2019 MOBILE ADVERTISING SUPPLY CHAIN SAFETY REPORT

A risk analysis of:

- Fraud & Brand Safety
- Consumer Privacy
- National Security

SERIES 1: THE GOOGLE PLAY STORE

pixalate

TABLE OF CONTENTS

EXECUTIVE SUMMARY

MOBILE SUPPLY CHAIN SAFETY

Consumers spend nearly 3 hours per day on mobile apps[a], and this constant activity attracts **big money** from advertisers: **Per eMarketer, over $100 billion will be spent on mobile in-app advertising in 2020[b].**

Our mobile advertising supply chain safety report series will **deep-dive into the risks** — including **advertiser**, **consumer**, and **national security** risks — that stem from the mobile app ecosystem. Our first report is a risk analysis regarding apps on the **Google Play Store**, which is the **world's biggest app store**[c] with **over 3 million** apps.

THE EVOLUTION OF RISK

Today's advertisers are not only tasked with **protecting budgets** from **deceptive practices**, they must also navigate the complex web of **international relations**, including **economical** and **cyberwarfare**.

The U.S. government's opening of a **national security review** on TikTok[d] — and the FBI's announcement that mobile apps from Russia are treated as "**potential counterintelligence threats**"[e] — underscore the new frontier facing advertisers.

- Pixalate

KEY TAKEAWAYS

Google Play Store Stats

Scale: ~**500k**[1] of 3.2m+[2] Play Store apps **support programmatic**

Delisted: >**890k apps**[2] **removed** from the store through Q3'19

Ad spend: ~5% of Q3 global **ad transactions**[3] went to delisted apps[4]

Advertiser Risk

Brand Safety: ~33% of ad transactions[3] go to **brand-unsafe apps**[5]

Ad fraud: >**25%** of Android ad transactions[1] are **invalid traffic** (IVT[6])

Chinese apps: Highest (~33%) IVT on China-registered[7] apps*

Consumer Privacy Risk

Permissions: ~80% of top U.S. apps[8] have "**dangerous permissions**"[9]

Privacy policies: ~12% of all Play Store apps have **no privacy policy**[10]

Children at risk: Over 80% of top U.S. apps **can reach children**[11]

National Security Risk

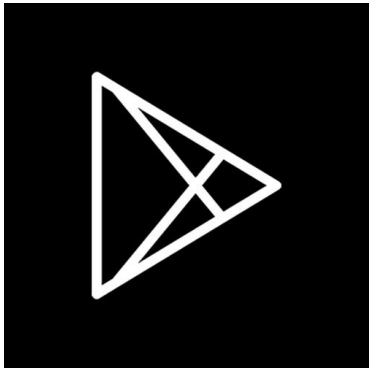
Registration[12]: Up to 72% of top U.S. apps are **registered** out of U.S.

China & Russia: ~14% of top apps are registered in **China** or **Russia**

Shell companies: Apps from **traditional shell locations**[13] up 12%

* Figure displays U.S. traffic IVT rates on China-registered[7] apps.

SECTION 1: GOOGLE PLAY STORE STATS



Google Play Store

Scale

Programmatic Apps

Delisted Apps

Advertiser Risk

Brand Safety

Ad Fraud (IVT[6])

Compliance

Consumer Privacy

Transparency

Child Privacy

“Dangerous Permissions”

National Security

Registration Information

“Dangerous Permissions”

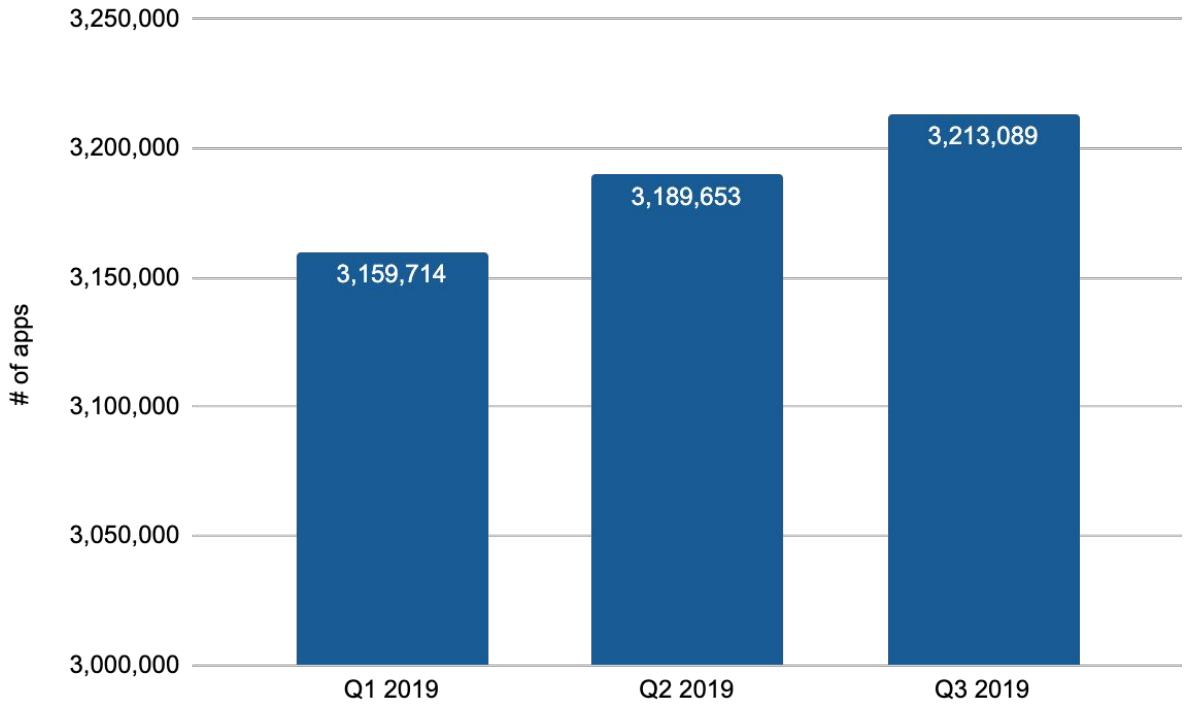
Delisted Apps

OVER 3.2 MILLION APPS ON THE GOOGLE PLAY STORE

Q1-Q3 2019.

3.2M

There are **3.2 million+ apps**[2] on the Google Play Store

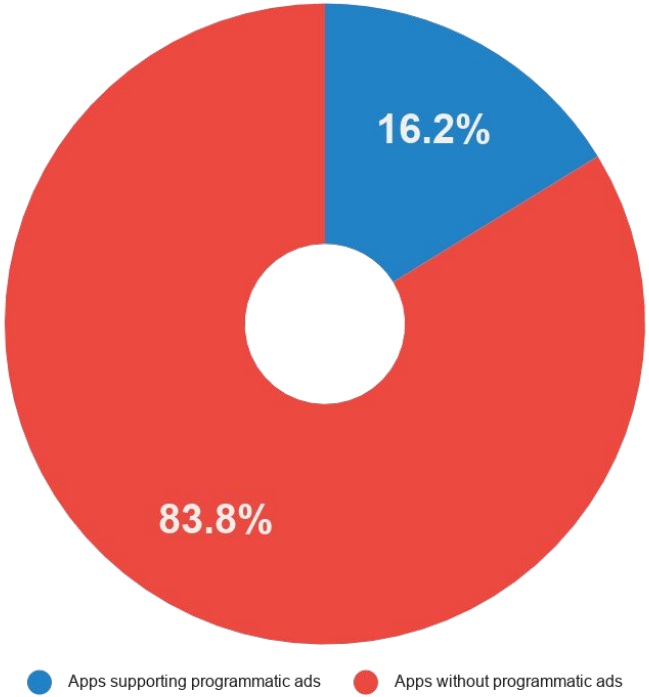


~500K GOOGLE PLAY STORE APPS SUPPORT PROGRAMMATIC

Q3 2019.

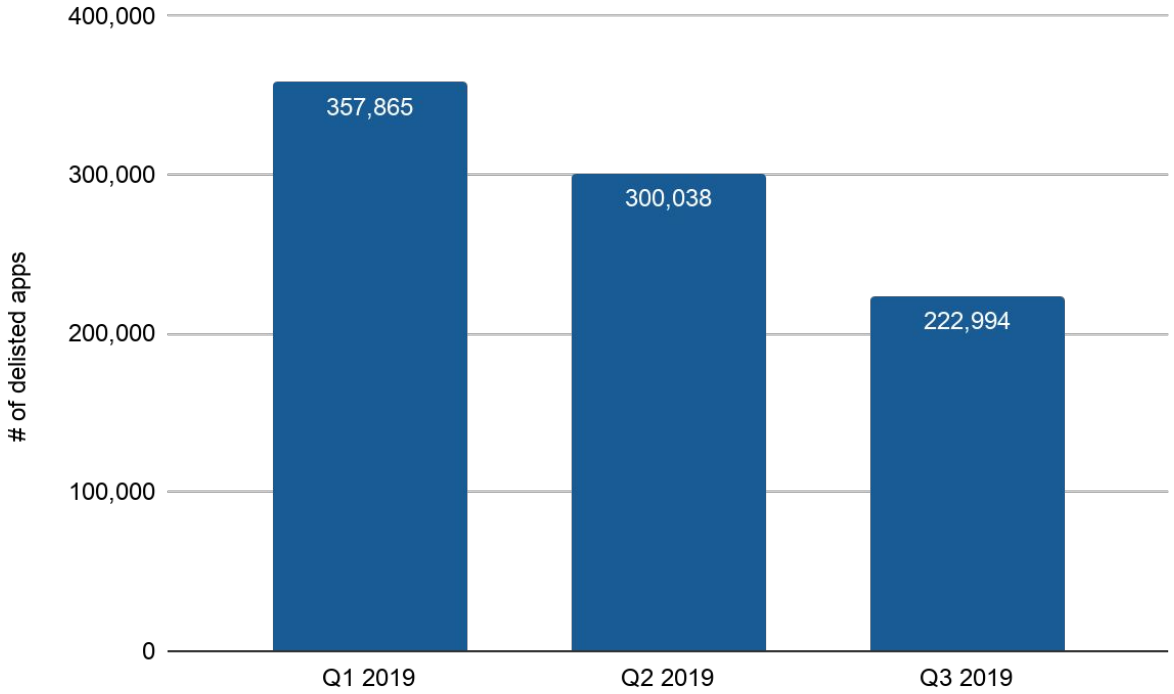
16%

of the **3.2 million+ apps**[2] on the Google Play Store support **programmatic advertising**[1]



881K APPS DELISTED THROUGH Q3 2019 (~9% CHURN PER QUARTER)

Q1-Q3 2019.



881k

Over 880k apps delisted[4] through Q3 2019

~9%

of the Play Store ecosystem churned per quarter

DELISTED APPS HAD 18 BILLION+ COMBINED DOWNLOADS

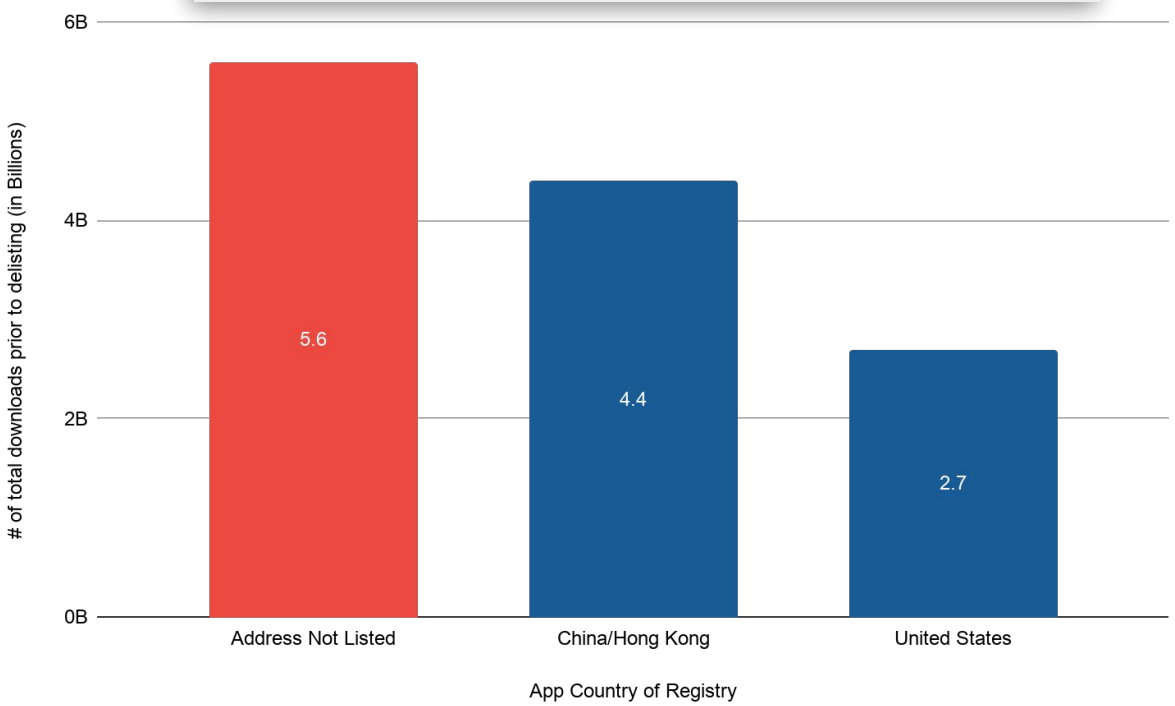
Q1-Q3 2019. DOWNLOAD NUMBERS AS OF THE LAST DATE EACH APP WAS LISTED IN THE GOOGLE PLAY STORE.

5.6B

The number of downloads[14] for apps **registered with no address** before those apps were delisted[4]

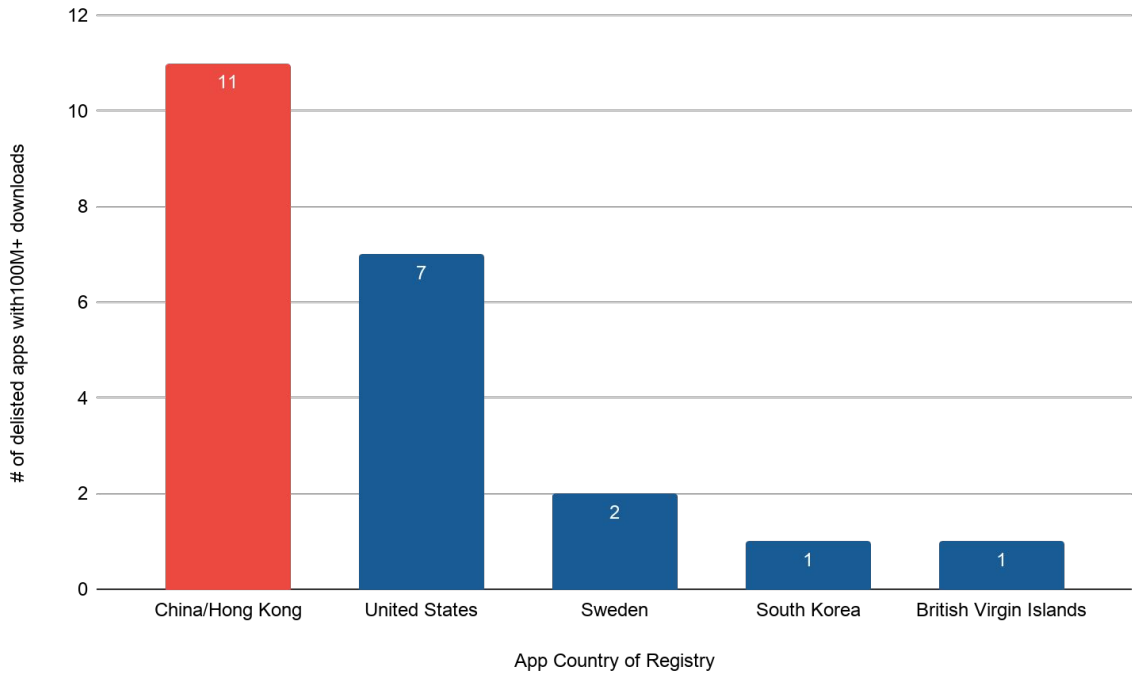
See the list of the top 100 delisted apps based on downloads here: https://pixal.at/delisted-apps

Which country's delisted apps had the most downloads? (in Billions)



50% OF DELISTED APPS WITH >100M+ DOWNLOADS WERE CHINESE

Q1-Q3 2019. DOWNLOAD NUMBERS AS OF THE LAST DATE EACH APP WAS LISTED IN THE GOOGLE PLAY STORE.



50%

of delisted apps[4] with 100M+ downloads[14] were **registered in China**[7]

See the list of the top 100 delisted apps based on downloads here: https://pixal.at/delisted-apps

DELISTED APPS THAT HAD 100M+ DOWNLOADS

Q1-Q3 2019. DOWNLOAD NUMBERS AS OF THE LAST DATE EACH APP WAS LISTED IN THE GOOGLE PLAY STORE.

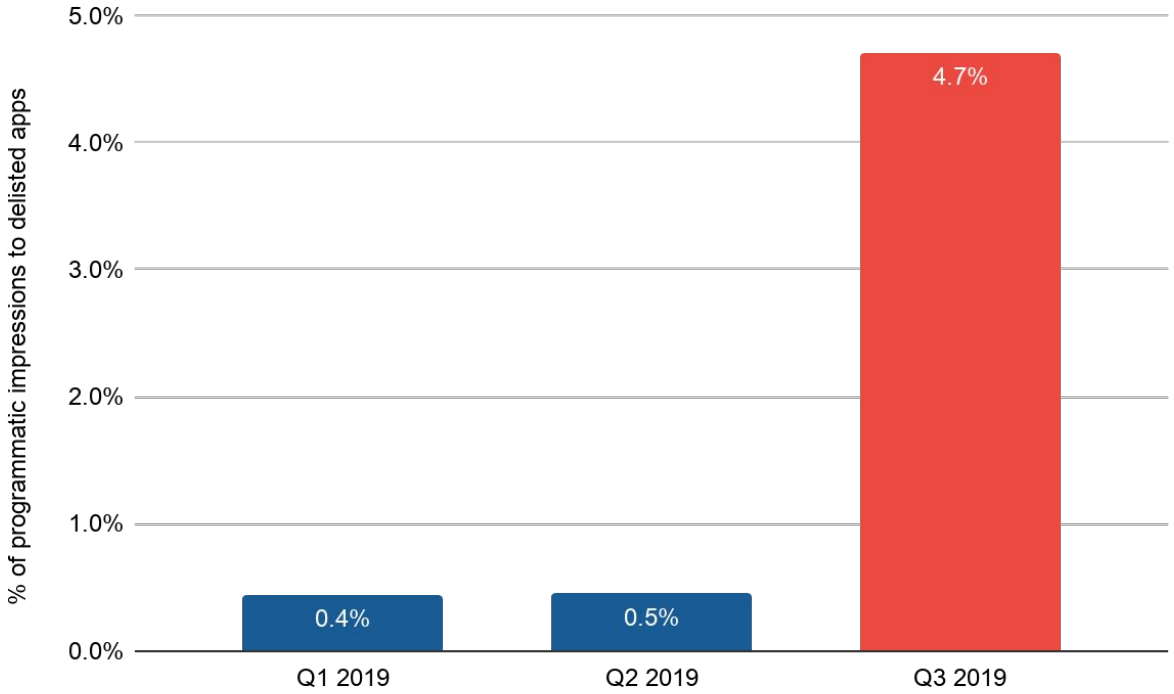
Note: Includes apps delisted as of 9/30/19; apps could have been added back to the Play Store after this date.

See the list of the top 100 delisted apps based on downloads here: https://pixal.at/delisted-apps

Country of Registry	App Title	Developer	Downloads
South Korea	Link Sharing	Samsung Electronics Co., Ltd.	500M+
Hong Kong (China)	Super-Bright LED Flashlight	ONE App Essentials.	500M+
China	TouchPal Emoji Keyboard: AvatarMoji, 3DTheme, GIFs	TouchPal Emoji Keyboard Team	100M+
China	TouchPal Keyboard-Cute Emoji,theme, sticker, GIFs	TouchPal	100M+
Sweden	Sketch - Draw & Paint	Sony Mobile Communications	100M+
Sweden	Xperia Lounge	Sony Mobile Communications	100M+
China	DU Recorder ‚Äì Screen Recorder, Video Editor, Live	Screen Recorder & Video Editor	100M+
United States	Peel Universal Smart TV Remote Control	Peel Technologies Inc.	100M+
United States	Peel Smart Remote	Peel Technologies	100M+
United States	Peel Smart Remote TV Guide	Peel Technologies	100M+
China	Master for Minecraft(Pocket Edition)-Mod Launcher	Nimo TV	100M+
British Virgin Islands	4shared	New IT Solutions	100M+
United States	Motorola Update Services	Motorola Mobility LLC.	100M+
Hong Kong (China)	Power Clean - Antivirus & Phone Cleaner App	LIONMOBI	100M+
United States	Private Zone - AppLock, Video & Photo Vault	Leomaster(AppLock & Privacy)	100M+
China	Hola Launcher- Theme,Wallpaper	Holaverse	100M+
United States	MARVEL Spider-Man Unlimited	Gameloft	100M+
China	PIP Camera-Photo Editor Pro	Fotoable,Inc.	100M+
Hong Kong (China)	DU Battery Saver - Battery Charger & Battery Life	DU APPS STUDIO - BATTERY&BOOSTER	100M+
Hong Kong (China)	Cache Cleaner-DU Speed Booster (booster & cleaner)	DU APPS STUDIO - BATTERY&BOOSTER	100M+
United States	Where's My Water? Free	Disney	100M+
United States	SuperSU	Codingcode	100M+

~5% OF IN-APP AD IMPRESSIONS[3] WENT TO DELISTED APPS

Q1-Q3 2019. MOBILE IN-APP PROGRAMMATIC AD IMPRESSIONS DELIVERED TO DELISTED GOOGLE PLAY STORE APPS, AS MEASURED BY PIXALATE.



5%

of Q3 2019 **programmatic ad transactions**[1] went **to delisted apps**[4], as measured by Pixalate

WHY THE JUMP IN Q3?

Google removed over 230 apps associated with the BeiTads adware discovery[f] in late Q2, and several of those apps continued to receive programmatic ads into Q3.

TOP 10 DELISTED APPS THAT CONTINUED TO RECEIVE ADS[3]

Q1-Q3 2019. APPS THAT CONTINUED TO RECEIVE PROGRAMMATIC ADS AFTER BEING DELISTED, RANKED BY GLOBAL IMPRESSIONS[3] POST-DELISTING, AS MEASURED BY PIXALATE.

App Icon	App Country of Registry	App Name	Developer	Category	Downloads
	Address Not Listed	Coreader- QR Code & Barcode Scanner	Micky Group	Entertainment	10M+
	Address Not Listed	Phone Color Screen - Colorful Call Flash Themes	Mahakal Studio	Personalization	50M+
	Hong Kong (China)	DailyFit	ZJB Group	Health & Fitness	50K+
	Address Not Listed	Messenger for Social App	Mahakal Studio	Social	5M+
	China	Easy Pedometer	Life Assistant Tech Group	Social	1M+
	China	Brightest Flash LED Lights	Flashlight Group	Productivity	10M+
	China	HealthFit - Abs Workout with No Equipment Needed	Meotty Group	Health & Fitness	1M+
	Address Not Listed	Horoscope Prediction - Zodiac Signs Astrology	Moxi Studio	Lifestyle	5M+
	China (Hong Kong)	Period Tracker Dora - Menstrual Calendar	YY Huang	Social	1M+
	China	TouchPal Emoji Keyboard: AvatarMoji, 3DTheme, GIFs	TouchPal Emoji Keyboard Team	Personalization	100M+

Note: Includes apps delisted as of 9/30/19; apps could have been added back to the Play Store after this date.

SECTION 2: ADVERTISER RISK

Advertiser Risk

Brand Safety

Ad Fraud (IVT[6])

Compliance

Google Play Store

Scale

Programmatic Apps

Delisted Apps

Consumer Privacy

Transparency

Child Privacy

“Dangerous Permissions”

National Security

Registration Information

“Dangerous Permissions”

Delisted Apps

~32% OF ADS[1] APPEAR NEXT TO POSSIBLY OBJECTIONABLE CONTENT[5]

Q1-Q3 2019. MOBILE IN-APP PROGRAMMATIC AD IMPRESSIONS DELIVERED TO GOOGLE PLAY STORE APPS, AS MEASURED BY PIXALATE.

31k apps* have **potentially brand-unsafe advisories**[5] and accounted for

32%

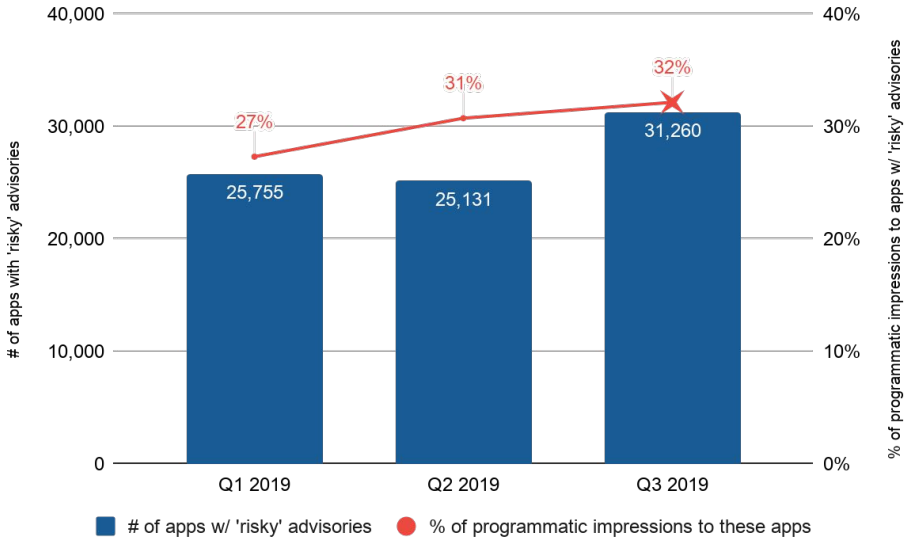
of global Q3 2019 programmatic impressions[1]

Including apps with...

*!#@ **Profanity**

Violence

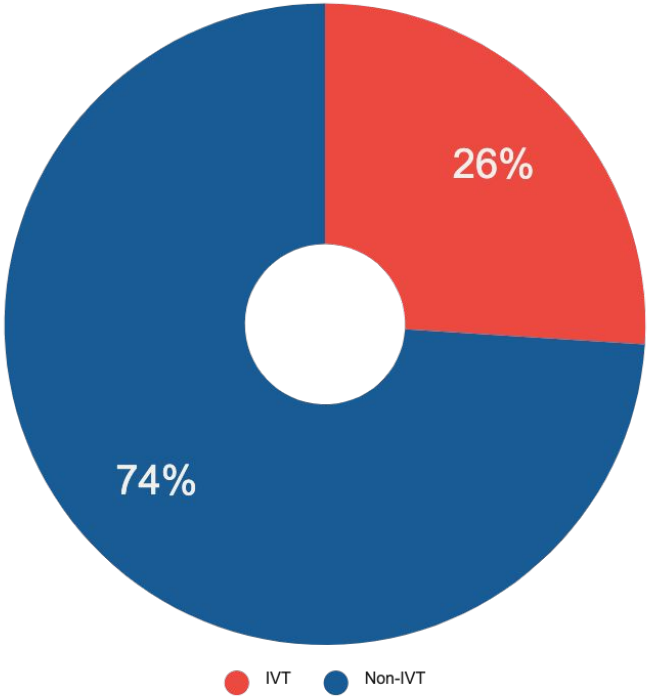
Mature Content



* Apps that support programmatic advertising, as measured by Pixalate.

AD FRAUD (IVT) RATE: OVER 25% OF ANDROID ADS[3] ARE INVALID

Q3 2019. INCLUDES DISPLAY AND VIDEO PROGRAMMATIC ADVERTISING. INVALID TRAFFIC (IVT) MEASURED BY PIXALATE. GLOBAL.

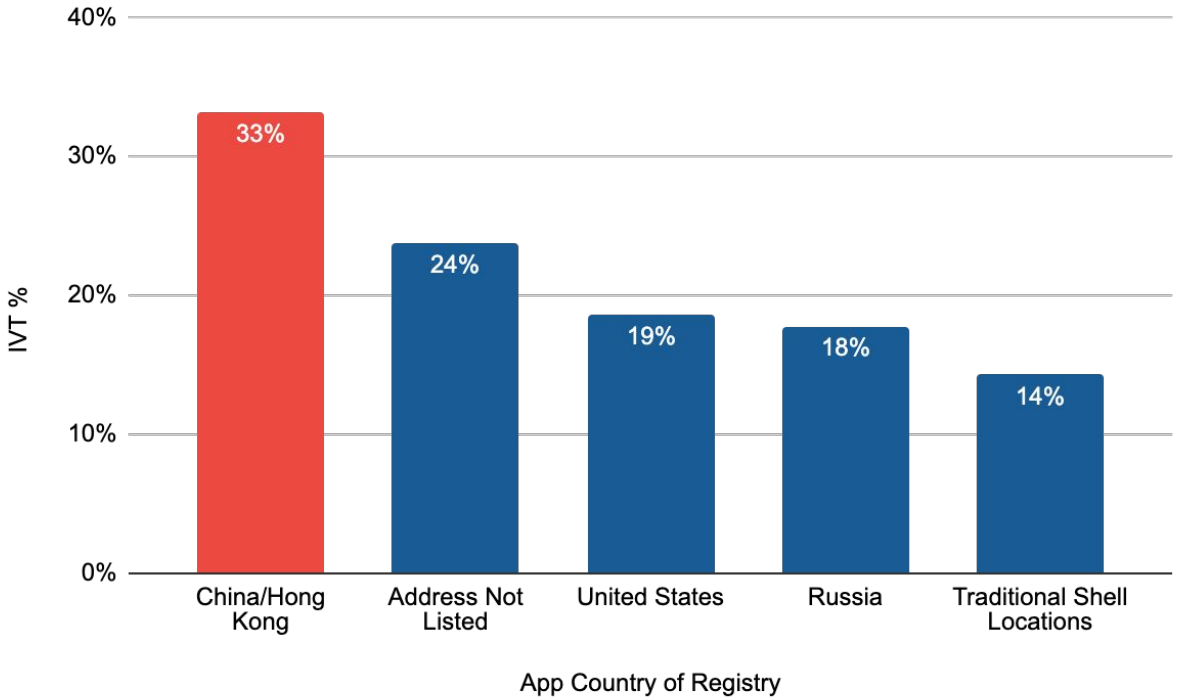


26%

the global **ad fraud** (IVT[6]) rate of programmatic mobile in-app advertising on Android devices, as measured by Pixalate

AD FRAUD BY COUNTRY: CHINESE APPS HAD HIGHEST IVT RATE (33%)

Q1-Q3 2019. INCLUDES DISPLAY AND VIDEO PROGRAMMATIC ADVERTISING. U.S. TRAFFIC. INVALID TRAFFIC (IVT) MEASURED BY PIXALATE.



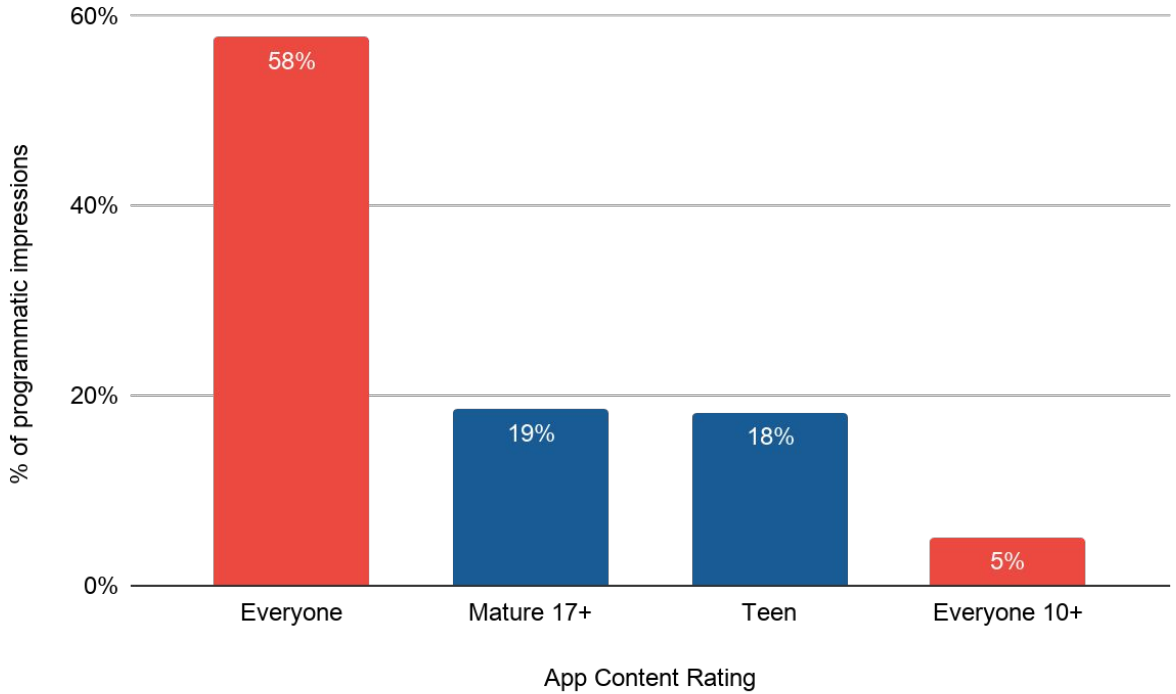
33%

programmatic **ad fraud** (IVT[6]) rate on **China-registered[7] apps***, as measured by Pixalate

* Chart displays U.S. traffic IVT rates by app country of registry.

63% OF ADS[1] WENT TO APPS THAT CAN REACH CHILDREN

Q1-Q3 2019. GLOBAL. INCLUDES DISPLAY AND VIDEO PROGRAMMATIC ADVERTISING. U.S. TRAFFIC. MEASURED BY PIXALATE.



63%

of global impressions[1] went to apps with **'Everyone'** content ratings, meaning they **can reach children**[11]

SECTION 3: CONSUMER PRIVACY RISK

Google Play Store

Scale

Programmatic Apps

Delisted Apps

Advertiser Risk

Brand Safety

Ad Fraud (IVT[6])

Compliance

Consumer Privacy

Transparency

Child Privacy

“Dangerous Permissions”

National Security

Registration Information

“Dangerous Permissions”

Delisted Apps

12% OF PLAY STORE APPS MIGHT NOT BE GDPR COMPLIANT

Q3 2019.

12%

of all apps appear to have no **privacy policy**[10]

1.4%

of programmatic-supporting apps appear to have no **privacy policy**[15]

70%

are registered to **non-corporate emails**[15]

17%

appear not to have **Terms of Service**[15]

9%

have **private registration** information[15]

GDPR & OTHER LAWS

GDPR Chapter 3[9] requires that privacy notices explain the purpose(s) and legal basis for processing of personal information in a concise, transparent, intelligible and easily accessible form.

WHAT ARE 'DANGEROUS PERMISSIONS' IN THE GOOGLE PLAY STORE?

Per Google[h], **"dangerous permissions"**[9] "...cover areas where the app wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps."
There are a total of **30 "dangerous permissions."** Below are **examples**; see our methodology for the full list:

"Dangerous Permission"	Description
WRITE_EXTERNAL_STORAGE	Allows an application to write to external storage.
CAMERA	Required to be able to access the camera device.
CALL_PHONE	Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call.
BODY_SENSORS	Allows an application to access data from sensors that the user uses to measure what is happening inside his/her body, such as heart rate.
RECORD_AUDIO	Allows an application to record audio.
READ_CALENDAR	Allows an application to read the user's calendar data.
READ_CALL_LOG	Allows an application to read the user's call log.
READ_CONTACTS	Allows an application to read the user's contacts data.
WRITE_CALENDAR	Allows an application to write the user's calendar data.
WRITE_CONTACTS	Allows an application to write the user's contacts data.
READ_PHONE_STATE	Allows read only access to phone state, including the phone number of the device, current cellular network information, the status of any ongoing calls, and a list of any Phone Accounts registered on the device.
ANSWER_PHONE_CALLS	Allows the app to answer an incoming phone call.
ACCESS_FINE_LOCATION	Allows an app to access precise location.
ACCESS_COARSE_LOCATION	Allows an app to access approximate location.
ACCESS_BACKGROUND_LOCATION	Allows an app to access location in the background.

10 MOST COMMON 'DANGEROUS PERMISSIONS'

Q1-Q3 2019. AMONG THE TOP 10K APPS BASED ON PROGRAMMATIC AD VOLUME IN THE US, AS MEASURED BY PIXALATE.

"Dangerous Permission"[9]	% of top 10k U.S. apps[8] with this permission	Description
Write External Storage	71%	Grants access to save content to your phone without you knowing after granting permission
Read External Storage	57%	Grants access to see and identify files on your phone
Access Coarse Location	35%	Grants access to information passed by others apps, WiFi, cellular towers in order to approximate location
Access Fine Location	34%	Grants access to GPS information to find exact location
Read Phone State	31%	Grants read only access to phone state, including the phone number of the device, current cellular network information, the status of any ongoing calls, and more.
Camera	17%	Grants access to your camera
Get Accounts	18%	Grants access to the account type and username on the user's device and gives access to check which features are enabled on the account
Record Audio	11%	Grants access to microphone to record audio
Activity Recognition	7%	Grants access to identify body movement and general handling of the phone
Read Contacts	5%	Grants access to read contact information

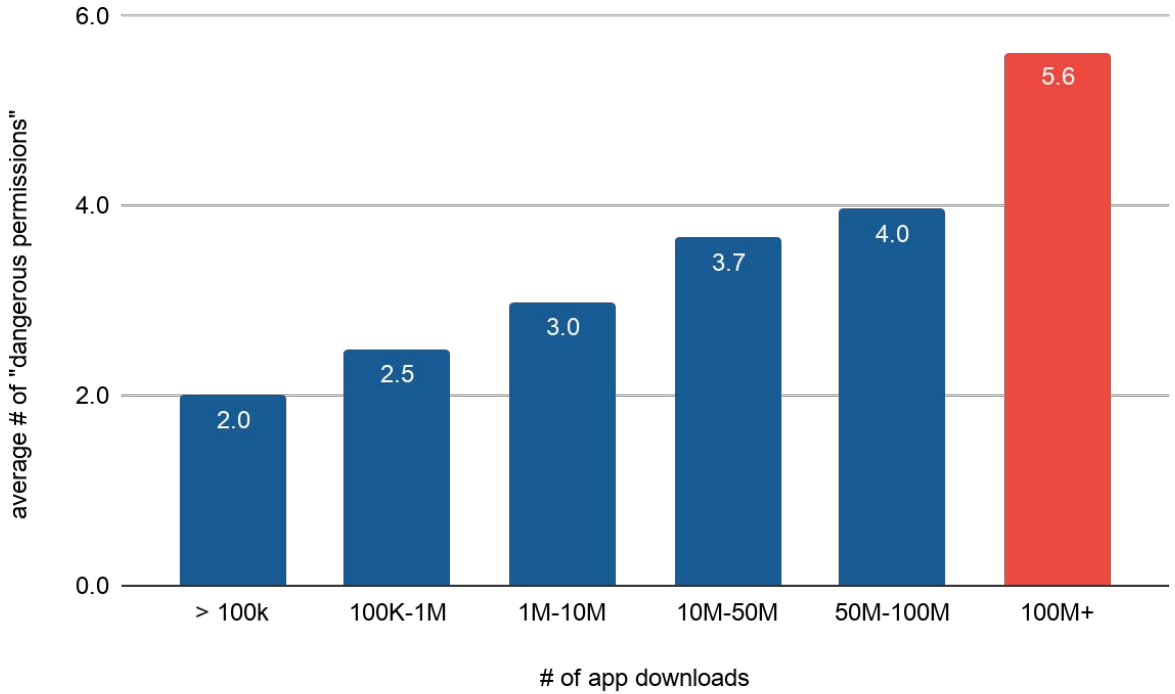
See our methodology for a full list of "dangerous permissions."

APPS WITH 100M+ DOWNLOADS HAD THE MOST 'DANGEROUS PERMISSIONS'

Q1-Q3 2019. DEPICTS AVERAGE # OF 'DANGEROUS PERMISSIONS' BY TOTAL APP DOWNLOADS (DOWNLOAD NUMBERS GROUPED)[2].

5.6

the average number of "**dangerous permissions**"[9] on apps with **100M+ downloads**[16]



See our methodology for a full list of "dangerous permissions."

'Dangerous Permissions'

>80% OF TOP US APPS[8] HAVE 'DANGEROUS PERMISSIONS'

Q1-Q3 2019. 'TOP APPS' REFERS TO TOP 10K GOOGLE PLAY STORE APPS BASED ON PROGRAMMATIC AD VOLUME, AS MEASURED BY PIXALATE.

81%

of the top 10k apps[8] in the U.S. have at least one "**dangerous permission**"[9]

"**Dangerous permissions**" include apps that can access user's personal data, including:

- Camera
- Microphone
- GPS coordinates

See our methodology for a full list of "dangerous permissions."

>80% OF TOP US APPS[8] CAN REACH CHILDREN

Q1-Q3 2019. 'TOP APPS' REFERS TO TOP 10K GOOGLE PLAY STORE APPS BASED ON PROGRAMMATIC AD VOLUME, AS MEASURED BY PIXALATE.

83%

of the top 10k apps[8] in the U.S. **can reach children**[11]

Among the top 10k apps, these are the **app categories** with the most apps that **can reach children**:

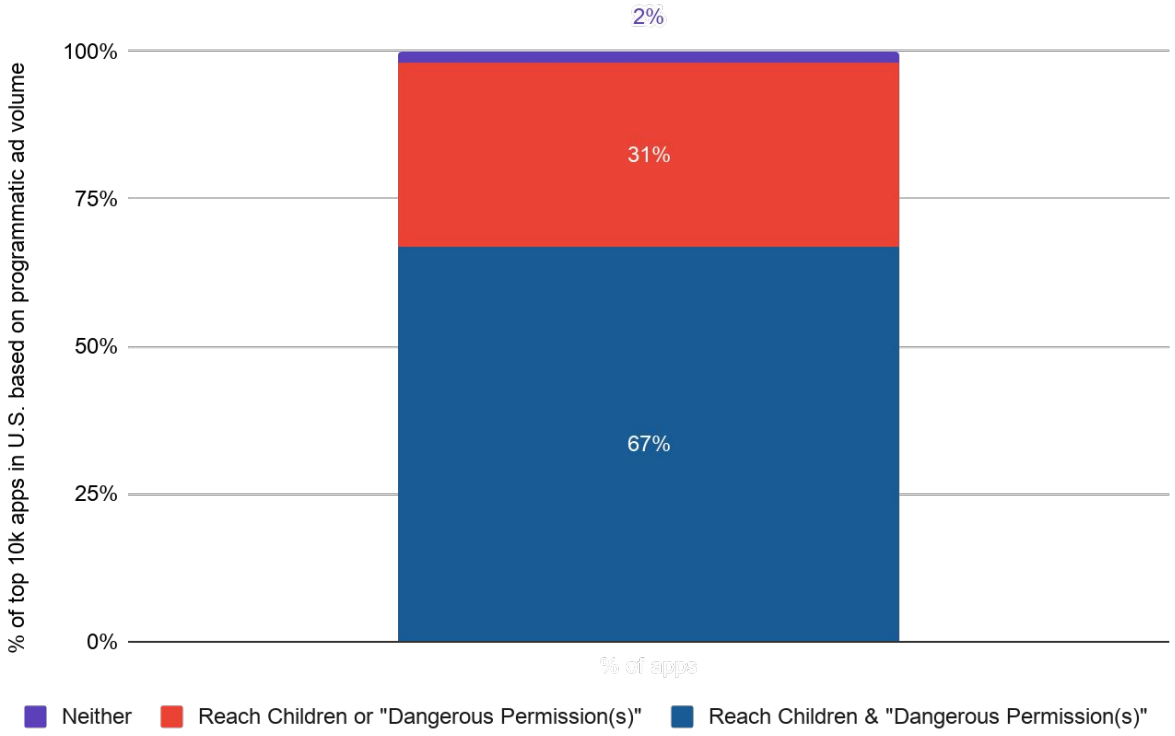
- Games
- News & Magazines
- Tools

TOP APPS[8]: 67% CAN REACH CHILDREN & HAVE 'DANGEROUS PERMISSIONS'

Q1-Q3 2019. 'TOP APPS' REFERS TO TOP 10K GOOGLE PLAY STORE APPS BASED ON PROGRAMMATIC AD VOLUME, AS MEASURED BY PIXALATE.

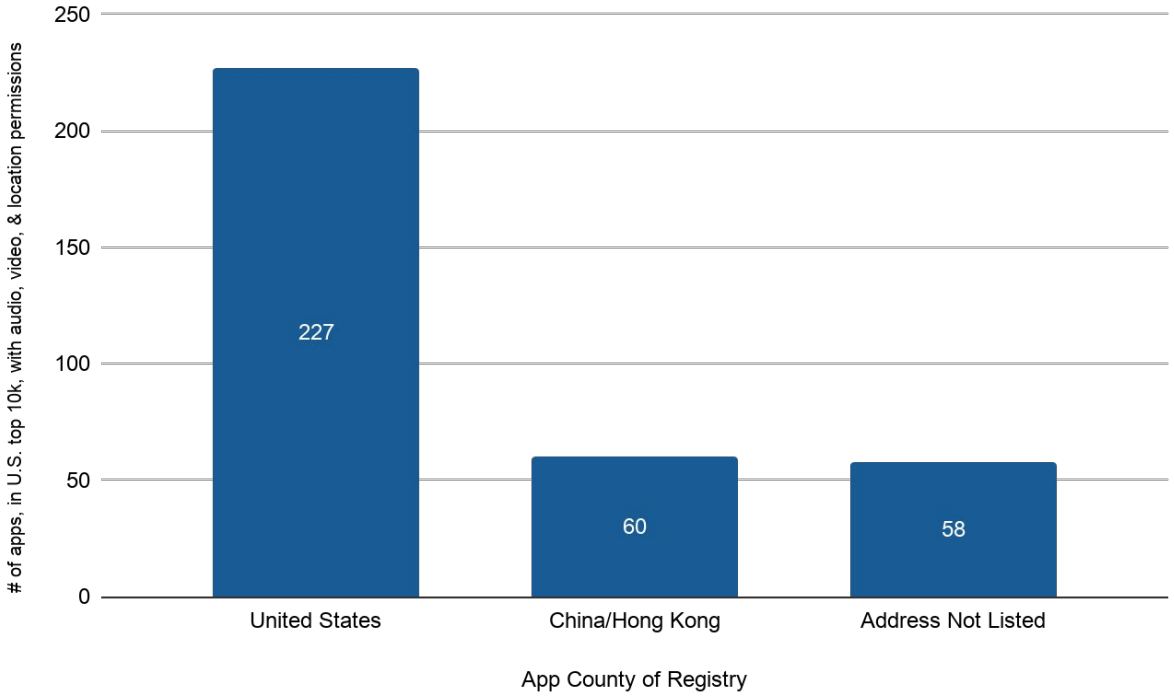
67%

of top U.S. apps can **reach children**[11] and have at least one "**dangerous permission**"[9]



419 TOP APPS[4] CAN REACH CHILDREN & ACCESS CAMERA, AUDIO, GPS

Q1-Q3 2019. 'TOP APPS' REFERS TO TOP 10K GOOGLE PLAY STORE APPS BASED ON PROGRAMMATIC AD VOLUME, AS MEASURED BY PIXALATE.



419

of top U.S. apps can **reach children**[11] & have **all** of the following dangerous permissions[9]:

- Camera Access
- Microphone Access
- Precise Location Access

118 of these apps are registered in **China**[7] or have **no address listed**

SECTION 4: NATIONAL SECURITY RISK

Google Play Store

Scale

Programmatic Apps

Delisted Apps

Advertiser Risk

Brand Safety

Ad Fraud (IVT[6])

Compliance

Consumer Privacy

Transparency

Child Privacy

“Dangerous Permissions”

National Security

Registration Information

“Dangerous Permissions”

Delisted Apps

TOP APPS[8] TARGETING U.S. ARE FROM CHINA, S. KOREA, RUSSIA

Q1-Q3 2019. DEPICTS COUNTRY OF REGISTRY BREAKDOWN OF TOP 10K U.S. APPS[4]

72%

Up to 72% of the top 10k apps[8] in the U.S. **are registered outside of the U.S.** or in unknown locations*[12]

10 most common countries of app registration outside of the U.S.*

22%	11%	3%	3%	3%
Address not listed*	China[7]	South Korea	Russia	France
3%	**3%**	**2%**	**2%**	**2%**
United Kingdom	Canada	Traditional Shell Locations[13]	India	Israel

* Apps registered with no address could be from anywhere, including the U.S.

"Dangerous Permissions"

>80% OF TOP[8] US, CHINESE, RUSSIAN APPS HAVE 'DANGEROUS PERMISSIONS'

Q1-Q3 2019. % OF TOP 10K U.S. APPS[8], BY COUNTRY OF REGISTRY, WITH "DANGEROUS PERMISSIONS"[9]. MINIMUM 100 APPS REGISTERED PER COUNTRY TO BE LISTED.

ANY DANGEROUS PERMISSION


USA: 89%


CHINA[7]: 87%


INDIA: 84%


CANADA: 82%


NO ADDRESS: 82%


RUSSIA: 81%


UK: 75%


ISRAEL: 70%

ACCESS CAMERA


CHINA[7]: 28%


USA: 22%


GERMANY: 17%

RECORD AUDIO


INDIA: 16%


USA: 15%


CHINA[7]: 14%

ACCESS PRECISE LOCATION


USA: 53%


CANADA: 40%


NO ADDRESS: 36%

WRITE EXTERNAL STORAGE


CHINA[7]: 82%


USA: 75%


RUSSIA: 75%

Countries represent country of app registration.

CHINESE[7] APPS: TOP 10 WITH MOST 'DANGEROUS PERMISSIONS'

AMONG APPS IN THE TOP 10K[8] BASED Q1-Q3 2019 PROGRAMMATIC AD VOLUME IN THE US, AS MEASURED BY PIXALATE,

App Icon	Country of Registry	App Name	Developer	Category	Downloads	'Dangerous Permissions'
	Hong Kong (China)	Parallel Space - Multiple accounts & Two face	LBE Tech	Personalization	100M+	24
	China	CM Launcher 3D - Themes, Wallpapers	Cheetah Mobile Inc	Personalization	100M+	19
	China	GO SMS Pro - Messenger, Free Themes, Emoji	GOMO Apps	Communication	100M+	18
	China	Security Master - Antivirus, VPN, AppLock, Booster	Cheetah Mobile (AppLock & AntiVirus)	Tools	500M+	17
	China	Dual Space - Multiple Accounts & App Cloner	SUPERLITE	Tools	100M+	17
	China	Dual Space - Multi Accounts & Fresh Blue Theme	SUPERLITE	Personalization	5M+	17
	China	Dual Space Lite - Multiple Accounts & Clone App	SUPERLITE	Tools	10M+	17
	Hong Kong (China)	Vault - Hide Pics & Videos, App Lock, Free Backup	cxzh.ltd	Business	50M+	16
	China	APUS Message Center,ÄîIntelligent management	APUS Group	Tools	10M+	15
	China	Alarm Clock & Themes - Stopwatch, Timer, Calendar	GOMO	Health & Fitness	5M+	14

See the top 100 apps registered in China[7]
with the most downloads: https://pixal.at/popular-chinese-apps

DELISTED CHINESE[6] APPS: 37% MORE ACCESS TO 'READ PHONE STATE'

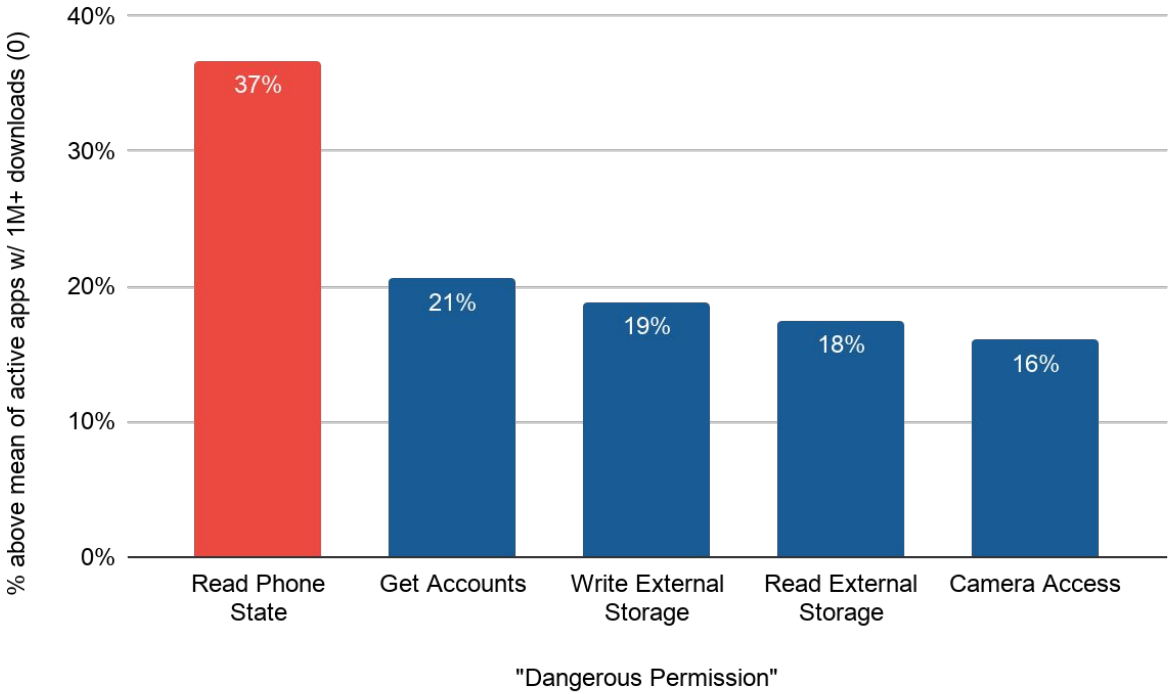
Q1-Q3 2019. COMPARES RATE OF PERMISSIONS GRANTED TO DELISTED APPS WITH 1M+ DOWNLOADS VERSUS ACTIVE APPS WITH 1M+ DOWNLOADS.

37%

popular* delisted apps[4] from **China**[7] had 37% more access to the '**Read Phone State**' permission than non-delisted apps of equal popularity

WHAT IS READ PHONE STATE?

This permission allows the app to see the phone number of the device, current cell network information, the status of any ongoing calls, & more[e].



* Apps with 1M+ downloads

RUSSIAN APPS: TOP 10 WITH MOST 'DANGEROUS PERMISSIONS'

AMONG APPS IN THE TOP 10K[8] BASED Q1-Q3 2019 PROGRAMMATIC AD VOLUME IN THE US, AS MEASURED BY PIXALATE

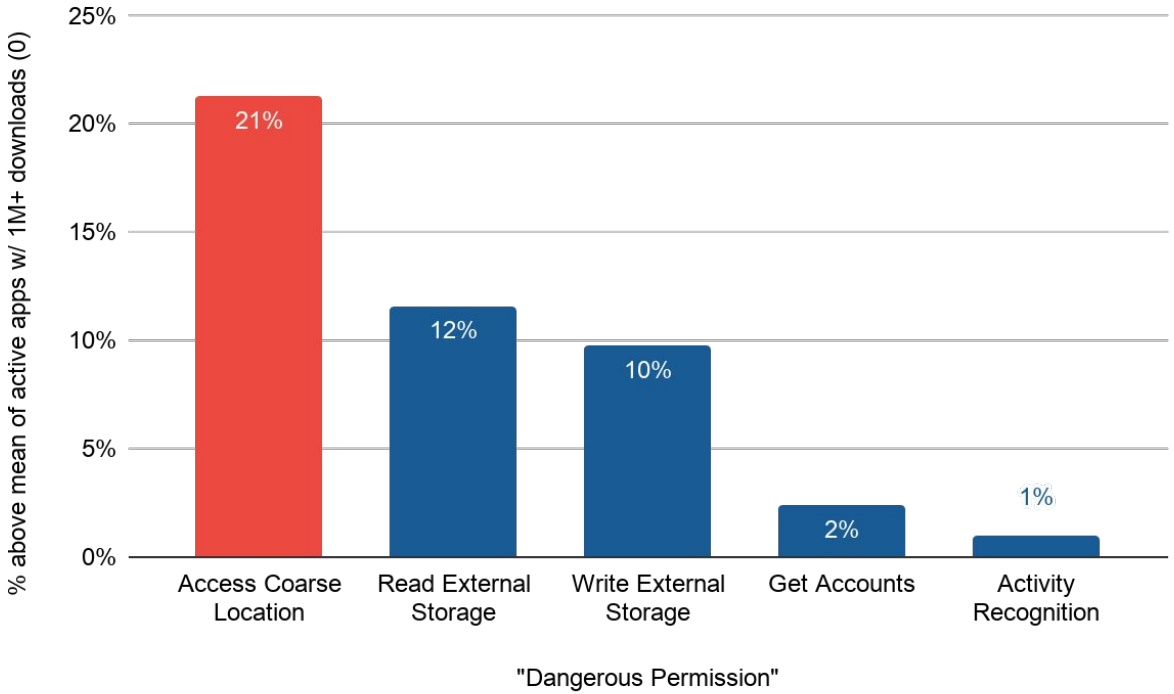
App Icon	Country of Registry	App Name	Developer	Category	Downloads	'Dangerous Permissions'
	Russia	OK	Odnoklassniki Ltd	Social	100M+	12
	Russia	Calls Blacklist - Call Blocker	Vlad Lee	Communication	10M+	9
	Russia	Pregnancy Tracker: Baby Due Date Calculator	Mobile Dimension LLC	Medical	1M+	8
	Russia	Undeleter Recover Files & Data	Fahrbot PRI	Tools	10M+	8
	Russia	Mobile Doc Scanner (MDScan) Lite	STOIK Soft	Business	1M+	7
	Russia	Tramp Simulator: Survival City	TaigaGames	Games	100K+	7
	Russia	Launcher Live Icons for Android	TSDC	Personalization	500K+	7
	Russia	Pregnancy Tracker week by week for pregnant moms	Pregnancy with Happy Mama photo - babysfera LLC*	Parenting	500K+	7
	Russia	Detectives - Free Books*	Heap of Books*	Books & Reference	500K+	6
	Russia	Voice notes - quick recording of ideas	gawk	Productivity	500K+	6

* Translation provided by Google Translate

See the top 100 apps registered in Russia with the most downloads: https://pixal.at/popular-russian-apps

DELISTED RUSSIA APPS: 21% MORE ACCESS TO 'COARSE LOCATION'

Q1-Q3 2019. COMPARES RATE OF PERMISSIONS GRANTED TO DELISTED APPS WITH 1M+ DOWNLOADS VERSUS ACTIVE APPS WITH 1M+ DOWNLOADS.



* Apps with 1M+ downloads

21%

popular* delisted apps[4] from **Russia** had 21% more access to the '**Access Coarse Location**' permission than non-delisted apps of equal popularity

WHAT IS COARSE LOCATION?

This permission allows the app access to the approximate location of the device.

SHELL[13] APPS: TOP 10 WITH MOST 'DANGEROUS PERMISSIONS'

AMONG APPS IN THE TOP 10K[8] BASED Q1-Q3 2019 PROGRAMMATIC AD VOLUME IN THE US, AS MEASURED BY PIXALATE

App Icon	Country of Registry	App Name	Developer	Category	Downloads	'Dangerous Permissions'
	Cyprus	Get new friends on local chat rooms	My Friends Social	Social	10M+	11
 *	British Virgin Islands	Cockroach Smasher Free Fun Game for Kids	Best Cool and Fun Games	Action	10M+	9
	British Virgin Islands	APUS File Manager (Explorer)	OneGogo	Tools	50M+	9
	Seychelles	Color Call-Phone Call Screen Theme, LED Flash	BuddyTech	Personalization	100K+	8
	Malta	⚽🏆FantaMaster Leghe & Guida Serie A 2019/2020	DigitalGoal Ltd	Games	500K+	8
	Seychelles	Super Flashlight - Brightest LED Light for Free	BuddyTech	Tools	500K+	7
	British Virgin Islands	Bunny Shooter Free Funny Archery Game	Best Cool and Fun Games	Games	10M+	7
	Cyprus	Downloader & Private Browser	Mirmay Limited	Tools	100M+	6
	Cyprus	Automatic Call Recorder	Appliqato	Tools	100M+	5
	Cyprus	3D Sense Clock & Weather	MACHAPP Software Ltd	Weather	500K+	5

* App removed from the Google Play Store on or after Oct. 1, 2019

See the top 100 apps registered in traditional shell locations with the most downloads: https://pixal.at/popular-shell-apps

DELISTED SHELL APPS: 18% MORE ACCESS TO 'WRITE EXTERNAL STORAGE'

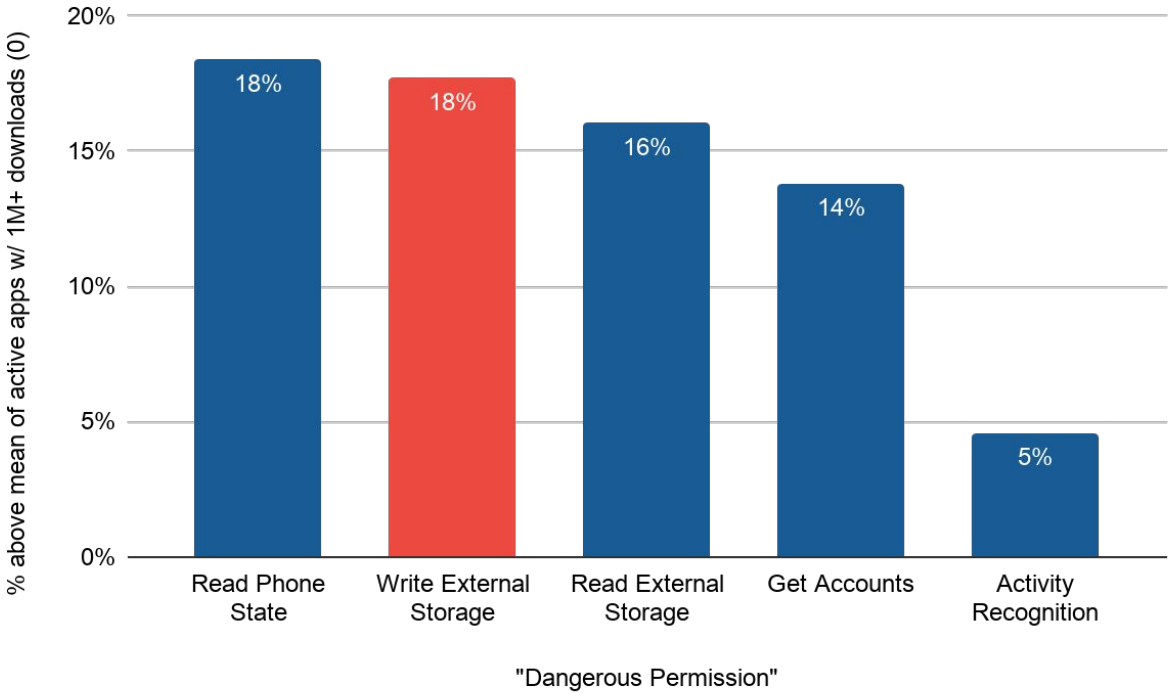
Q1-Q3 2019. COMPARES RATE OF PERMISSIONS GRANTED TO DELISTED APPS WITH 1M+ DOWNLOADS VERSUS ACTIVE APPS WITH 1M+ DOWNLOADS.

18%

popular* delisted apps[4] from **traditional shell locations**[13] had 18% more access to '**Write External Storage**' permissions than non-delisted apps of equal popularity

WHAT IS WRITE EXTERNAL STORAGE?

This permission allows the app to access & write to the phone's external storage, including reading, deleting, & saving files.



* Apps with 1M+ downloads

FAQs

WHY ARE YOU RELEASING THIS REPORT?

Pixalate's 2019 Mobile Advertising Supply Chain Safety Report brings transparency to a new frontier facing advertises, including ad fraud (IVT), brand safety, consumer privacy and data regulations, and economical and cyberwarfare.

WHY ARE YOU ANALYZING GOOGLE PLAY STORE APPS?

Pixalate's 2019 Mobile Advertising Supply Chain Safety Report is one in a series of ad supply chain intelligence analysis across various parts of the programmatic advertising ecosystem. Pixalate also recently released the H1 2019 OTT/CTV Supply Chain Intelligence Report featuring analysis on the state of the Connected TV (CTV) and over-the-top (OTT) ad supply chain.

WHAT IS A "DELISTED APP"?

An app is considered delisted if it existed in the Google Play Store in a given time period and then it was removed (either by Google or the app developer). For the purposes of this report, the time period included apps in the Google Play Store on or after January 1, 2019 but not on the Play Store as of September 30, 2019. Apps could have been added back to the Play Store after this date.

WHY ARE YOU HIGHLIGHTING APPS FROM CHINA, RUSSIA, & TRADITIONAL SHELL COMPANY LOCATIONS?

The U.S. government opened a national security review on TikTok, and the FBI announced that mobile apps from Russia are treated as "potential counterintelligence threats."

WHAT ARE 'DANGEROUS PERMISSIONS'?

According to Google's documentation: "The purpose of a permission is to protect the privacy of an Android user. Android apps must request permission to access sensitive user data (such as contacts and SMS), as well as certain system features (such as camera and internet)." Google adds: "Dangerous permissions cover areas where the app wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps." See our Methodology & Limitations for a full list of "dangerous permissions."

WHERE CAN I LEARN MORE?

Visit our website at https://www.pixalate.com to see more detailed lists regarding some of the most popular apps and the amount of dangerous permissions they have access to.

INDEX

1. As measured by Pixalate.

2. Data derived from crawls of the Play Store performed by Pixalate or one of Pixalate's third party licensors.

3. Refers to programmatic ad impressions, as measured by Pixalate.

4. Includes apps delisted on or after January 1, 2019 and not on the Google Play Store as of September 30, 2019. Apps delisted but added back to the Google Play Store on or after October 1, 2019 are not included.

5. Brand safety for a given app is determined based on the content ratings used by Google Play (e.g. apps with Mature content) as well as other brand safety categories found through a content analysis of the app by Pixalate (i.e. adult/sexual content, gambling, violence, drugs, alcohol, profanity, or unrestricted web access).

6. “IVT” stands for “Invalid Traffic.” Per the MRC, “‘Fraud’ is not intended to represent fraud as defined in various laws, statutes and ordinances or as conventionally used in U.S. Court or other legal proceedings, but rather a custom definition strictly for advertising measurement purposes.” Also per the MRC, “‘Invalid Traffic’ is defined generally as traffic that does not meet certain ad serving quality or completeness criteria, or otherwise does not represent legitimate ad traffic that should be included in measurement counts. Among the reasons why ad traffic may be deemed invalid is it is a result of non-human traffic (spiders, bots, etc.), or activity designed to produce fraudulent traffic.”

7. “China-registered” includes apps registered in Hong Kong.

8. “Top U.S. apps” refer to the top 10,000 mobile apps ranked by programmatic ad volume from Q1-Q3 2019, as measured by Pixalate.

9. “Dangerous permissions” are defined by Google and include all of the following permissions: 'write_external_storage', 'camera', 'use_sip', 'read_sms', 'send_sms', 'call_phone', 'receive_mms', 'receive_sms', 'body_sensors', 'get_accounts', 'record_audio', 'add_voicemail', 'read_calendar', 'read_call_log', 'read_contacts', 'write_calendar', 'write_call_log', 'write_contacts', 'accept_handover', 'read_phone_state', 'receive_wap_push', 'answer_phone_calls', 'read_phone_numbers', 'access_fine_location', 'activity_recognition', 'read_external_storage', 'access_coarse_location', 'process_outgoing_calls', 'access_background_location'. Data derived from crawls of the Play Store performed by Pixalate or one of Pixalate's third party licensors.

10. Of all apps on the Google Play Store. Data derived from crawls of the Play Store performed by Pixalate or one of Pixalate's third party licensors.

11. “Children” are defined as under the age of 13. This is in accordance with the Children's Online Privacy Protection Act (“COPPA”). Data derived from crawls of the Play Store performed by Pixalate or one of Pixalate's third party licensors.

INDEX (CONTINUED)

12. The country of registration for a given app is determined only if a) the app has a physical address published in its Google Play Store page, or otherwise b) from the registrant physical address of the publisher domain listed in the Google Play Store page excluding privately registered ones. If none of them is available, the physical address associated with an app cannot be determined.

13. “Traditional Shell Company Locations” as used in this report refers to any app registered in any of the following countries: Panama, Cyprus, Cayman Islands, Bahamas, Malta, Seychelles, British Virgin Islands, Barbados, Belize, Anguilla, Gibraltar, Nevis, Mauritius, Vanuatu, Costa Rica, Monaco.

14. Delisted app download data refers to the number of downloads an app had prior to its delisting. Data derived from crawls of the Play Store performed by Pixalate or one of Pixalate's third party licensors.

15. Of all apps that support programmatic advertising, as measured by Pixalate.

16. Download number as of September 30, 2019. Data derived from crawls of the Play Store performed by Pixalate or one of Pixalate's third party licensors.

REFERENCES

a. eMarketer: https://content-na1.emarketer.com/us-time-spent-with-mobile-2019

b. eMarketer: emarketer.com, October 2019.

c. Statista: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

d. New York Times: https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html

e. Bloomberg: https://www.bloomberg.com/news/articles/2019-12-02/russian-apps-could-pose-counterintelligence-threat-fbi-warns

f. The Sun: https://www.thesun.co.uk/tech/9225942/android-apps-break-phone-delete/

g. Intersoft Consulting: https://gdpr-info.eu/art-13-gdpr/

h. Google: https://developer.android.com/guide/topics/permissions/overview

METHODOLOGY & LIMITATIONS

Delisted Apps

An app is considered delisted if it existed in the Google Play store in a given time period of interest and then it was removed. Delisted apps are calculated at the month granularity level, i.e. all the app removals are grouped together according to the month they occurred. Delisted apps cannot reflect the initiator of the delisting action, i.e. Google or the app developer. Also if an app delisted on a given month is added back to the store later on, it will be counted as delisted only till the month that it was added back.

The impression activity from delisted apps is calculated based on the traffic seen starting the next month after the month of removal, as measured by Pixalate. Delisted app download data refers to the number of downloads an app had prior to its delisting; data derived from crawls of the Play Store performed by Pixalate or one of Pixalate's third party licensors.

Google Permissions

According to Google's documentation: "The purpose of a permission is to protect the privacy of an Android user. Android apps must request permission to access sensitive user data (such as contacts and SMS), as well as certain system features (such as camera and internet). Depending on the feature, the system might grant the permission automatically or might prompt the user to approve the request. A central design point of the Android security architecture is that no app, by default, has permission to perform any operations that would adversely impact other apps, the operating system, or the user. This includes reading or writing the user's private data (such as contacts or emails), reading or writing another app's files, performing network access, keeping the device awake, and so on."

All the permissions that an Android app needs to be granted should be listed in the "manifest file" of the app. Google classifies these permissions as "Dangerous" if they could potentially affect the user's privacy or the device's normal operation, such as the SEND_SMS permission." The user must explicitly agree to grant those permissions. The list of "dangerous permissions" is as follows:

- 'write_external_storage'
- 'camera'
- 'use_sip'
- 'read_sms'
- 'send_sms'
- 'call_phone'
- 'receive_mms'
- 'receive_sms'
- 'body_sensors'
- 'get_accounts,
- 'record_audio'
- 'add_voicemail'
- 'read_calendar'
- 'read_call_log'
- 'read_contacts'
- 'write_calendar'
- 'write_call_log'
- 'write_contacts'
- 'accept_handover'
- 'read_phone_state'
- 'receive_wap_push'
- 'answer_phone_calls'
- 'read_phone_numbers'
- 'access_fine_location'
- 'activity_recognition'
- 'read_external_storage'
- 'access_coarse_location'
- 'process_outgoing_calls'
- 'access_background_location'

METHODOLOGY & LIMITATIONS (CONTINUED)

App Programmatic Activity
App programmatic activity is calculated based on the impression data seen by Pixalate.

COPPA Risks
Children's Online Privacy Protection Act ("COPPA") imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. Pixalate defines COPPA risk for mobile apps as the collection of personal information (e.g. device ID) from mobile devices through mobile apps that are accessible to children under 13 years of age (inclusive of apps available to "Everyone").

Privacy Policy
An app is considered as having a privacy policy if it has one published in its Google Play Store page.

Country of Registration
The country of registration for a given app is determined only if a) the app has a physical address published in its Google Play Store page, or otherwise b) from the registrant physical address of the publisher domain listed in the Google Play Store page excluding privately registered ones. If none of them is available, the physical address associated with an app cannot be determined.

Shell Company Countries
The list of traditional shell company countries (or "shell countries" for brevity) corresponds to countries traditionally used to establish shell corporate entities and, for the purposes of this report, includes the following:

- Anguilla
- Bahamas
- Barbados
- Belize
- British Virgin Islands
- Cayman Islands
- Costa Rica
- Cyprus
- Gibraltar
- Malta
- Mauritius
- Monaco
- Nevis
- Panama
- Seychelles
- Vanuatu

Brand Safety
Brand safety for a given app is determined based on the content ratings used by Google Play (e.g. apps with Mature content) as well as other brand safety categories found through a content analysis of the app by Pixalate (i.e. adult/sexual content, gambling, violence, drugs, alcohol, profanity, or unrestricted web access).

Download Thresholds
Download figures referred to within this report are determined based on the published number of downloads at the Google Play Store, rounded down; data derived from crawls of the Play Store performed by Pixalate or one of Pixalate's third party licensors. For example, if Google Play Store states 10M+ downloads, Pixalate considers this 10M downloads and no more.

METHODOLOGY & LIMITATIONS (CONTINUED)

Top Apps With 'Dangerous Permissions'
For this analysis, Pixalate has included apps among the top 10,000 in terms of highest programmatic advertising volume in the United States, as measured by Pixalate, irrespective of fraud rates or block-listing decisions made. The apps are ranked by total number of "dangerous permissions."

Ad Fraud, or Invalid Traffic (IVT)
Per the MRC, "'Fraud' is not intended to represent fraud as defined in various laws, statutes and ordinances or as conventionally used in U.S. Court or other legal proceedings, but rather a custom definition strictly for advertising measurement purposes." Also per the MRC, "'Invalid Traffic' is defined generally as traffic that does not meet certain ad serving quality or completeness criteria, or otherwise does not represent legitimate ad traffic that should be included in measurement counts. Among the reasons why ad traffic may be deemed invalid is it is a result of non-human traffic (spiders, bots, etc.), or activity designed to produce fraudulent traffic."

DISCLAIMER

The content of this report reflects Pixalate's opinions with respect to the factors that Pixalate believes can be useful to the digital media industry. Any proprietary data shared is grounded in Pixalate's proprietary technology and analytics, which Pixalate is continuously evaluating and updating. Any references to outside sources should not be construed as endorsements. Pixalate's opinions are just that, opinions, which means that they are neither facts nor guarantees.

Per the MRC, "'Fraud' is not intended to represent fraud as defined in various laws, statutes and ordinances or as conventionally used in U.S. Court or other legal proceedings, but rather a custom definition strictly for advertising measurement purposes. Also per the MRC, "'Invalid Traffic' is defined generally as traffic that does not meet certain ad serving quality or completeness criteria, or otherwise does not represent legitimate ad traffic that should be included in measurement counts. Among the reasons why ad traffic may be deemed invalid is it is a result of non-human traffic (spiders, bots, etc.), or activity designed to produce fraudulent traffic."

It is important to also note that the mere fact that an app receives "dangerous permissions" (as defined by Google), can reach "children" (as defined by COPPA), appears to be transmitting personal data from the European Union to countries that have not yet been identified by the European Commission as having adequate privacy safeguards, does not appear to have published a privacy policy and/or a registration address, or is registered in a traditional tax haven country or a country that appears to be receiving heightened scrutiny by, among other governmental bodies, the Committee on Foreign Investment in the United States (CFIUS), does not necessarily mean that such app, or its publisher, is actually exploiting data subjects. Instead, we are merely rendering an opinion that these facts may be suggestive of heightened risks to data subjects.

QUESTIONS?

In Q1 2020, Pixalate will host a webinar to review our findings. Register today & share your questions:

https://pixal.at/mobile-safety-webinar

pixalate

THANK YOU

CONNECT WITH US

INFO@PIXALATE.COM

PIXALATE.COM

pixalate