A guide to the AppCensus system

Right now, privacy policies are one of the main tools that parents are expected to use to protect children's privacy when playing apps.

But privacy policies are often long, too hard to read and ambiguous.

These policies say what companies "may" do with personal data, rather than unequivocally specifying what a company *will* and *will not* do with that data.

Privacy decisions based simply on what data an app *might* access is an imperfect strategy.

The goal of the AppCensus system is to help parents make more informed decisions about their children's privacy by showing them exactly what data various apps collect, and with whom they were observed sharing it.

APPCENSUS:

- runs apps on real mobile phones in its testing laboratory; installing each app, granting the requested permissions, and using for a period of time.
- observes when apps access and share personal information, as well as unique persistent identifiers that can be used to track users over time and across services.
- collects as much data as possible about what the app is doing on the phone and what data it sends over the Internet.
- allows Appcensus to see:
  - *what data apps have permission to access;*
  - *what data apps actually access;*
  - *to whom they send that data; and*
  - *whether they do so securely.*

Appcensus results reflect the actual behaviour of the apps when they are used.

ACCM, in partnership with AppCensus, has developed a parent-friendly privacy check format for the most popular Android apps played by children in Australia. The Appcensus analyses for each app are delivered to ACCM using this format and incorporated into ACCM's ongoing app review system. The list of Top 50 children's apps checked in Australia will be updated regularly.

The information in these privacy checks can help you decide whether or not you are happy for your child to use a particular app.

WHAT DO THE APPCENSUS PRIVACY CHECKS PRODUCE?

When downloading an app, you are likely to be asked to grant permissions to access some of your personal details plus to use parts of your device, such as camera, microphone etc. Such data can be needed to facilitate the operation of the app, but some may be gathered for other purposes.

The AppCensus checks on the ACCM website will produce three outputs. These are:

a) The permissions (personal data and device identifiers) requested and if used
b) Whether the app transmits personal data and to whom
c) Whether such data transfer is encrypted (ie secure).

HERE ARE THE TERMS USED:

"Uses dangerous permissions" and *"Permissions requested and used"*

Features that are protected by permissions are extremely common, so their existence alone does not imply bad behaviour. Ask yourself whether it's appropriate for the app to be accessing that type of data, based on your knowledge of what the app is supposed to do (but keep in mind that sometimes an app does need permissions for reasons that are not obvious).

However, they are important to observe in instances where an ostensibly simple app has access to too many features (e.g., a flashlight app that can access your location), or where an app required access to information without the adequate permission to do so (e.g., an app that learns your location, but never asked you if that was OK) (see Appendix A for the different types of dangerous permissions that may be requested).

- *The permissions that an app has been granted indicate the types of data that it may access.*
- *Become familiar with the types of permissions that are requested. For example, a READ permission allows an app to read the contents of a file, whilst a WRITE permission allows adding or removing the contents of a file.*

"Transmits personal/sensitive data"

Every device has several 'persistent identifiers' that can be accessed by third-party apps and can be used to track users over time and across services. A persistent identifier is a globally unique number. Several identifiers, like "WiFi BSSID" are persistent, in that they are difficult, impossible, or illegal to change for the average user, making them the perfect instruments for persistently tracking behaviour. (see Appendix B for the different types of personal identifiers that may be transmitted).

"server name / company / secure"

Knowing what permissions have been granted is important, but it's even more important to know what data was observed actually being transmitted off of the device and to whom, and whether it's sent securely.

Who gets the data may change from one moment to the next; for advertising purposes many different recipients may bid for the user's attention.

SOME CAUTIONS

AppCensus might not actually detect all transmissions of private data: what's found is certain, but the app might not have engaged in other behaviours during the testing period, but might if played for longer or under different circumstances. Use of the data after it leaves the app is uncertain – it may be reshared with others.

ICONS

The following icons are used in the app check format to signal those apps that have had privacy checks, and use and/or transmit your personal data.

Uses Dangerous Permissions

If you see this icon you will know that the app has requested, though not necessarily used, dangerous permissions.

Transmits Sensitive Data

If you see this icon you will know that the app has transmitted sensitive data. Check to see whether this data was transmitted securely.

No tracking found in current check

If you see this icon you will know that at the time of testing no dangerous permissions were requested or used and no data was transmitted.

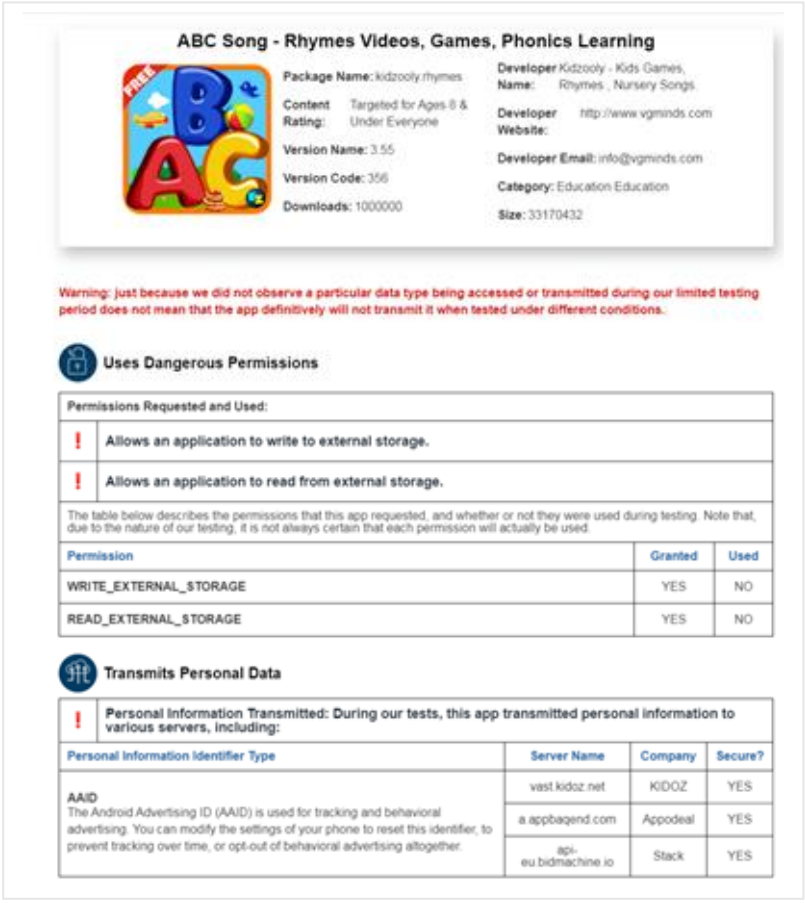
No Privacy Policy

If you see this icon you will know that the app did not have a privacy policy at the time of testing. Therefore, you should be very cautious if using the app.

HERE'S A SAMPLE APPCENSUS PRIVACY CHECK

Uses dangerous permissions:

As you can see in the example given, this particular app does request dangerous permissions, however, during testing these permissions were not actually used. Note that just because AppCensus did not observe a particular permission-protected data type being accessed during their limited testing period does not mean that the app definitively will not access it when tested under different conditions.



ABC Song - Rhymes Videos, Games, Phonics Learning

Package Name: kidzooly.rhymes
Content Rating: Targeted for Ages 8 & Under Everyone
Version Name: 3.55
Version Code: 356
Downloads: 1000000
Developer Name: Kidzooly - Kids Games, Rhymes , Nursery Songs
Developer Website: http://www.vgminds.com
Developer Email: info@vgminds.com
Category: Education Education
Size: 33170432

Warning: just because we did not observe a particular data type being accessed or transmitted during our limited testing period does not mean that the app definitively will not transmit it when tested under different conditions.

Uses Dangerous Permissions

Permissions Requested and Used:	
!	Allows an application to write to external storage.
!	Allows an application to read from external storage.

The table below describes the permissions that this app requested, and whether or not they were used during testing. Note that, due to the nature of our testing, it is not always certain that each permission will actually be used.

Permission	Granted	Used
WRITE_EXTERNAL_STORAGE	YES	NO
READ_EXTERNAL_STORAGE	YES	NO

Transmits Personal Data

!	Personal Information Transmitted: During our tests, this app transmitted personal information to various servers, including:		
Personal Information Identifier Type	Server Name	Company	Secure?
AAID The Android Advertising ID (AAID) is used for tracking and behavioral advertising. You can modify the settings of your phone to reset this identifier, to prevent tracking over time, or opt-out of behavioral advertising altogether.	vast.kidoz.net	KIDOZ	YES
	a.appbagend.com	Appodeal	YES
	api-eu.bidmachine.io	Stack	YES

Transmits personal data

As you can also see in the example given, this particular app does transmit personal data. In this instance, there is only one data type transmitted, however, it was transmitted to three different locations. An important aspect to note is that, in each case, the data was transmitted securely. This means that the data was 'encrypted with transport layer security', meaning that the data was sent over the Internet in an encrypted form to ensure that others are unable to see the data that is being transmitted. All communications should be encrypted and if they are not this is definitely a cause for concern.

Overall, AppCensus data shows that tracking is ubiquitous on the Internet and that parents are not given enough information to make informed decisions about their children's privacy, much less their own.

For further reading

Dr Serge Egelman, co-founder of AppCensus, explains why AppCensus privacy checks help parents: https://childrenandmedia.org.au/assets/files/apps-can-trap/Serge-explains-why-AppCensus-privacy-checks-help-parents.pdf

And https://blog.appcensus.io/2019/02/14/ad-ids-behaving-badly/

****

AppCensus

MACQUARIE University

Produced in partnership with the Macquarie University Department of Psychology.

accan

ACCM acknowledges the support of the Australian Communications Consumer Action Network (ACCAN) which funded the research for this project.

Appendix A: Dangerous Permissions

The following lists the dangerous permissions that apps may request:

"**ACCEPT_HANDOVER**": "Allows a calling app to continue a call which was started in another app. An example is a video calling app that wants to continue a voice call on the user's mobile network."

"**ACCESS_BACKGROUND_LOCATION**": "Allows an app to access location in the background. If you're requesting this permission, you must also request either \\textttACCESS_COARSE_LOCATION or \\textttACCESS_FINE_LOCATION. Requesting this permission by itself doesn't give you location access."

"**ACCESS_COARSE_LOCATION**": "Allows an app to access approximate location."

"**ACCESS_FINE_LOCATION**": "Allows an app to access precise location."

"**ACCESS_MEDIA_LOCATION**": "Allows an application to access any geographic locations persisted in the user's shared collection."

"**ACTIVITY_RECOGNITION**": "Allows an application to recognize physical activity."

"**ADD_VOICEMAIL**": "Allows an application to add voicemails into the system."

"**ANSWER_PHONE_CALLS**": "Allows the app to answer an incoming phone 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."

"**CALL_PHONE**": "Allows an application to initiate a phone call without going through the Dialer user interface for the user to confirm the call."

"**CAMERA**": "Required to be able to access the camera device."

"**GET_ACCOUNTS**": "Allows access to the list of accounts in the Accounts Service."

"**PROCESS_OUTGOING_CALLS**": "Allows an application to see the number being dialed during an outgoing call with the option to redirect the call to a different number or abort the call altogether."

"**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."

"**READ_EXTERNAL_STORAGE**": "Allows an application to read from external storage."

"**READ_PHONE_NUMBERS**": "Allows read access to the device's phone number(s). This is a subset of the capabilities granted by \\textttREAD_PHONE_STATE but is exposed to instant applications."

"**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 PhoneAccounts registered on the device."

"**READ_SMS**": "Allows an application to read SMS messages."

"**RECEIVE_MMS**": "Allows an application to monitor incoming MMS messages."

"**RECEIVE_SMS**": "Allows an application to receive SMS messages."

"**RECEIVE_WAP_PUSH**": "Allows an application to receive WAP push messages."

"**RECORD_AUDIO**": "Allows an application to record audio."

"**SEND_SMS**": "Allows an application to send SMS messages."

"**USE_SIP**": "Allows an application to use SIP service."

"**WRITE_CALENDAR**": "Allows an application to write the user's calendar data."

"**WRITE_CALL_LOG**": "Allows an application to write (but not read) the user's call log data."

"**WRITE_CONTACTS**": "Allows an application to write the user's contacts data."

"**WRITE_EXTERNAL_STORAGE**": "Allows an application to write to external storage."

Appendix B: Personal identifiers

The following lists the personal identifiers that apps may request:

'name': 'This is the name of the phone\'s owner.'

'phone': 'This is the phone number that is used to call the phone.'

'email': 'This is the e-mail address registered to the phone (i.e., any email accounts that can be checked from the phone\'s mail app).'

'location': 'This is the current location of the phone, down to at least street level.'

'geolatlon': 'This is the current location of the phone, down to at least street level.'

'routerssid': 'This refers to the names of nearby Wi-Fi networks, which could be used to reveal the current location of the phone.'

'routermac': 'This refers to the serial numbers of nearby Wi-Fi routers, which could be used to reveal the current location of the phone.'

'wifi':

'imei': 'The International Mobile Equipment Identity (IMEI) is a fixed serial number that is used to route calls to your phone. It is also a globally unique identifier that could be used to track you over time and across apps. It cannot be reset.'

'wifimac': 'The Wi-Fi MAC address is a fixed serial number that is used to identify your phone when transmitting and receiving data using Wi-Fi. It is also a globally unique identifier that could be used to track you over time and across apps. It cannot be reset.'

'aaid': 'The Android Advertising ID (AAID) is used for tracking and behavioral advertising. You can modify the settings of your phone to reset this identifier, to prevent tracking over time, or opt-out of behavioral advertising altogether.'

'gsfid': 'The Google Services Framework (GSF) ID is a number that uniquely identifiers your Google account. It is a globally unique identifier that could be used to track you over time and across apps and devices, and can only be reset by deleting your Google account.'

'androidid': 'The Android ID is a random serial number that is created when you first configure your phone. It is a globally unique identifier that could be used to track you over time and across apps, and can only be reset by performing a factory reset of your phone.'

'hwid': 'This is a fixed serial number that is reported by your phone\'s hardware. It is also a globally unique identifier that could be used to track you over time and across apps. It cannot be reset.'

'simid': 'This is a fixed serial number that is reported by your phone\'s SIM card, which is used to route calls to your phone. It is also a globally unique identifier that could be used to track you over time and across apps. It can only be reset by replacing your SIM card.'

'fingerprint': 'This refers to a list of your phone\'s current configuration parameters, including a description of your phone\'s hardware and software. While this is often used by developers to collect performance data and detect software bugs, it could also be used to construct a unique "fingerprint" of your device for tracking purposes.'

'photo': 'This refers to photos from your phone\'s camera or photo library.'

'audio': 'This refers to audio recorded from your phone\'s microphone.'

'video': 'This refers to videos from your phone\'s camera or photo library.'