Shedding Light on Mobile App Store Censorship

Vasilis Ververis
Humboldt University, Berlin, Germany
ververis@kth.se

Marios Isaakidis
University College London, London, UK
m.isaakidis@cs.ucl.ac.uk

Valentin Weber
Centre for Technology and Global Affairs
University of Oxford, Oxford, UK
valentin.weber@cybersecurity.ox.ac.uk

Benjamin Fabian
University of Telecommunications Leipzig (HfTL)
Humboldt University, Berlin, Germany
bfabian@wiwi.hu-berlin.de

ABSTRACT

This paper studies the availability of apps and app stores across countries. Our research finds that users in specific countries do not have access to popular app stores due to local laws, financial reasons, or because countries are on a sanctions list that prohibit foreign businesses to operate within its jurisdiction. Furthermore, this paper presents a novel methodology for querying the public search engines and APIs of major app stores (Google Play Store, Apple App Store, Tencent MyApp Store) that is cross-verified by network measurements. This allows us to investigate which apps are available in which country. We primarily focused on the availability of VPN apps in Russia and China. Our results show that despite both countries having restrictive VPN laws, there are still many VPN apps available in Russia and only a handful in China. In addition, we have included findings of a global search for the availability of privacy-enhancing and other apps that are known to be censored. Finally, we observe that it is difficult to find out which apps have been removed or are unavailable on the examined app stores. As a consequence, we urge all app store providers to introduce app store transparency reports, which would include when apps were removed and for what reasons.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; *Human and societal aspects of security and privacy*; • **Networks** → **Network services**; • **Social and professional topics** → **Censorship**; **Technology and censorship**; **Censoring filters**; **Net neutrality**; **Network access restrictions**; **Acceptable use policy restrictions**; **Government technology policy**; **Governmental regulations**; **Import / export controls**; *Computing / technology policy*; *Network access control*; Broadband access; • **Information systems** → *Specialized information retrieval*.

UMAP'19 Adjunct, June 9–12, 2019, Larnaca, Cyprus

ACM ISBN 978-1-4503-6711-0/19/06…$15.00
https://doi.org/10.1145/3314183.3324965

KEYWORDS

app stores, censorship, country availability, mobile applications, China, Russia

ACM Reference Format:
Vasilis Ververis, Marios Isaakidis, Valentin Weber, and Benjamin Fabian. 2019. Shedding Light on Mobile App Store Censorship. In *27th Conference on User Modeling, Adaptation and Personalization Adjunct (UMAP'19 Adjunct), June 9–12, 2019, Larnaca, Cyprus.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3314183.3324965

1 INTRODUCTION

The widespread adoption of smartphones over the past decade saw an extreme rise in the development, distribution and usage of mobile applications: computer programs that are specifically designed for mobile devices. For brevity, throughout the paper we will be referring to them as applications or apps. Their use cases cover a wide domain ranging from entertainment to banking, medicine, education, and communication. Mobile applications are used by billions of people on a daily basis for both personal and business purposes.

The main distribution channels for applications are a handful of centralized platforms known as app stores. The characteristics of these depend on the operating system (OS) of the mobile device. Most app stores take the form of an online store, that regulates free or paid applications, and distributes them in various countries. App stores are actually common in other platforms as well, such as in Linux distributions and in game distribution [20].

The main goal of this paper is to investigate the availability of apps in several app stores across different countries. We focus on the following three app stores: Google Play (i.e. Google Play Store) operated by Google LLC, iTunes Store (i.e. Apple App Store) operated by Apple Inc., and Tencent MyApp (i.e. Tencent App Store) operated by Tencent Holdings Ltd. The first two account for a large percentage of Android and iOS mobile devices, while the latter operates primarily in China and is the largest app store in that country. For Android-supported devices, there are further app stores with significantly less market share; for iOS devices, the Apple App Store is the only available app store.

A large part of our study focuses on Russia and China, two major mobile app markets. In order to estimate the inclusiveness of our study, we have gauged the percentage of the market share that the Apple App store, Google Play Store, and Tencent App Store occupy in respective markets. In China, Apple has the largest app store by downloads with 500 million downloads in March 2017 [3]. It is followed by the Tencent App Store that recorded 250 million

downloads during the same month, which amounts to 25% of the Android market share. Tencent App Store is the leading Chinese Android app market accounting for 13.71% of the market share measured in monthly average users of the second of 2018 [9]. Tencent App Store is predominantly targeted at Chinese speakers and is hence available in Chinese language [22]. Tencent App Store is differentiating its terms of service between users that reside anywhere in the world and Chinese residents (regardless of the nationality), Chinese nationals (even if they reside outside China), and Chinese companies [19].

2 RELATED WORK

In this section, we present a literature review and classify related work to better highlight its importance and similarity to the studies in our paper. We structure this section into the following aspects: app store regulations, app store comparisons, and app store mining.

2.1 App Store Regulation

Hestres, Luis E. analyzes [32] Apple's guidelines and approval process, discusses content based rejections of apps, and outlines the consequences of this process for developers' and consumers' freedom of expression. It also argues for principles that guarantee *app neutrality* while also guaranteeing device safety and quality control. Síthigh, Daithí Mac [37] assesses the regulation of smartphone app stores and highlights the importance of forms of regulation that are not linked to a violation of competition law. *Developer-focused issues* deals with the relationship between Apple and app developers; three themes of Apple's Guidelines are identified (content, development and payments), and the ways in which control can be challenged (through jailbreaking, web apps and regulatory intervention) are scrutinized.

2.2 App Store Comparisons

Lim, Soo Ling et al. [36] conducted one of the largest surveys to date of app users across the world, investigating user adoption of the app store concept, app needs, and rationale for selecting or abandoning an app. They collected data from more than 15 countries. The analysis of data provided by 4,824 participants showed significant differences in app user behaviors across countries. Ghazawneh, Ahmad and Ola Henfridsson [31] provide a paradigmatic analysis of different app stores that helps to understand the relationship between application marketplaces, platforms and platform ecosystems. They generate a typology that distinguishes four kinds of digital application marketplaces; closed, censored, focused and open marketplaces. Seneviratne, Suranga et al. [41] propose a method to detect spam apps solely using app metadata available at the time of publication, according to a set of checkpoint heuristics that reveal the reasons behind their removal. Their analysis suggests that approximately 35% of the apps being removed are very likely to be spam apps. They map the identified heuristics to several quantifiable features and show how distinguishing these features are for spam apps.

Peltonen, Ella et al. [40] carry out an analysis of geographic, cultural, and demographic factors in mobile usage. Their research sample is gathered from 25,323 Android users from 44 countries and 54,776 apps in 55 categories, and demographics information collected through a user survey. Their paper reveals significant differences in app category usage across countries that reflect geographic boundaries. They demonstrate that the country category gives more information about application usage than any demographic, with geographic and socio-economic subgroups in the data. Albrecht, Urs-Vito et al. [26] propose SARASA, a semiautomatic retrospective app store analysis, which provides a step-by-step filtering of apps by formal criteria. A full survey of the metadata of 103,046 apps from Apple' s German App Store in the Medicine and Health & Fitness categories was carried out.

2.3 App Store Mining

Martin, William et al. [38] studies information about applications obtained from app stores.

Their survey describes and compares the areas of research that have been explored thus far, drawing out common aspects, trends and directions future research should take to address open problems and challenges. Fu, Bin et al. [30] propose WisCom, a system that can analyze millions of user ratings and comments in mobile app markets at three different levels of detail: (a) discovery of inconsistencies in reviews; (b) identification of reasons why users like or dislike a given app through an interactive, zoomable view of how users' reviews evolve over time and (c) identification of users' major concerns and preferences of different types of apps. A limitation to their study is that they are analyzing apps that are only available on Google Play Store.

Chen, Ning et al. [28] propose an app review mining framework performing comprehensive analytics from raw user reviews by (i) first extracting informative user reviews and by filtering noisy and irrelevant ones, (ii) then grouping the informative reviews automatically using topic modeling, (iii) further prioritizing the informative reviews by an effective review ranking scheme, (iv) and finally presenting the group-s of most "informative" reviews via an intuitive visualization approach. Their limitation is that they have used only four Android apps to evaluate their review mining framework. Tang et al. [42] conducted an empirical study of a large-scale set of fake apps. They have collected over 150,000 samples of popular applications and performed a quantitative study of fake samples and fake authors' developing trends.

3 METHODOLOGY

The focus of this paper is the availability of mobile apps in major app stores (Google Play Store, Apple App Store, Tencent App Store) across different countries.

In order to understand which applications are unavailable in a country, we collected data by querying the official search engines of the app stores for a given term and for specific apps (see Section 3.1). So as to eliminate false positives, we identified the countries where Google, Apple and Tencent operate their app stores and the reasons why a country might be excluded (see Section 3.2). For that, we conducted research on the terms of service of these companies, their official online documentation, their user forums, and we got in contact with their support teams and app developers. Moreover, we referred to news sources for building a test list with

Group	Countries
CG1	Google Play unavailable: Syria, North Korea
CG2	Abshar, Orbot, Signal and Skype unavailable in Google Play: South Sudan, Sint Maarten, Bonaire, Sint Eustatius, Saba
CG3	96 countries where iTunes is officially not available
CG4	All of the apps in our test list unavailable in iTunes: Cocos Island, Christmas Island, Guam, Heard Island and McDonald Islands, British Indian Ocean Territory, Kiribati, Marshall Islands, Northern Mariana Islands, Norfolk Island, Nauru, United States Minor Outlying Islands

Table 1: Country Groups with regards to how and why they are censored

candidate apps that are unavailable in specific regions, and for interpreting our findings.

Throughout the paper we cluster countries with regards to the way and the reasons why they are censored, in four Country Groups, as they appear in Table 1.

3.1 Querying Mobile App Stores

For our research we made queries directly to the three app stores we are targeting. All of them can be accessed in two ways: either via their mobile application, or via the website they maintain. The respective query URLs (see Table 2) do not require authentication and they support searching for a term and retrieving details for a given application. To that extent, they can be used for future research on app stores, since they provide additional information including application categories, the number of installations of an app, its review ratings, price, developer and release information.

In addition, the query URLs support parameters for filtering the results. Both Google Play and iTunes provide a way to query the app stores in different countries, by including the desired ISO 3360 country code in the query parameters [12]. We take advantage of this feature to find out what the query results would be for users in a specific country.

Parsing the results of the queries can be simplified with scraper scripts. In our source code repository [11] we have uploaded wrappers for the *google-play-scraper* and *app-store-scrapper* node.js packages, together with a script that queries the app stores in different geographic areas. Also, we have uploaded the corresponding results for the term "vpn" and for apps that are reported to be censored (such as Psiphon and the Onion Browser).

3.2 App Store Operation Across Countries

In order to minimize false positives on app availability per app store and per country, we consulted the list of supported countries each company is operating their app store in. Currently we only take into consideration the Apple iTunes and Google Play app stores, as they are the only ones with an official country availability list on their websites, and since the Tencent MyApp store is primarily targeting users in China.

3.2.1 Google Play. According to Google's documentation, the supported locations for distribution to Google Play users are listed [18] to a total of 144 countries, and a "Rest of the World" category. The actual countries included in the "Rest of the World" category, or at least their number, is not publicly available. In addition, the available information does not clarify the reason why the Google Play Store is not operating in a country; whether that is due to sanctions, regulations, or company and in-country policies.

By looking on the crawled app data for Google Play we found out that Play Store is not available in Syria and North Korea (ISO 3360 country codes SY and KP). That brings us to believe that Google Play Store is most probably not operating in these countries, whereas in other countries with US sanctions we were able to retrieve app information. For these two countries (SY and KP) we are going to use the group notation Countries Group (CG) 1 throughout the paper.

3.2.2 Apple iTunes. The Apple App Store provides a list of the countries it is available in, which is more transparent than the Google Play Store list. We found Apple App store to not operate almost on an entire hemisphere, i.e. 96 countries [8]. We use the notation Countries Group (CG) 3 for these countries. At first we thought that we misunderstood something or that we overlooked a website where more countries are listed. For this reason we contacted the Apple App Store customer support that directed us to the same page that we base our findings on [8], along with information on how one can change one's Apple App Store country. Upon further inquiries they were not able to provide us with more information on why these countries are blocked from operating Apple App Store.

Some restrictions may apply because of export restrictions. This is why stores are not available in Iran, North Korea, and Syria for instance. In some countries like Serbia, the Apple App Store is not available for legal or commercial reasons. This could be due to practical matters, such as Apple not having a registered legal entity in Serbia, or perhaps even because the sale would most likely be initiated in foreign currency. Maybe for that reason the Serbian Google Play Store shows prizes only in US dollar and not in the local dinar. Countries like Morocco and Rwanda (where the Apple App Store) that are not available may also fall in this category. But again we cannot be sure given the limited information available to the public.

4 FINDINGS OF MOBILE APP STORE CENSORSHIP

For our measurements we created a list comprised of free and open source censorship circumvention, anonymity and messaging mobile apps; I2P, Psiphon, Onion Browser, Orbot, Signal, and Shadowsocks. In order to verify claims about blocked or otherwise unavailable apps in different countries we added Skype (a widely used voice application), the New York Times news app, LinkedIn social network app and the controversial Abshar app developed by the government of Saudi Arabia.

In Table 3, we list the app names together with their IDs (when available) in all three app stores along with the unavailable list of countries per app. All apps on Apple App Store were not available (apart from the other 96 unavailable countries) in Cocos Islands (CC), Christmas Island (CX), Guam (GM), Heard Island and McDonald Islands (HM), British Indian Ocean Territory (IO), Kiribati (KI), Marshall Islands (MH), Northern Mariana Islands (MP), Norfolk Island (NF), Nauru (NR) and United States Minor Outlying Islands (UM). For the aforementioned countries we are going to use the group notation Countries Group (CG) 4. Onion Browser,

App Store	Search for a term	Lookup App Details
Google Play	https://play.google.com/store/search?c=apps&q={term}&gl={country}	https://play.google.com/store/apps/details?id={Google Play Id}&gl={country}
Apple App Store	https://itunes.apple.com/search?term={term}&country={country}	https://itunes.apple.com/lookup?id={iTunes Id}&country={country}
Tencent MyApp	https://android.myapp.com/myapp/searchAjax.htm?kw={term}	https://android.myapp.com/myapp/detail?apkName={MyApp Id}

Table 2: The URLs for querying the app stores for a term and for the details of a given application. {term}: the search term, {Google Play ID/iTunes ID/MyApp ID}: the ID of the app in each platform, {country}: the country code

App Name	Google Play Id	iTunes Id	MyApp Id	Unavailable countries
Abshar	sa.gov.moi	1004966456	N/A	CG1, CG3, CG4
I2P	net.i2p.android	N/A	+	
LinkedIn	com.linkedin.android	288429040	+	CG1, CG3, CG4, CN, RU*
New York Times	com.nytimes.android	284862083	N/A	CG1, CG3, CG4
Onion Browser	N/A	519296448	N/A	CG1, CG3, CG4, CN
Orbot	org.torproject.android	N/A	N/A	CG1
Psiphon	com.psiphon3.subscription	1276263909	N/A	CG1, CG3, CG4, CN
Signal	org.thoughtcrime.securesms	874139669	+	CG1, CG3, CG4
Skype	com.skype.raider	304878510	N/A	CG1, CG3, CG4, CN
Shadowsocks	com.github.shadowsocks	N/A	N/A	CG1
Keyword Search: VPN	CG1, CG2	CG1, CG2, CN	CN	

Table 3: An indicative list of queries for apps and keywords in different countries. Includes app identifiers in each app store. +: Same app ID with Google Play, *: Unavailable in Google Play Store and Apple App Store, CG1-4: Country Groups (see Table 1)

Psiphon and Skype apps were found unavailable in China, whereas LinkedIn app was unavailable in both Russia and China. These findings confirm the multitude of reports and new Chinese regulations that ban unlicensed VPN providers or censorship circumvention apps to operate in China [43]. LinkedIn is unavailable in both Google Play Store and Apple App Store in Russia, because the government banned the company's app and website [15].

Apart from countries in CG1, while performing a full text search for the queries abshar, orbot, signal and skype we got an empty response for the countries South Sudan, Sint Maarten and Bonaire, Sint Eustatius and Saba, we are going to refer to these countries as Countries Group (CG) 2.

Tencent App Store seems to have a strict policy on VPNs, since neither keyword searches nor a search of the specified app list (see Table 3) yielded results. We found I2P to be available; an anonymous peer to peer network and that could be confirmed by the relative high number of I2P nodes in China [33]. Similarly The LinkedIn app, which is blocked in China and Russia is available, as well as the Signal instant messaging app. All apps share the same app ID as in Google Play Store.

In our analysis we cover around 50% of the app store market share in Russia and around 30% in China. Censoring an app on Apple App store or Tencent App Store in China will have a larger effect than on Google Play Store, which is barred from the market in China [42]. Similarly censoring an app from Google Play Store in Russia has a greater effect than excluding an application from the Apple App store, due to Google's larger footprint within the country.

4.1 Verification

We cross-checked our results from different vantage points. We have uploaded the results of our queries for the terms "VPN", "proxy", "代理", "🅵擬私人網路", "🅵拟私人网络", "私人互联网接入", "规避", "circumvent", "专用网络", "互联网网络", "加密通讯", "翻墙", and mobile applications that are being censored in Table 3 in our git source repository [11].

We were able to cross-verify our methodology (presented in section 3) with publicly available data from OONI; a free software project which collects and processes network measurements with the aim of detecting network anomalies, such as censorship, surveillance, and traffic manipulation [29]. OONI data show that the LinkedIn app on Google Play Store[1] was not accessible (returned an HTTP Code 404) [2].

By using OONI's API [3] we were able to obtain all anomalous measurements for the Google Play App Store URL of LinkedIn. Specifically we identified at least 52 different network vantage points of Russian autonomous systems; 12389, 12714, 12790, 12958, 15378, 16345, 20807, 21367, 24588, 25159, 25490, 25513, 28745, 28812, 29226, 29497, 31133, 31213, 31376, 31430, 3216, 3239, 3253, 34533, 35807, 39289, 41661, 41682, 41691, 41733, 42610, 42668, 43595, 44640, 47395, 48092, 48190, 48642, 49478, 51035, 51570, 51604, 5429, 5563, 56330, 56377, 6856, 8359, 8369, 8402, 8427 and 8595. The queries to the API and tools to extract the ASes can be found in our repository [11].

5 VPN MOBILE APP REGULATIONS IN RUSSIA AND CHINA

In the following section we compare the law on VPNs as well as availability of the top global VPN providers within China and Russia. These two case studies provide an in depth examination of two major app markets and are an addition to the large N comparison of app availability worldwide.

The law on VPNs had been quite loose for the past few years. In 2017, however, China restricted VPN usage more seriously. This is due to a *Notice of the Ministry of Industry and Information Technology on Clearing up the Market for Regulating Internet Access Services* and China's 2017 cyber security law [24, 25]. In essence, only government approved VPNs are allowed [4]. On this legal basis, China requested Apple to remove 674 VPN apps from its app store [1], [10]. In turn, VPN providers received letters from Apple

[1] https://play.google.com/store/apps/details?id=com.linkedin.android
[2] https://archive.fo/dWPiS
[3] https://api.ooni.io

saying that the content they provide is illegal in China and consequently their application had to be removed [2]. We conducted a keyword search of "VPN" on the Russian and Chinese Apple App Stores and manually verified the results. Apple's app store in China returned 54 results, which included not only the title of the app but also content that describes an app. A manual search through the results showed that less than 5 apps are actual VPN apps. It is expected that the VPNs available are government approved and surveilled ones. In most countries the number amounts to around 200 returns in results. VPN availability on the Apple App store in China is consequently low. None of the major foreign VPNs were available for download in China. It is expected that domestic alternatives are available, but these have poor privacy policies and are expected to share data with the government [39]. We also searched the Apple App Store in China for "proxy", "代理", "🄵擬私人網路", "🄵拟私人网络", "私人互联网接入", "规避", "circumvent", "专用网络", "互联网网络", "加密通讯", "翻墙", and evaluated the results one by one. These searches provided many results that matched the keyword searches. However, they contained less than five apps in total that provide VPN services.

Russia for its part instituted restrictions on VPN usage in 2017 through its amendments to the *Law on Information, Information Technologies and Information Protection* [23]. The law stipulates that VPNs are allowed but they have to make sure that no censored websites are accessed through them [21] and that they have to share user data with the Russian government [7]. The law also states that search engines have to delete VPN service related results from its services or else they will be fined [16]. In 2018 Russia went a step further and banned 50 VPNs and censorship circumvention tools [17] that allowed users to access the Telegram messaging app, which was also prohibited by the government [34].

Despite similar Russian and Chinese laws, VPN apps are still available on app stores in Russia. A keyword search for "VPN" returned 199 results, including major VPN providers. This shows that the ban is not as thoroughly implemented in Russia. This loose implementation was also reported on by Russian news and observers. The environment in Russia may be less strict because of technical challenges with the implementation, such as difficulties with distinguishing VPNs that are used by private or commercial VPNs, or problems with forcing foreign VPNs into compliance with the law. In China the environment is much harsher with almost no VPNs available in the Apple and Tencent App stores.

6 THIRD-PARTY APP STORES

A significant factor that contributes to mobile app censorship is the strategy of mobile operating system developers (Google for android, and Apple for iOS) to maintain the monopoly of the app ecosystems through the lockout of third-party app stores. Centralization of app distribution to a handful of app stores makes it easier for governments to block specific apps. According to court cases against Google and Apple for allegations under anti-competitive actions legislation [5, 6], their motivation for obstructing alternative app stores is mainly financial, since they profit from commissions on app purchases, monetization of user analytics, and the promotion of their own services. On the other side, this strategy is justified as a security safeguard, because there can be no guarantees of the validity of the applications distributed by independent app stores.

From the point of view of app availability, third-party app stores are appealing to users because they do not enforce country-specific censorship. For example, users in Russia, where LinkedIn is not available on Apple App Store and Google Play Store (see Section 4), can still download the app from AppAddict [13] and Aptoide [14] respectively. However, in order to do that, they have to manually degrade their security, e.g. by modifying their settings to allow the installation of software from unknown sources, or even by jailbreaking their devices and thereby voiding their warranty. Furthermore, they have to trust third-party app stores to deliver the genuine applications and that they will make updates available in the future. In general, independent app stores bring freedom to users and developers, and contribute to a healthy software ecosystem. However, they are less regulated, do not always collaborate directly with the developers of the apps, and their revenue models are unclear [35].

7 CONCLUSION

Given the centralized nature of app stores one may think that finding out whether a specific app is available in their country is straightforward. It turns out that this question is not so easy to answer. Unfortunately, there are no transparency reports on app availability, and none of the app stores that we study provides information about which apps are censored and for what reasons. Also, it is unclear how users will receive updates on installed apps that get banned.

Our report presents a methodology for querying the major app stores – Google Play Store, Apple App Store, Tencent App Store – to find out whether (a) they are operating in a country, and (b) whether an app is available in that country. In that way, we were able to identify geographical regions where app stores are not available. Moreover, we collected evidence of unreported censorship, specifically for censorship circumvention, anonymity and messaging mobile apps. Furthermore, we took a closer look into VPN mobile app availability in China and Russia. The environment in China is much stricter than in Russia, with none of the major VPN apps being available in the Apple App Store and Tencent App Store. Russia is looser with its implementation of VPN restrictions on app stores. As a countermeasure, users can download censored applications via third-party app stores, but this can potentially degrade their security and privacy.

8 RECOMMENDATION

Our recommendation is that app store companies ought to launch app transparency reports. In 2018, Apple announced that future reports would include information on government removal requests of apps. However, to the best of our knowledge Apple has not yet followed up on its promise [27]. Google has no mechanism to publicly report take down requests of apps either.

Our paper highlights how opaque the global app market is and that companies such as Google, Apple, and Tencent need to become more transparent about their operations. We recommend them to introduce app transparency reports that would include

the identification of apps that were removed due to government requests and the reasons for their removal. Furthermore, they should indicate why their app store is not available in certain countries, and whether this is for political, financial, or legal reasons.

ACKNOWLEDGMENTS

We are especially grateful to Greatfire.org, Nguyen Phong Hoang and Flora Wang for their insightful comments.

REFERENCES

[1] 2017. Apple drops hundreds of VPN apps at Beijing ' s request. https://www.ft.com/content/ad42e536-cf36-11e7-b781-794ce08b24dc [Online; accessed 16. Apr. 2019].
[2] 2017. Apple removes VPN Apps from China App Store | ExpressVPN. https://www.expressvpn.com/blog/china-ios-app-store-removes-vpns [Online; accessed 16. Apr. 2019].
[3] 2017. Top App Stores & mobile apps in China for Q1 2017. https://www.chinainternetwatch.com/20410/top-app-stores-mobile-apps-q1-2017 [Online; accessed 16. Apr. 2019].
[4] 2018. China's Cybersecurity Law: An Intro for Foreign Businesses. https://www.china-briefing.com/news/chinas-cybersecurity-law-an-introduction-for-foreign-businesspeople [Online; accessed 16. Apr. 2019].
[5] 2018. European Commission - PRESS RELEASES - Press release - Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine. http://europa.eu/rapid/press-release_IP-18-4581_en.htm [Online; accessed 16. Apr. 2019].
[6] 2018. In re Apple iPhone Antitrust Litig., 846 F.3d 313 (9th Cir. 2017) (No. 17-204).
[7] 2018. Russia Will Penalize For Using and Promoting VPN Services, So Now What? | VPNBase. https://vpnbase.com/blog/russia-will-penalize-for-using-and-promoting-vpn-services [Online; accessed 16. Apr. 2019].
[8] 2019. App Store, iTunes Store, and Apple Books availability. https://support.apple.com/en-us/HT204411 [Online; accessed 16. Apr. 2019].
[9] 2019. AppInChina Chinese App Store Rankings - AppInChina | The Market. https://www.appinchina.co/market/app-stores [Online; accessed 16. Apr. 2019].
[10] 2019. China will block all non-approved VPNs from next month. https://www.techradar.com/news/china-will-block-all-non-approved-vpns-from-next-month [Online; accessed 16. Apr. 2019].
[11] 2019. hack66/appavail. https://github.com/hack66/appavail [Online; accessed 16. Apr. 2019].
[12] 2019. iTunes Search API - Affiliate Resources. https://affiliate.itunes.apple.com/resources/documentation/itunes-store-web-service-search-api/#searchexamples [Online; accessed 16. Apr. 2019].
[13] 2019. LinkedIn - AppAddict. https://www.appaddict.org/view.php?trackid=288429040 [Online; accessed 16. Apr. 2019].
[14] 2019. LinkedIn 4.1.249 Download APK for Android - Aptoide. https://linkedin-android.en.aptoide.com [Online; accessed 16. Apr. 2019].
[15] 2019. Not Found. http://web.archive.org/web/20190313183244/https://play.google.com/store/apps/details?id=com.linkedin.android&gl=ru [Online; accessed 16. Apr. 2019].
[16] 2019. Russia to Fine Search Engines for Linking to Banned VPN services. https://thehackernews.com/2018/06/russian-vpn-services.html [Online; accessed 16. Apr. 2019].
[17] 2019. Russian telecom watchdog blocks 50 VPN services and anonymizers for Telegram access. http://tass.com/economy/1002762 [Online; accessed 16. Apr. 2019].
[18] 2019. Supported locations for distribution to Google Play users - Play Console Help. https://support.google.com/googleplay/android-developer/table/3541286 [Online; accessed 16. Apr. 2019].
[19] 2019. Tencent xn–r70as2s - Terms of Service. https://www.tencent.com/en-us/zc/termsofservice.shtml [Online; accessed 16. Apr. 2019].
[20] 2019. Welcome to Steam. https://store.steampowered.com [Online; accessed 16. Apr. 2019].
[21] 2019. What is Russia's new VPN law all about? https://www.bbc.com/news/technology-41829726 [Online; accessed 16. Apr. 2019].
[22] 2019. xn–kbtj09tu77awtl. https://android.myapp.com [Online; accessed 16. Apr. 2019].
[23] 2019. Федеральный закон от 29.07.2017 № 276-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации". http://publication.pravo.gov.ru/Document/View/0001201707300002?index=14&rangeSize=1 [Online; accessed 16. Apr. 2019].
[24] 2019. 中华人民共和国网络安全法. http://web.archive.org/web/20190331080839/http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm [Online; accessed 16. Apr. 2019].
[25] 2019. 工业和信息化部关于清理规范互联网网络接入服务市场的通知. http://www.miit.gov.cn/n1146290/n4388791/c5471946/content.html [Online; accessed 16. Apr. 2019].
[26] Urs-Vito Albrecht, Uta Hillebrand, and Ute von Jan. 2018. Relevance of trust marks and CE labels in German-language store descriptions of health apps: analysis. *JMIR mHealth and uHealth* 6, 4 (2018).
[27] Ashley Carman. 2018. Apple will start reporting government requests to remove apps from the App Store. *Verge* (May 2018). https://www.theverge.com/2018/5/25/17396512/apple-transparency-report-app-takedown-requests
[28] Ning Chen, Jialiu Lin, Steven C. H. Hoi, Xiaokui Xiao, and Boshen Zhang. 2014. AR-miner: Mining Informative Reviews for Developers from Mobile App Marketplace. In *Proceedings of the 36th International Conference on Software Engineering (ICSE 2014)*. ACM, New York, NY, USA, 767–778. https://doi.org/10.1145/2568225.2568263
[29] Arturo Filastò and Jacob Appelbaum. 2012. OONI: Open Observatory of Network Interference. In *Free and Open Communications on the Internet*. USENIX. https://www.usenix.org/system/files/conference/foci12/foci12-final12.pdf
[30] Bin Fu, Jialiu Lin, Lei Li, Christos Faloutsos, Jason Hong, and Norman Sadeh. 2013. Why people hate your app: Making sense of user feedback in a mobile app store. In *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 1276–1284.
[31] Ahmad Ghazawneh and Ola Henfridsson. 2015. A paradigmatic analysis of digital application marketplaces. *Journal of Information Technology* 30, 3 (2015), 198–208.
[32] Luis Hestres. 2013. App neutrality: Apple ' s app store and freedom of expression online. (2013).
[33] Nguyen Phong Hoang, Panagiotis Kintis, Manos Antonakakis, and Michalis Polychronakis. 2018. An Empirical Study of the I2P Anonymity Network and Its Censorship Resistance. In *Proceedings of the Internet Measurement Conference 2018 (IMC '18)*. ACM, New York, NY, USA, 379–392. https://doi.org/10.1145/3278532.3278565
[34] Sean Hollister. 2018. Russia bans Telegram encrypted messaging app. *CNET* (Apr 2018). https://www.cnet.com/news/russia-bans-telegram-encrypted-messaging-app
[35] Slinger Jansen and Ewoud Bloemendal. 2013. Defining App Stores: The Role of Curated Marketplaces in Software Ecosystems. In *Software Business. From Physical Products to Software Services and Solutions*, Georg Herzwurm and Tiziana Margaria (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 195–206.
[36] Soo Ling Lim, Peter J Bentley, Natalie Kanakam, Fuyuki Ishikawa, and Shinichi Honiden. 2015. Investigating country differences in mobile app user behavior and challenges for software engineering. *IEEE Transactions on Software Engineering* 41, 1 (2015), 40–64.
[37] Daithí Mac Síthigh. 2013. App law within: rights and regulation in the smartphone age. *International Journal of Law and Information Technology* 21, 2 (2013), 154–186.
[38] William Martin, Federica Sarro, Yue Jia, Yuanyuan Zhang, and Mark Harman. 2017. A survey of app store analysis for software engineering. *IEEE transactions on software engineering* 43, 9 (2017), 817–847.
[39] Simon Migliano. 2018. Free VPN Apps: Chinese Ownership, Secretive Companies & Weak Privacy. *Top10VPN* (Dec 2018). https://www.top10vpn.com/free-vpn-app-investigation
[40] Ella Peltonen, Eemil Lagerspetz, Jonatan Hamberg, Abhinav Mehrotra, Mirco Musolesi, Petteri Nurmi, and Sasu Tarkoma. 2018. The hidden image of mobile apps: geographic, demographic, and cultural factors in mobile usage. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services*. ACM, 10.
[41] Suranga Seneviratne, Aruna Seneviratne, Mohamed Ali Kaafar, Anirban Mahanti, and Prasant Mohapatra. 2015. Early detection of spam mobile apps. In *Proceedings of the 24th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 949–959.
[42] Chongbin Tang, Sen Chen, Lingling Fan, Lihua Xu, Yang Liu, Zhushou Tang, and Liang Dou. 2019. A Large-Scale Empirical Study on Industrial Fake Apps. *CoRR* abs/1902.00647 (2019). arXiv:1902.00647 http://arxiv.org/abs/1902.00647
[43] Haoyu Wang, Zhe Liu, Jingyue Liang, Narseo Vallina-Rodriguez, Yao Guo, Li Li, Juan Tapiador, Jingcun Cao, and Guoai Xu. 2018. Beyond Google Play: A Large-Scale Comparative Study of Chinese Android App Markets. In *Proceedings of the Internet Measurement Conference 2018 (IMC '18)*. ACM, New York, NY, USA, 293–307. https://doi.org/10.1145/3278532.3278558