Mobile apps and children's privacy: a traffic analysis of data sharing practices among children's mobile iOS apps

Despite policy recognition of children's vulnerability online, children's apps (or parental apps involving children's data) may share user data with third parties, which may be used to create detailed, long-term profiles of children, generating privacy risks.[1 2] These risks have attracted policy attention from the Federal Trade Commission; Apple Inc. subsequently stipulated that apps developed for children may not send personally identifiable or device information to third parties and should not include third-party trackers or advertising.

We conducted a cross-sectional study of top user-rated mobile apps labelled for children under 12 years available in the Apple App store in Australia, Canada, the UK and the USA as of July 2022 (https://kids-apps.healthprivacy.info). We aimed to (1) Characterise their data sharing practices through analysing their network traffic; (2) Identify the third parties who received the information transmitted from these apps. Building off previously reported methods,[3] we created a parent/child dummy profile and measured network traffic analysis during simulated app use to identify transmission of 21 prespecified types of user data and its network destinations. For identified data recipients, we examined their websites to categorise data recipients' main activities.

We purposively sampled 25 of 6264 apps identified by an App Store crawling program because they were highly rated by users (84% or 21/25 rated >4.4/5.0), had a privacy policy (96%, 24/25) and represented a variety of store categories including Productivity, Lifestyle, Utilities and Social Networking (32%, 8/25), Education (28%, 7/25), Entertainment (20%, 5/25), and Games (20%, 5/25), and Medical, Health and Fitness (12%, 3/25).

All sampled apps (100%, 25/25) shared user data with varying degrees of sensitivity outside the app (table 1). Almost half of the apps (44%, 11/25) transmitted at least one piece of data to third parties considered to be personal information under the European Union's General Data Protection Rules.

Included apps transmitted user data to 165 unique hosts (median 10, IQR 5–17). Forty hosts (24%, 40/165) were associated with the app's developer or its parent company. One hundred and thirty-eight hosts (84%, 138/165) were third parties including those providing infrastructure-related services (19%, 31/165), such as cloud services, and analysis services (65%, 108/165), such as advertising or analytics for commercial purposes (table 2). Amazon.com, Inc., Apple Inc. and Google LLC accounted for over a third of the unique hosts (58/165, 35%) in our traffic analysis and received data from all apps in the study as either a first party or third party (table 2). Despite Apple Inc.'s guidelines, 18 apps (72%) transmitted data to analysis-related third parties not associated with Apple Inc.

Children's data are commonly shared with third parties, suggesting there are privacy risks in using children's apps.[4] Thus, an industry self-regulatory approach to addressing children's privacy risks in apps may be limited. The implications of data sharing may manifest across aspects of childhood including those related to education, entertainment and health, and extend into adulthood. Privacy regulation should require transparency and accountability of data sharing practices from developers and third parties and promote user control over data sharing.

Table 1 Proportion of apps sharing user data and type of destination (n=25)

	User data type	No. of apps sharing with their developers (%)	No. of apps sharing to infrastructure-related third parties (%)	No. of apps sharing to analysis-related third parties (%)
Data considered 'personal data'*	Device ID†	5 (20)	4 (16)	10 (40)
	Email address†	6 (24)	4 (16)	3 (12)
	Name/last name†	6 (24)	1 (4)	1 (4)
	Birthday	6 (24)	1 (4)	0
	IMEI number	0	1 (4)	0
	Password	2 (8)	1 (4)	1 (4)
	Host name	0	0	1 (4)
	Fine grain location	2 (8)	0	2 (8)
	Local IP address	2 (8)	0	0
	Coarse grain location	1 (4)	0	0
	Personal factors	2 (8)	0	0
	Personal conditions	1 (4)	0	0
	Gender	2 (8)	0	0
Data not considered 'personal data'	OS version	15 (60)	22 (88)	25 (100)
	Device name	11 (44)	19 (76)	24 (96)
	Country	3 (12)	14 (56)	16 (64)
	Time zone	6 (24)	11 (44)	20 (80)
	Connection type	4 (16)	4 (16)	21 (84)
	Phone information	1 (4)	0	2 (8)
	Browsing	1 (4)	0	0
	Jailbrokenness	0	0	1 (4)

*Considered personal data under the General Data Protection Rules (GDPR), that is, 'any information relating to an identified or identifiable natural person'.
†Unique identifier.
IMEI, international mobile equipment identity; IP, internet protocol; OS, operating system.

Table 2 Categorisation of all third parties (n=108) and third parties excluding Apple Inc./Google LLC/Amazon.com, Inc. (n=79) performing analysis-related services

Main activity	N (%) third parties		Description	Examples
	All	Excluding Apple, Amazon, Google		
Advertising	38 (35.2%)	35 (44.3%)	Includes services that provide ad attribution to tie each user to the ads they interact with; buying and selling of ad space; ad serving and ad management; and analytics that enable ad targeting and personalisation.	Adjust; Amazon Ads; AppsFlyer; Google Marketing Platform; Mintegral; Awin; Quantcast; Singular; Tapjoy
Analytics	36 (33.3%)	27 (34.1%)	Freemium services; in exchange, companies retain the right to collect, aggregate and commercialise de-identified end-user data; companies provide services to app developers including error and bug reporting, and analysis of user numbers, characteristics and behaviours; some also offer the ability to understand users' behaviours across devices and platforms and integrate with advertising data to target marketing activities.	Apple Cookie Tracking; Bugsnag; Mixpanel; Crashlytics; Nominatim; Iterable; Instapage; New Relic
User engagement	12 (11.1%)	10 (12.7%)	Freemium services; in exchange, companies retain the right to collect, aggregate and commercialise de-identified end-user data; these software integrations allow developers to analyse how users navigate an app, features users find most engaging and provide push notifications to increase user engagement.	Apple Game Centre; Google Help; Zendesk; Optinmonster; Gravatar
Social media	5 (4.6%)	4 (5%)	Integration with social media platforms, allowing apps to share users' data with social media or to import social media data into the app; this could include a Facebook login, status updates related to the app, sharing content via social media, or finding a list of contacts who have also installed the app; this integration also allows for cross-platform advertising	Facebook Graph API; Pinterest; YouTube
Customer identity and access management	4 (3.7%)	1 (1.3%)	Customer identity and access management software is a type of identity technology that allows organisations to securely manage authentication and authorisation of customer identities.	Google Sign in Service; Amazon Cognito Authentication; Google Identity
Device verification/ID	4 (3.7%)	0	Services that allow organisations to verify the credentials of an incoming request from a device or external system, so that certain functionalities may be reserved for known, trusted, and legitimate users.	Apple Verification for Legal Phone Access; Apple Check Device Warranty; Apple Verification for Permission to Use App
App store	3 (2.8%)	0	An app store is a digital storefront designed to allow visitors to search, review, and purchase media and apps offered for sale electronically.	Apple iTunes; Google Play; iTunes Search API
Privacy	2 (1.9%)	0	Services that allow users to manage their privacy settings when using particular programmes or applications, such as opting out of advertisements, granting permission to collect user information when engaging with ads, and cookie tracking.	Apple Ad Privacy for User; Privacy Manager Google Chrome
Subscription services/in-app purchases	2 (1.9%)	1 (1.3%)	Services that allow app developers to manage purchases and subscriptions within their app and collect data on revenue generated from these purchases.	Google Play Developer API; Qonversion
Geofencing	1 (0.93%)	0	The use of GPS or RFID technology by organisations to create a virtual geographical boundary, enabling software to trigger a response when a mobile device enters or leaves a particular area.	Apple Geofencing
Unknown	1 (0.93%)	1 (1.3%)	Third parties that may have a broad range of capabilities and uses, with no indication of the specific use within the context of this study.	NA

API, application programming interface; GPS, global positioning system; RFID, radio frequency identification.

Jessica Pimienta,[1] Jacco Brandt,[2] Timme Bethe,[2] Ralph Holz,[2] Andrea Continella,[2] Lindsay Jibb,[1,3] Quinn Grundy [1]

[1]Lawrence S. Bloomberg Faculty of Nursing, University of Toronto, Toronto, Ontario, Canada
[2]Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, Enschede, Netherlands
[3]Child Health Evaluative Sciences, Hospital for Sick Children, Toronto, Ontario, Canada

Correspondence to Dr Quinn Grundy, University of Toronto, Toronto M5T 1P8, Ontario, Canada; quinn.grundy@utoronto.ca

Acknowledgements The authors thank ip2location.com for support in providing an academic license to their geo-IP database.

Contributors QG and LJ acquired funding, designed the study, supervised, and participated in data collection and content analysis. JP participated in data collection and content analysis. JB conducted the traffic analysis. TB conducted the traffic analysis. AC and RH designed the study, supervised the traffic analysis. JP and QG act as guarantors.

Funding Government of Canada's New Frontiers in Research Fund (NFRF) (NFRFE-2019-00806).

Competing interests None declared.

Patient consent for publication Not applicable.

Ethics approval Not applicable.

Provenance and peer review Not commissioned; externally peer reviewed.

To cite Pimienta J, Brandt J, Bethe T, *et al*. *Arch Dis Child* Epub ahead of print: [*please include* Day Month Year]. doi:10.1136/archdischild-2023-325960

Accepted 26 July 2023

Arch Dis Child 2023;**0**:1–2. doi:10.1136/archdischild-2023-325960

ORCID iD
Quinn Grundy http://orcid.org/0000-0002-7640-8614

REFERENCES

1 Jibb L, Amoako E, Heisey M, *et al*. Data handling practices and commercial features of Apps related to children: A Scoping review of content analyses. *Arch Dis Child* 2022;107:665–73.
2 Zhao F, Egelman S, Weeks HM, *et al*. Data collection practices of mobile applications played by preschool-aged children. *JAMA Pediatr* 2020;174:e203345.
3 Grundy Q, Chiu K, Held F, *et al*. Data sharing practices of medicines related Apps and the mobile Ecosystem: traffic, content, and network analysis. *BMJ* 2019;364:l920.
4 Binns R, Lyngs U, Van Kleek M, *et al*. Third party tracking in the mobile Ecosystem. WebSci '18; Amsterdam Netherlands. New York, NY, USA: ACM, May 15, 2018:23–31