, as we discuss below.

A prominent event is the rise of the so-called "Islamic State" in Iraq and Syria (known as ISIS) in the last decade,

Application	2013-2017			2018			2019			2020		
	Text	Audio	Video	Text	Audio	Video	Text	Audio	Video	Text	Audio	Video
Viber	✓	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓
Tango	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
FaceTime	✓(iMessage)	✗	✗	✓(iMessage)	✓	✓	✓(iMessage)	✓	✓	✓(iMessage)	✓	✓
YeeCall	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Skype	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
WhatsApp	✓	✗	✗	✓	✗	✗	✓	✗	✗	✓	✓	✓
Line	✓	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓
Telegram	✗	✗	NA	✗	✗	NA	✓	✓	NA	✓	✓	NA
AllApp	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Google Duo	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Houseparty	NA	NA	NA	NA	NA	NA	✓	✓	✓	✓	✓	✓
WeChat	NT	NT	NT	NT	NT	NT	✗	✗	✗	✗	✗	✗
SOMA	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Snapchat	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Google Hongout	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Facebook Messenger	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
imo	✓	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓
JusTalk	NT	NT	NT	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 3: Breakdown of Internet filtering results against popular messaging mobile applications. We tested the text, audio and video communication services. Symbols show if a communication service is supported (✓), blocked (✗), not applicable (NA) (e.g. service not available at the time), or not tested (NT). Note that the results displayed for the period 2013-2017 are based on personal experience and not extensive measurements. Also note that the release date of all apps except HouseParty (released in 2019) is either before or within this period. For instance, Line, Telegram, and Google Duo were initially released in 2011, 2013, and 2016, respectively.

whose effect emerges in our measurements. We tested the accessibility of 5 ISIS-friendly websites (which we obtained by scouring the web and following previous practice we do not disclose for ethical reasons) and found that all of them were blocked. ISIS and its affiliates have exploited social media websites, such as Twitter, to spread their propaganda and to recruit new members [20]. This type of activity has in turn been countered by efforts from the Saudi Arabian government by regulating information access for Saudi citizens. For instance, at the Shura Council, the chairman of the Islamic and judicial affairs committee called for the blocking of all ISIS websites, since they considered them to advocate terrorism and destabilization to the region [5], a stance that has been followed by many other countries and institutions as well [11, 12, 16, 19, 21]. In addition, many Saudi citizens launched an online campaign on Twitter aiming to lock down user accounts belonging to or supporting ISIS [15].

Another prominent event is the increased political tension between Qatar and Saudi Arabia, which was also captured in our measurements. Because of these tensions, the Saudi authorities blocked some Qatari news web sites [3] in 2017. For instance, a warning page by the Ministry of Culture and Information was displayed when we tried to visit `www.aljazeera.com`; one of the most popular news websites in Qatar. In addition, in April 2020, we obtained a list of Qatari news sites [3] and found that all of them were blocked.

Another notable event is the ongoing conflict between Saudi Arabia and Iran. Following an attack on the Saudi embassy in Tehran in January 2016 [2], Saudi Arabia cut all diplomatic relations with Iran. Our measurements show evidence that this event had impact on the Internet filtering. For instance, in 2018, our measurements show that some Iranian sites (mostly from the *News* category) got blocked.

Finally, in April 2020, we observed a change in the access for some Turkish sites compared to the earlier measurements. Upon investigation, we found that Saudi authorities blocked two prominent Turkish news websites, Anadolu and TRT Arabic platforms, amid what the Ministry of Media communicated as continued violations of their regulations. We conjecture that the move was partly driven by a campaign on Twitter by Saudi citizens calling for the Turkish news platforms to be blocked [22].

4 Conclusion

Our longitudinal study of *digital filtering* shows that Saudi Arabia has made progress towards opening its digital border. We argue that our study consists of two novelties: (a) we consider mobile applications as an integral part of digital openness; and (b) we investigate and assess the technical details of four different types of filtering mechanisms in the kingdom over the period of three years. In addition, the three year span of our study enables us to observe changes in the filtering policy and view these changes in the wider geopolitical context experienced by the kingdom and the region.

Acknowledgment

This material is based on work supported by Taibah University (TU) and the Saudi Ministry of Education (MOE). Any opinions, findings, and conclusions or recommendations expressed in this work are those of the authors and do not necessarily reflect the views of the funding agencies.

References

[1] Wechat arrives in saudi arabia. *Saudi Gazette*, 2013. , available at http://saudigazette.com.sa/article/47305.

[2] Hun condemns attack on saudi embassy in iran. *BBC News*, 2016. , available at https://www.bbc.com/news/world-middle-east-35229385.

[3] Here is a list of all qatari web sites that are blocked in saudi arabia. *Alarabiya*, 2017. , available at http://ara.tv/z8sek.

[4] Whatsapp calls are blocked in saudi arabia .. the reasons are organizational. *Sabq*, 2019. , available at https://sabq.org/wY2Vmk.

[5] Alarabiya. Saudi arabia .. al-shura demands to ban all isis web sites. *Alarabiya*, 2016. , available at http://ara.tv/gqz88.

[6] Alexa Top Sites. The alexa top sites web service. , available at https://aws.amazon.com/alexa-top-sites/.

[7] Alexa Top Sites. The top 500 sites on the web (2018). , available at https://www.alexa.com/topsites, note = Online; accessed 27 April 2020.

[8] Communications and Information Technology Commission (CITC). General Information on Filtering Service. http://web1.internet.sa/en/general-information-on-filtering-service/. Online; accessed 14 April 2020.

[9] Communications and Information Technology Commission (CITC). Anti-Cyber Crime Law. https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx, 2007.

[10] Communications and Information Technology Commission (CITC). In line with the needs of the user and in line with global trends, CITC announces the launch of Internet communications applications. http://www.citc.gov.sa/ar/mediacenter/pressreleases/Pages/2017092001.aspx, 2017.

[11] DW. Turkey blocks websites loyal to isis. *DW*, 2015. , available at https://p.dw.com/p/1FyTF.

[12] Facebook. Hard questions: How we counter terrorism. *Facebook*, 2017. , available at https://about.fb.com/news/2017/06/how-we-counter-terrorism/.

[13] Helen Gaskell. Whatsapp's new call service to be blocked in ksa. *ITP.net*, 2015. , available at https://www.itp.net/602475-whatsapps-new-call-service-to-be-blocked\-in-ksa.

[14] Andrew Griffin. Facebook messenger blocked in saudi arabia: Chat apps have voice and video call functions banned over regulations. *Independent*, 2016. , available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-messenger-blocked-in-saudi-arabia-chat\-apps-have-\voice-and-video-call-functions-\banned-over-a7027301.html.

[15] Majed Al Hazaa. A popular campaign to close isis accounts on twitter. *Alarabiya*, 2015.

[16] Natasha Lomas. Uk outs extremism blocking tool and could force tech firms to use it. *TechCrunch*, 2018. , available at https://techcrunch.com/2018/02/13/uk-outs-extremism-blocking-tool-and-could-force\-tech-firms-to\-use-it/.

[17] Anuradha Mathrani and Massoud Alipour. Website blocking across ten countries: A snapshot. In *PACIS*, page 152, 2010.

[18] Zubair Nabi. The anatomy of web censorship in pakistan. In *FOCI*, 2013.

[19] Noon. Iraq: Minister of communications: Blocking isis websites tops our ministerial program. *Noon*, 2014. , available at http://www.non14.net/public/56224.

[20] Charlie Osborne. Anonymous targets isis social media, recruitment drives in opisis campaign. *ZDNet*, 2015. , available at https://www.zdnet.com/article/anonymous-targets-isis-social-media-recruitment\-drives-\in-opisis-campaign/.

[21] Don Reisinger. Twitter has suspended 1.2 million terrorist accounts since 2015. *Fortune*, 2018. , available at https://p.dw.com/p/1FyTF.

[22] The New Arab. Saudi Arabia blocks Turkish news sites Anadolu, TRT amid continued Ankara-Riyadh tensions. available at https://english.alaraby.co.uk/english/news/2020/4/12/saudi-arabia-blocks-turkish-news-sites-anadolu\-trt, note = Online; accessed 14 April 2020 , year = 2020.

[23] Michael Carl Tschantz, Sadia Afroz, Shaarif Sajid, Shoaib Asif Qazi, Mobin Javed, and Vern Paxson. A bestiary of blocking: The motivations and modes behind website unavailability. In *8th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 18)*, 2018.

[24] Sebastian Ushe. Saudi arabia blocks viber messaging service. *BBC News*, 2013. , available at https://www.bbc.com/news/world-middle-east-22806848.

[25] John-Paul Verkamp and Minaxi Gupta. Inferring mechanics of web censorship around the world. In *FOCI*, 2012.

[26] Xueyang Xu, Z Morley Mao, and J Alex Halderman. Internet censorship in china: Where does the filtering occur? In *International Conference on Passive and Active Network Measurement*, pages 133–142. Springer, 2011.