Álvaro Feal*, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla

# Angel or Devil? A Privacy Study of Mobile Parental Control Apps

**Abstract:** Android parental control applications are used by parents to monitor and limit their children's mobile behaviour (*e.g.,* mobile apps usage, web browsing, calling, and texting). In order to offer this service, parental control apps require privileged access to system resources and access to sensitive data. This may significantly reduce the dangers associated with kids' online activities, but it raises important privacy concerns. These concerns have so far been overlooked by organizations providing recommendations regarding the use of parental control applications to the public.

We conduct the first in-depth study of the Android parental control app's ecosystem from a privacy and regulatory point of view. We exhaustively study 46 apps from 43 developers which have a combined 20M installs in the Google Play Store. Using a combination of static and dynamic analysis we find that: these apps are on average more permissions-hungry than the top 150 apps in the Google Play Store, and tend to request more dangerous permissions with new releases; 11% of the apps transmit personal data in the clear; 34% of the apps gather and send personal information without appropriate consent; and 72% of the apps share data with third parties (including online advertising and analytics services) without mentioning their presence in their privacy policies. In summary, parental control applications lack transparency and lack compliance with regulatory requirements. This holds even for those applications recommended by European and other national security centers.

**Keywords:** Parental control, Android, mobile apps, static analysis, dynamic analysis

**PACS:**

DOI Editor to enter DOI
Received ..; revised ..; accepted ...

## 1 Introducción

La dependencia de la sociedad de los servicios móviles para realizar actividades diarias ha aumentado drásticamente en la última década [79]. Los niños no son una excepción a esta tendencia. Solo en el Reino Unido, el 47 % de los niños de entre 8 y 11 años tiene su propia tableta y el 35 % posee un teléfono inteligente [63]. Desafortunadamente, Internet alberga una gran cantidad de contenido potencialmente dañino para los niños, como imágenes sexuales sin censura [20], contenido violento [89] y lenguaje fuerte [50], que es de fácil acceso para los menores. Además, los niños pueden (sin saberlo) exponer datos sensibles en línea que eventualmente podría caer en manos de depredadores [2], o que podría desencadenar conflictos con sus compañeros [30].

Con el objetivo de salvaguardar la vida digital de los niños, algunos padres recurren a *aplicaciones de control parental* para monitorear actividades de los niños y para controlar lo que pueden hacer con sus teléfonos inteligentes [61, 76]. La típica aplicación de control parental permite a los padres filtrar, monitorear o restringir comunicaciones, contenido, funciones del sistema y aplicaciones ejecución [87]. Otras aplicaciones brindan a los padres informes detallados sobre el uso de teléfono, sus interacciones sociales y su ubicación física. Un ejemplo de la primera es la plataforma de descubrimiento de contenido *Safe Mode with Free Games for Kids* de *KIDOZ*, y de esta última es la aplicación *Norton Family*.

Para proporcionar estas funciones, las aplicaciones de control parental se basan en la colección y manejo del comportamiento de los niños (por ejemplo, ubicación, actividades de navegación y llamadas telefónicas) y datos personales (por ejemplo, identificadores únicos y contactos), en muchos casos, utilizando técnicas y métodos similares a los del software espía [27]. Sin embargo, como ocurre con muchos Las aplicaciones

***Corresponding Author: Álvaro Feal:** IMDEA Networks Institute / Universidad Carlos III de Madrid, E-mail: alvaro.feal@imdea.org
**Paolo Calciati:** IMDEA Software Institute / Universidad Politécnica de Madrid, E-mail: paolo.calciati@imdea.org
**Narseo Vallina-Rodriguez:** IMDEA Networks Institute / ICSI, E-mail: narseo.vallina@imdea.org
**Carmela Troncoso:** Spring Lab EPFL, E-mail: carmela.troncoso@epfl.ch
**Alessandra Gorla:** IMDEA Software Institute, E-mail: alessandra.gorla@imdea.org

de Android, el software de control parental también pueden integre SDK de publicidad de terceros que consuman datos —para monetizar su software— y SDK de análisis: para supervisar el comportamiento de sus usuarios, crear informes de errores, y crear perfiles de usuario. Como consecuencia del modelo de permisos de Android, estos Los SDK disfrutan del mismo conjunto de permisos otorgados por el usuario a la aplicación de host. Las aplicaciones también pueden exponer inadvertidamente datos a observadores de red en ruta si utilizan protocolos inseguros para transmitir datos confidenciales. Estas prácticas implican grandes riesgos de privacidad para los menores, por ejemplo, si Los datos se utilizan para perfilar el comportamiento o el desarrollo de los niños, o si los datos se ve comprometido [62].

Para ayudar a los padres a elegir entre las soluciones de control parental, los centros de seguridad a nivel europeo [1, 33] han analizado una serie de soluciones de control parental. Su análisis considera cuatro dimensiones: funcionalidad, eficacia, usabilidad y seguridad, definida como su eficacia para disuadir a los niños de eludir el sistema. Sin embargo, estos informes *no proporcionan ningún análisis de riesgo de privacidad*, ni consideran la falta de transparencia u otras posibles violaciones de la privacidad relevante leyes con disposiciones específicas para salvaguardar la privacidad de los menores, por ejemplo, la Regulación General de Protección de Datos (RGPD) [29] y la Children Online Privacy and Protection Act (COPPA) [35].

En este artículo, presentamos el primer análisis integral orientado a la privacidad de aplicaciones de control parental para Android desde un punto de vista técnico y normativo punto de vista. Estudiamos aplicaciones de 46 utilizando tanto aplicaciones estáticas como dinámicas. métodos de análisis para caracterizar su comportamiento en tiempo de ejecución y sus datos prácticas de recopilación e intercambio de datos. También estudiamos la precisión y integridad de sus políticas de privacidad, identificando posibles violaciones de normativa existente para proteger a los menores. Observamos que durante nuestro análisis no recopilamos ningún dato de niños ni de ningún otro usuario. (§ 3.1.4 describe las consideraciones éticas).

Nuestros principales resultados son los siguientes:

A. El análisis de contaminación estática revela que tanto las aplicaciones como las librerias de terceros integradas difunden información sensible, como el IMEI, ubicación o dirección MAC (§ 4). Las aplicaciones también usan *permisos personalizados* para obtener funcionalidades expuestas por desarrolladores de otras aplicaciones o proveedores de teléfonos, revelando asociaciones (comerciales) entre ellos.
B. Descubrimos que casi el 75% de las aplicaciones contienen bibliotecas de terceros que recogen datos para publicidad, redes sociales y servicios analíticos (§ 5). Además, 67% aplicaciones comparten datos privados sin el consentimiento del usuario (§ 6.3), incluso aunque algunas de estas aplicaciones son recomendadas por organismos públicos (p. ej., SIP-Bench III [1, 33]). A pesar de procesar los datos de los niños, 4% de las aplicaciones utilizan librerías que afirman no estar dirigidas a los niños y, por lo tanto, no requieren de medidas para cumplir con las leyes de privacidad específicas para niños (p. ej., la regla COPPA de EE. UU. [35]). Además, solo dos de las siete librerías relacionadas con anuncios que se encuentran cumplen con COPPA de acuerdo con la lista de bibliotecas autocertificadas de Google para niños de 2019 [42].
C. Los flujos salientes del 35% de estas aplicaciones están dirigidas a terceros, pero 79% de las aplicaciones no nombran estas organizaciones en sus políticas de privacidad (§ 6). Encontramos 67% aplicaciones que recopilan datos confidenciales sin el consentimiento del usuario, y 6 aplicaciones que no implementan mecanismos de seguridad básicos como el uso de cifrado para el tráfico de Internet.
D. A pesar de ser requerido por las regulaciones [29, 35], solo la mitad de las aplicaciones informan claramente a los usuarios sobre su recopilación de datos y prácticas de procesamiento (§ 7). Mientras 59% de las aplicaciones admiten el uso de datos sensibles por parte de terceros, solo 24% divulga la lista completa de terceros incrustado en el software. Además, 18% no informa de ninguna actividad de intercambio de datos a pesar de que encontramos evidencia de recopilación de datos a través de SDK integrados.

## 2 Aplicaciones de Control Parental

Las aplicaciones de control parental de Android ofrecen diversas funciones para controlar las actividades digitales de los niños. En línea con el anterior trabajo [55, 87], clasificamos aplicaciones que permiten a los padres monitorear el comportamiento de los niños, incluyendo ubicación [46], como *herramientas de monitoreo*; y clasificamos las aplicaciones que permiten a los padres filtrar contenido y definir reglas de uso para

limitar las acciones de los niños como *aplicaciones de restricción*. Algunas aplicaciones ofrecen múltiples funcionalidades simultáneamente, y etiquetamos ellos como *monitoreo* ya que es la más invasiva de las dos categorías.

La forma en que las aplicaciones de control parental hacen cumplir estas funcionalidades es variado. Las alternativas comunes son reemplazar el lanzador de Android con una superposición personalizada en la que solo están disponibles las aplicaciones incluidas en la lista blanca; instalar un navegador web donde los desarrolladores tengan control total para monitorear y restringir el tráfico web; o aprovechando la VPN de Android permiso [13] para obtener visibilidad completa y control sobre el tráfico de la red. Los criterios más comunes para personalizar el comportamiento de la aplicación son la edad. y listas negras / listas blancas. El primero restringe el tipo de contenido o define el nivel de seguimiento en función del edad de los niños. En general, los niños mayores tienen acceso a un conjunto más grande de páginas web y aplicaciones que los jóvenes. En este último, los padres pueden enumerar aplicaciones o páginas web que consideran inapropiadas para sus hijos, o agregar contenido apropiado a listas blancas.

La mayoría de las aplicaciones de control parental tienen dos componentes o modos: *i*) la aplicación o modo principal, y *ii*) la aplicación o el modo para niños. La aplicación principal puede ejecutarse en el niños o en el dispositivo de los padres que permite el acceso a la aplicación para niños datos y al tablero para configurar reglas de monitoreo o bloqueo. Cuando el modo para padres se ejecuta en el dispositivo de los niños, el el monitoreo se puede realizar localmente en este dispositivo. Sin embargo, cuando la aplicación para padres e hijos se ejecuta en diferentes dispositivos, la aplicación para niños a menudo carga información en un servidor central para para permitir el acceso remoto a la información de los niños a los padres. Muchas aplicaciones de nuestro estudio proporcionan un panel de control basado en web en el que los padres pueden acceder a toda la información y cambiar tanto las reglas de control como las de bloqueo. Este enfoque *requiere* subir datos a la nube, y como a resultados, los padres deben confiar en los proveedores de servicios para no difundir ni tratar los datos de los niños para fines secundarios distintos a los declarado en la política de privacidad.

Para ayudar a los desarrolladores de aplicaciones para niños, Google ha hecho públicas las mejores prácticas de desarrollo [5], así como una lista de publicidad y seguimiento de terceros autocertificados bibliotecas que respetan la privacidad de los niños [42]. Si bien las aplicaciones de control parental no se enumeran necesariamente en la Programa diseñado para familias (DFF) [41], un programa de Google Play para publicar aplicaciones dirigidas (y adecuadas para) niños, dada su naturaleza, esperamos que sigan las normas especiales disposiciones y seguir las mejores prácticas para recopilar datos sobre menores.

## 2.1 Marco normativo

Los menores pueden estar menos preocupados por los riesgos y consecuencias de la difusión de sus datos a Internet [29, 56]. Esto ha motivado reguladores para desarrollar leyes de privacidad estrictas para proteger la privacidad de los niños como la Children Online Privacy Protection Act (COPPA) en los EE. UU. La COPPA dicta que los datos personales de los niños menores de 13 solo se pueden recopilar mediante servicios en línea, juegos y dispositivos móviles solicitudes después de obtener el consentimiento paterno explícito y verificable [35]. En la UE, el Reglamento General de Protección de Datos (RGPD) hace cumplir la transparencia de la privacidad y requiere datos recolectores para obtener el consentimiento de los sujetos europeos antes de la recopilación datos personales de ellos, indicando claramente el propósito para el que se recopila [29]. Como en el caso de la regla COPPA de EE. UU., la RGPD contiene artículos adicionales en relación con la privacidad de los menores—a saber, el art. 8 [48] y el recital 38 [49] de la RGPD—que requiere que las organizaciones obtengan consentimiento verificable del padre o tutor legal de un menor bajo la edad de 16 años antes de recopilar y procesar sus datos personales. Ambas regulaciones prohíben explícitamente la recolección y el procesamiento de los datos del menor con fines de marketing o elaboración de perfiles de usuario, y desarrolladores para implementar las mejores prácticas de seguridad (por ejemplo, uso de cifrado) y divulgar la presencia y las prácticas de recopilación de datos de bibliotecas de terceros integradas, como publicidad y servicios de analítica [29, 35].

# 3 Metodología de recolección y análisis de datos

Google Play no proporciona ninguna categoría específica para aplicaciones de control parental. Los identificamos buscando la cadena *"Aplicación de control*

*parental"* en el motor de búsqueda de Google Play. Como este proceso puede producir falsos positivos, eliminamos manualmente cualquier aplicación que no implemente funcionalidades de control parental. Repetimos este proceso en diferentes puntos durante el proyecto para agregar aplicaciones recién publicadas a nuestro estudio. En total, encontramos 61 aplicaciones de control parental . Curiosamente, la mayoría de estas aplicaciones son clasificadas como *Herramientas* (42% de las aplicaciones) por los desarrolladores, a pesar de la presencia de la categoría más específica *Parenting* (15% de las aplicaciones).

Los desarrolladores de aplicaciones de Android a menudo lanzan nuevas versiones para incluir nuevas funciones a su software o para parchear vulnerabilidades [26]. Estos cambios pueden tener un impacto en la privacidad de los usuarios [71]. Rastreamos APKPure [14]—un conjunto de datos público que contiene versiones históricas de aplicaciones Android—para obtener 429 versiones antiguas para la lista de 61 aplicaciones para que podamos estudiar su evolución en el tiempo. Descartamos versiones anteriores a 2016, ya que las consideramos demasiado antiguas para nuestro estudio. Esto también resulta en el descarte de 15 aplicaciones que no se han actualizado desde 2016. Como anécdota, uno de los desarrolladores solo hizo la versión para padres disponible a través de Google Play, mientras que su contraparte solo está disponible mediante descarga directa en el sitio web del desarrollador. Decidimos descargar la versión para niños para evitar sesgos en nuestro análisis dinámico. Nuestro conjunto de datos final contiene 419 versiones de 46 aplicaciones de control parental (enumeradas en la Tabla 8 en el Apéndice).

Para cada aplicación, recolectamos metadatos disponibles públicamente en la tienda Google Play: descripciones de aplicaciones, número de descargas, valoraciones de usuarios, políticas de privacidad, y detalles del desarrollador. Usamos estos metadatos en nuestro análisis para contextualizar nuestra resultados, que muestran diferencias potenciales entre el tipo de desarrollador y la popularidad de la aplicación, y para analizar la integridad de las políticas de privacidad. [1]

**Popularidad de las apps.** La cantidad de instalaciones por aplicación, una métrica que se usa a menudo para inferir la popularidad [84, 90], varía extensamente. El conjunto de datos contiene 22% de aplicaciones con más de 1 millón de descargas, mientras que 37% de las aplicaciones tienen menos de 100.000 descargas. Cuando se consideran juntos, las 46 aplicaciones han sido instaladas por más de 22M usuarios (límite inferior). Las aplicaciones más descargadas suelen tener una mejor calificación de usuario (en promedio 3.5 de 5 para aplicaciones con más de 1 millón de descargas) que aquellos con una menor cantidad de instalaciones (en promedio 3.2 de 5 para aplicaciones con menos de 100k instalaciones).

**Desarrolladores de las apps.** Extraemos los certificados de firma de las aplicaciones para identificar el conjunto de empresas (o personas) detrás de las aplicaciones de control parental. Descubrimos que la mayoría de los desarrolladores lanzan una sola aplicación de control parental, excepto para 3 desarrolladores que han lanzado dos aplicaciones. Además de las aplicaciones de control parental identificadas, 21% de los desarrolladores también publican software no relacionado en Google Play . Los casos más notables son *Yoguesh Dama* [45], una empresa india que ha publicado 38 aplicaciones (para control de volumen, bloqueo de pantalla, fondo de pantalla y más), y *Kid Control Dev* [44] una empresa rusa que también crea aplicaciones como linternas.

Se puede suponer que el uso de aplicaciones de control parental se basa principalmente en la confianza. Por lo tanto, investigamos si la identidad del desarrollador de la aplicación juega un papel en la elección de los padres. Nuestra hipótesis inicial es que los padres podrían preferir el software desarrollado por reconocidas empresas de seguridad como *McAfee* o *Norton*. Sin embargo, encontramos que estos desarrolladores solo tienen en cuenta 9% del total de aplicaciones, y que no son los más instalados, solo uno de ellos alcanza 1 millón de instalaciones. Las aplicaciones de control parental más populares son las desarrolladas por empresas especializadas en software para niños (por ejemplo *Kiddoware* [53] y *Screen Time Labs* [75]). La mayoría de las aplicaciones de control parental parecen monetizar su software a través de compras en la aplicación (de 1 EUR a 350 EUR) para desbloquear características y licencias mensuales, sin embargo normalmente ofrecen un período de prueba gratuito.

**Apps desaparecidas.** Observamos que 10 de las aplicaciones se eliminaron de la tienda de aplicaciones de Google desde nuestra colección inicial de aplicaciones (febrero de 2018). La razón por la que estas aplicaciones se han eliminado de la lista no está clara: su eliminación podría ser desencadenada por los desarrolladores (por

**1** El conjunto de 46 aplicaciones puede no contenee todas las aplicaciones de control parental disponibles, pero las aplicaciones son diversas desde diferentes puntos de vista y pueden ser consideradas como un conjunto de datos representativo.

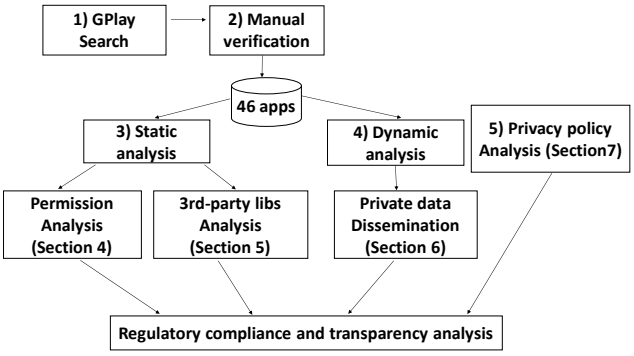


**Fig. 1.** Tubería de análisis para evaluar los riesgos de privacidad y el cumplieminto de la regulación en las aplicaciones de control parental.

ejemplo, las empresas ya no están en funcionamiento), o mediante el proceso de desinfección de la tienda de Google Play (Play Protect [7]). Todavía analizamos estas aplicaciones e informamos cuando no se puedan probar porque ya no funcionan.

## 3.1 Tubería de análisis

Para realizar nuestro análisis aprovechamos las ventajas estáticas y dinámicas técnicas de análisis previamente desarrolladas por la comunidad investigadora—en algunos casos extendiéndolos para cumplir con nuestros objetivos de investigación—como se muestra en la Figura 1. Utilizamos análisis tanto estáticos como dinámicos para superar las limitaciones que presentan cuando se utilizan en aislamiento [70]. § 8 analiza las limitaciones de nuestro método.

### 3.1.1 Análisis estático

Para cada aplicación y versión, primero analizamos el archivo de manifiesto de Android [11] para comprender su comportamiento de alto nivel sin analizar el código binario. Concretamente, buscamos: *i*) aplicaciones con solicitudes de permiso inusuales y *ii*) aplicaciones que solicitan un número de permisos distintos entre versiones. Complementamos este análisis con análisis de contaminación estática para investigar la difusión de datos personales potencial mediante aplicaciones y SDK de terceros integrados. Finalmente, observamos el código binario para identificar bibliotecas de terceros incrustadas en la aplicación usando LibRadar [57]. Este último paso es fundamental para atribuir los comportamientos observados a su responsable. Presentamos los resultados de nuestro análisis estático en § 4 y § 5. El análisis estático no tiene visibilidad de la lógica del lado del servidor y no puede analizar aplicaciones con código fuente ofuscado. Además, puede informar falsos positivos, por lo que lo complementamos con análisis dinámico, como se discute a continuación.

### 3.1.2 Análisis dinámico

El hecho de que las aplicaciones declaren un permiso determinado o incorporen un SDK de terceros determinado no no significa que se usará el permiso o que se ejecutará la librería. Usamos análisis dinámico para recopilar evidencia real de difusión de datos personales (§ 6.2), evaluar las prácticas de seguridad de estas aplicaciones en relación con las comunicaciones de red (§ 6.4), e identificar los formularios de consentimiento presentados al usuario en tiempo de ejecución (§ 6.3). Usamos la aplicación Lumen Privacy Monitor [69], una herramienta de análisis de tráfico avanzado para Android que aprovecha el permiso de VPN de Android para capturar y analizar el tráfico de la red, incluidos los flujos cifrados, localmente en el dispositivo y en el espacio de usuario. El uso de Lumen solo proporciona un límite inferior a todas las comunicaciones de red en una aplicación, ya que solo puede capturar flujos activados por el usuario, el sistema o estímulos ambientales y rutas de código en tiempo de ejecución. Lograr una cobertura completa de las acciones de las aplicaciones de control parental es complicado y requiere mucho tiempo: debemos configurar manualmente una cuenta principal y luego exhaustivamente probar la aplicación imitando el uso del teléfono por parte de un niño. El proceso de prueba de las aplicaciones debe ser manual ya que el ejercitador de Android Monkey [8] no es capaz de completar formularios de inicio de sesión o probar las funciones de la aplicación de forma no aleatoria [28]. Proporcionamos detalles sobre la metodología de prueba en § 6.2.

### 3.1.3 Análisis de políticas de privacidad

Realizamos un análisis manual de la última versión de las políticas de privacidad de las aplicaciones (§ 7) obtenidas de su perfil de Google Play. Los inspeccionamos para identificar: *i*) si las aplicaciones proporcionan información comprensible y condiciones claras de uso y políticas de privacidad para los usuarios finales; *ii*) si sse cumple con las disposiciones de las regulaciones de privacidad; y *iii*) si el texto divulgado coinciden con

su comportamiento en términos de acceso y difusión de datos sensibles y la presencia de bibliotecas de terceros.

### 3.1.4 Consideraciones éticas

Trabajos anteriores han demostrado el uso de aplicaciones de control parental. puede tener implicaciones éticas [27, 59], por lo tanto, **no recopilamos datos reales de niños ni de otro usuario**. Realizamos nuestra recopilación de datos sobre cuentas falsas operadas por nosotros mismos. Además, toda la interacción con las aplicaciones se realiza mediante los autores de este documento, sin la participación de niños o usuarios finales.

Nos enfocamos en comprender las prácticas de seguridad y privacidad de estas aplicaciones para determinar hasta qué punto podrían ser una amenaza para la privacidad de los niños. También destacamos que algunos de los problemas de privacidad encontrados en aplicaciones móviles puede ser el resultado de malos hábitos de codificación y falta de conciencia, especialmente al integrar SDK de terceros que abusan de la privacidad, en lugar de un mal comportamiento intencional del desarrollador. Comunicamos nuestro conclusiones a la Agencia Española de Protección de Datos (AEPD) y otros agencias gubernamentales que promueven la seguridad en Internet, a saber, IS4K [1] de INCIBE.

# 4 Análisis de permisos

Android implementa un modelo de permisos para controlar el acceso de la aplicación a datos personales (por ejemplo, contactos y correo electrónico) y recursos sensibles del sistema (por ejemplo, sensores como GPS para acceder a la ubicación) [10]. El análisis de los permisos solicitados por una aplicación ofrece una idea de alto nivel de los recursos y datos del sistema protegidos a los que la aplicación tiene acceso. Además de la lista de permisos oficiales de Android definida en Android Open Source Project—agrupados en diferentes niveles de riesgo, los más sensibles etiquetados como "peligrosos"—cualquier aplicación puede definir sus propios "permisos personalizados" [39, 81] para exponer sus recursos y capacidades a otras aplicaciones. Estudiamos el uso de los permisos de Android y su evolución en diferentes versiones para estudiar a qué datos acceden las aplicaciones de control parental, cómo cambia en las versiones de la aplicación [26, 71], por. ej. para adaptarse a requisitos de privacidad más estrictos en el nivel de plataforma [12], si estos datos son potencialmente enviado a través de Internet, si estos permisos son utilizados por SDK de terceros, la propia aplicación o ambos; y si hay diferencias notables entre las aplicaciones de supervisión y restricción en términos de solicitud de permisos.

## 4.1 Prevalencia y uso de permisos

La figura 2 muestra los permisos solicitados por cada una de las aplicaciones de nuestro conjunto de datos, así como la categoría del permiso. La parte superior del gráfico muestra las aplicaciones de restricción y la parte inferior las aplicaciones de seguimiento. En cuanto a las columnas, diferenciamos los permisos según su nivel de riesgo de privacidad [6]:

A. Permisos peligrosos: (primer bloque desde la izquierda, en azul), aquellos que potencialmente podrían afectar el la privacidad del usuario o al funcionamiento normal del dispositivo y, por lo tanto, debe ser concedidos explícitamente por el usuario.
B. Permisos signature: (segundo bloque, en naranja)—aquellos que el sistema otorga solo si la aplicación solicitante está firmada con el mismo certificado que la aplicación que declaró el permiso. También representamos los permisos del sistema en la misma categoría, incluso aquellos que están obsoletos en las versiones recientes de Android, pero aún funcionan en versiones anteriores.
C. Permisos personalizados (último bloque, en amarillo)—ie aquellos que las aplicaciones definen para proteger sus recursos.

Debido a limitaciones de espacio, no mostramos los permisos normales—aquellos que regulan el acceso a datos o recursos que suponen poco riesgo para la privacidad del usuario, y son otorgados automáticamente por el sistema. Sin embargo, son parte de nuestro estudio.

En la Figura 2 usamos degradados de color para mostrar los cambios en las solicitudes de permisos de las aplicaciones a lo largo del tiempo. Los colores más oscuros muestran que todas las versiones de la aplicación solicitan el permiso (es decir, sin cambios). La figura 2 muestra que, como se esperaba debido a su propia naturaleza, en general, las aplicaciones de control parental necesitan muchos permisos para ofrecer su servicio. Considerando el valor mediano, las aplicaciones de control parental solicitan 27 permisos, 9 de ellos están etiquetados como peligrosos. A modo de comparación, las 150

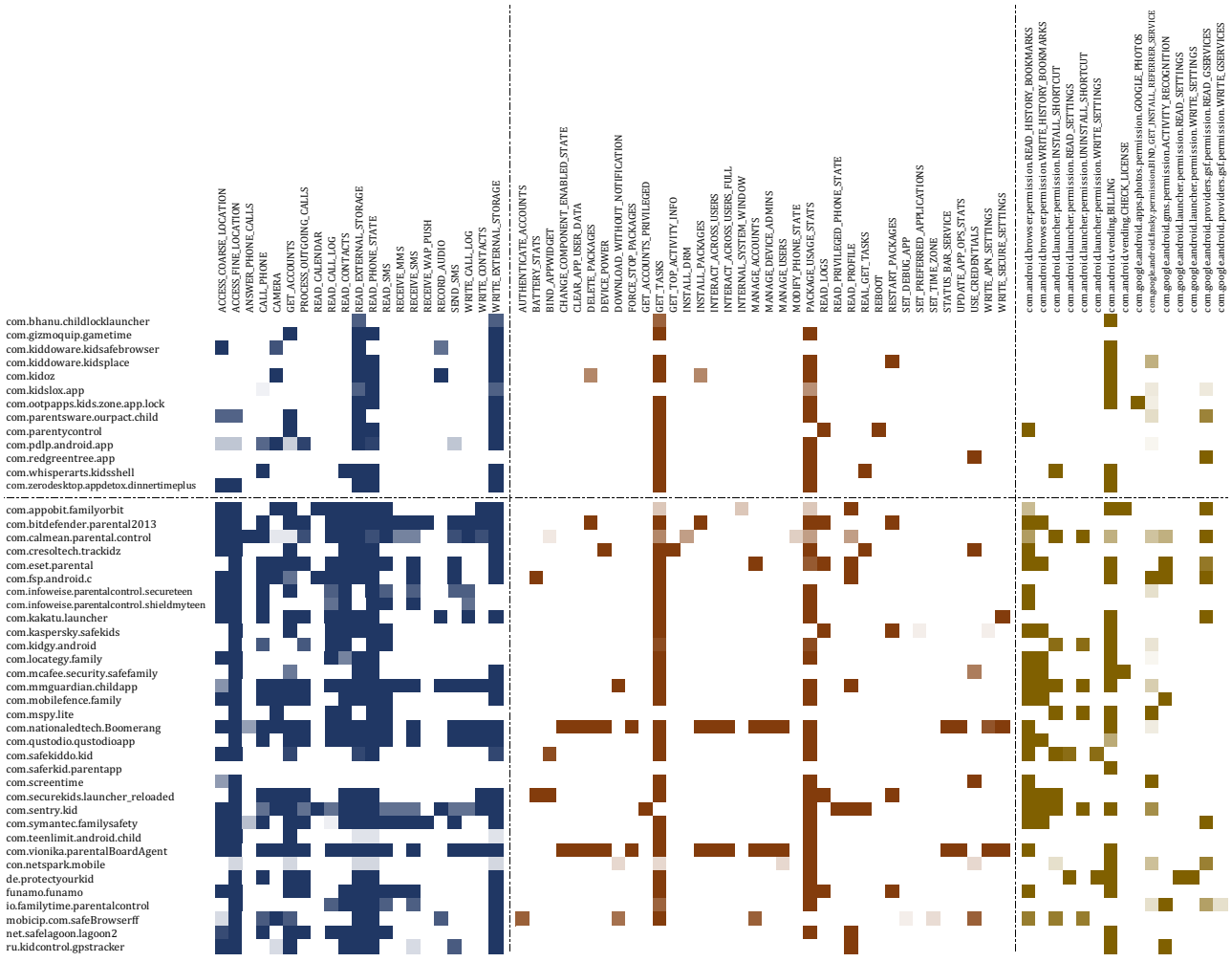


**Fig. 2.** Mapa de calor de permisos. Enumeramos una aplicación por fila e indicamos los permisos que solicita. Mostramos aplicaciones de restricción en la parte superior y de seguimiento en la parte inferior. Diferenciamos permisos peligrosos (azul), signature (naranja), y personalizados (amarillo). La intensidad de color muestra el porcentaje de versiones que solicitan el permiso, cuanto más oscuro significa un mayor número de lanzamientos.

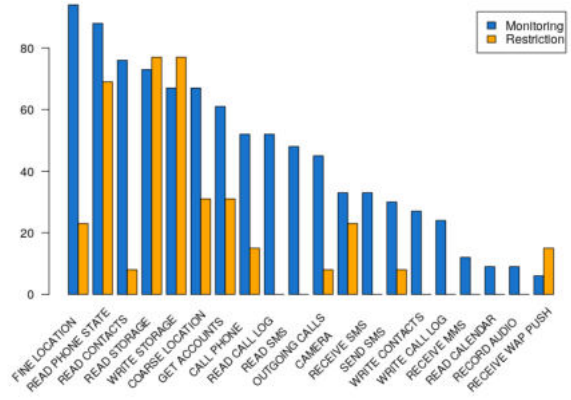


**Fig. 3.** Comparación del porcentaje de aplicaciones que solicitan permisos peligrosos entre las aplicaciones de Monitoreo y Restricción.

aplicaciones principales de Google Play Store en mayo de 2019 solicitan 18 permisos, 5 de ellos etiquetados como peligrosos. De hecho, encontramos que el caso más extremo en nuestro conjunto de datos (*Boomerang*) solicita 91 permisos, de cuáles 16 son peligrosos; mucho más de lo que normalmente pasa en otras aplicaciones que pueden resultar invasivas para la privacidad.[2]

Encontramos que más de 80% aplicaciones de control parental, independientemente de su categoría, solicitan acceso a ubicación, contactos y permisos de almacenamiento. Los permisos no peligrosos más solicitados por las aplicaciones de control parental están relacionados con el administrador de paquetes de Android

**2** Como referencia, *Facebook* solicita 59 permisos, 16 de los cuales son peligrosos.

(posiblemente para monitorear las aplicaciones instaladas), y también para controlar el sistema ajustes. A pesar de que nos centramos principalmente en permisos peligrosos, es importante destacar que los no peligrosos también pueden ser dañinos. Un ejemplo es el permiso `BIND_ACCESSIBILITY_SERVICE`, que se solicita por 11 aplicaciones de la categoría de monitoreo, y 1 de las aplicaciones de restricción. Este permiso puede usarse para monitorear y controlar el bucle de retroalimentación de la IU y hacerse cargo del dispositivo [38]. Durante el proceso de instalación muchas de estas aplicaciones explican que dicho permiso es necesario para controlar mejor las acciones del niño. Asimismo, a pesar de no ser marcado explícitamente como "peligroso", algunos de los permisos de sistema obsoletos también son dignos de mención, ya que protegen los funcionalidades como la capacidad de recuperar la lista de ejecución procesos en el dispositivo. Además, el modelo de permisos se puede aprovechar para acceder a datos personales sin el consentimiento del usuario a través de canales laterales, como usar información WiFi para obtener ubicación a nivel de ciudad o la información de la dirección MAC como un identificador [70].[3] Si bien el tipo de servicio proporcionado por estas aplicaciones puede justificar el uso de permisos tan peligrosos, la presencia de librerías de terceros que pueden aprovechar estos privilegios para recopilar datos de los niños es una amenaza a la privacidad que analizaremos en detalle en § 5. [4]

En el otro lado del espectro, notamos que dos controles parentales las aplicaciones no solicitan ningún permiso peligroso. Uno de ellos (*Aplicación de control parental de Redgreentree*) reemplaza la configuración predeterminada de Android lanzador para permitir que el niño use solo aplicaciones aprobadas por el padre. La otra aplicación (*SaferKid*) es la versión parental (lo que explica la falta de permisos peligrosos) presentes en nuestro conjunto de datos porque los desarrolladores solo colgó la aplicación complementaria y no la versión para niños de la aplicación disponible en Google Play.

**Solicitudes de permisos anómalas.** Si bien la mayoría de las aplicaciones solicitan permisos peligrosos, encontramos que algunas son raramente utilizadas por la mayoría de las aplicaciones de control parental. Analizamos en profundidad el permisos que son solicitados por solo el 10%, o menos, de las aplicaciones en nuestro conjunto de datos, — considerando aplicaciones de supervisión y restricción por separado — para identificar si estos permisos están justificados. También buscamos cualquier información sobre su política de privacidad que pueda justificar su uso. La tabla 1 proporciona un resumen de los permisos para los que no encontramos justificación en la descripción de la aplicación o política de privacidad. Dos aplicaciones de restricción solicitan permisos para enviar SMS, procesar llamadas salientes y leer contactos. Sin embargo, solo pudimos encontrar una justificación para uno de ellos en la descripción de la aplicación. En cuanto a la categoría de seguimiento, identificamos siete aplicaciones que solicitan permisos anómalos (como recibir WAP push, grabar audio y leer calendario). Tres de ellos ya no están indexados en Google Play (*Kakatu*, *Family Orbit* y *Bitdefender*). Los cuatro restantes no justifican por qué requieren acceso a estos permisos en su Google Play descripción o política de privacidad.

**Solicitudes de permiso en versiones de aplicaciones.** Los estudios anteriores muestran que las aplicaciones de Android tienden a aumentar el número de solicitudes de permisos en las versiones de la aplicación [25, 80, 85]. Mientras que el 24% de las aplicaciones de nuestro conjunto de datos aumenta el número de permisos solicitados a lo largo del tiempo, descubrimos que otro 24% de las aplicaciones reducen la cantidad de permisos solicitado con el tiempo, *opuesto* a la tendencia general. Parte de esta disminución se explica por el hecho de que a principios de 2019 Google cambió su política de permisos para que las aplicaciones no pudieran acceder a SMS y permisos de llamadas a menos que fueran la aplicación de mensajería predeterminada [43].

**Aplicaciones de restricción vs. aplicaciones de seguimiento** El objetivo de las aplicaciones de seguimiento es recopilar datos de comportamiento y uso de teléfono y notificárselo a sus padres, ya sea a través de un portal web o en un sitio específico para padres aplicación complementaria. Por lo tanto, como revela la Figura 2, las aplicaciones de monitoreo tienden a solicitar permisos más peligrosos que las aplicaciones de restricción. La figura 3 profundiza en los casos específicos. Nuestras observaciones empíricas están alineadas con nuestras expectativas: en comparación con las aplicaciones de restricción, Las aplicaciones de monitoreo suelen solicitar los permisos necesarios para recopilar datos de niños. como geolocalización, leer registro de llamadas o leer SMS. La diferencia entre las aplicaciones

**3** De hecho, Android 10 introdujo permisos especiales para evitar el uso de la dirección MAC como substituto de la ubicación y el acceso a identificadores no reseteables

**4** Debido al modelo de permisos de Android, las bibliotecas de terceros heredan el mismo conjunto de permisos que la aplicación host.

**Table 1.** Solicitudes de permisos inusuales. Informamos si las aplicaciones han sido borrados de Google Play (columna GPlay).

| App | GPlay | Permissions |
|---|---|---|
| com.pdlp.android.app | | PROCESS_OUTGOING_CALLS<br>SEND_SMS |
| com.whisperarts.kidsshell | | READ_CONTACTS |
| com.appobit.familyorbit | ✓ | READ_CALENDAR |
| com.mmguardian.childapp | | RECORD_AUDIO |
| com.bitdefender.parental2013 | ✓ | RECEIVE_WAP_PUSH |
| com.sentry.kid | | READ_CALENDAR<br>RECORD_AUDIO |
| com.symantec.familysafety | | RECEIVE_WAP_PUSH |
| com.fsp.android.c | | READ_CALENDAR |
| com.kakatu.launcher | ✓ | RECORD_AUDIO |

de supervisión y restricción es notable incluso para permisos personalizados (ver Figura 2), y en en particular con respecto a los permisos de control del navegador. Las aplicaciones de segimiento acceden el historial de marcadores del navegador más que las aplicaciones de restriccion ; sin embargo, las aplicaciones de restricción tienden a depender más de permisos específicos del navegador para controlar la actividad de navegación en el dispositivo del niño.

**Posible difusión de información.** La alta tasa de solicitudes de permisos peligrosos no implica que las aplicaciones de control parental difundan información sensible a través de la red, ya sea a sus servidores propios o de terceros. Aplicamos análisis estático para estimar en qué medida estas aplicaciones acceden y difunden el información sensible a la que acceden y con quién. Usando el análisis de contexto y flujo implementado en Flowdroid [16], observamos que las aplicaciones en nuestro conjunto de datos incluyen 1.034 invocaciones de métodos para acceder a datos cuando se agregan, nunca menos de 78, y en promedio 324. Nosotros También observe que el 67% de las aplicaciones también tienen al menos 1 receptor—una parte del sistema operativo donde los datos pueden salir del sistema, como la interfaz de red—en código accesible, lo que sugiere posibles fugas de información. Flowdroid informa al menos un flujo de información válido en 14 de estas aplicaciones, con el caso extremo de *Kids Zone*, para el cual destaca *72 fugas potenciales*. Si bien parece que la mayoría de las fugas de información informadas implican registrar las acciones del usuario (por ejemplo, abrir una nueva actividad, registro de una autenticación fallida / exitosa, etc.), también observamos fugas más críticas que involucran datos sensibles como identificadores únicos. Específicamente, encontramos que dos aplicaciones (*SecureTeen* y *ShieldMyTeen*) comparten la dirección MAC y SSID a través de Internet (se pueden utilizar como canal lateral para identificar el dispositivo y geolocalizar al usuario [70]). Las aplicaciones mencionadas anteriormente y *Dinner Time Plus* también difunden el IMEI, un identificador único; y cuatro aplicaciones (*MMGuardian*, *Shield My Teen*, *GPS Tracker* y *Mobilefence*) difundir la geolocalización a nivel GPS. Seguiremos investiguando en § 5.2 el origen y el destino de estas fugas de información.

**Permisos personalizados.** Android ofrece a los desarrolladores la oportunidad de definir permisos personalizados para exponer partes de las funcionalidades de las aplicaciones a otras aplicaciones [81]. En el caso de permisos personalizados, el usuario nunca puede aceptarlos o rechazarlos, ya que se otorgan automáticamente sin mostrar una advertencia o formulario de consentimiento al usuario, a diferencia de los permisos oficiales de Android. Aunque no mostramos estos permisos en la Figura 2 por razones de claridad, incluimos un gráfico que muestra el número y tipo de permisos personalizados para cada aplicación en nuestro conjunto de datos en la Figura 5 en el Apéndice.

Encontramos 28 permisos personalizados que, a juzgar por su nombre, han sido declarados por los desarrolladores de aplicaciones de control parental. Encontramos ejemplos de permisos personalizados de aplicaciones complementarias, como el *Spin Browser* [21], que sustituye al navegador predeterminado del usuario, o la aplicación principal complementaria (por ejemplo *com.safekiddo.parent*). Estos permisos se utilizan desde la aplicación para niños para acceder o controlar funcionalidades de las aplicaciones complementarias. También encontramos aplicaciones que utilizan permisos personalizados declarados por otros desarrolladores, como la aplicación *Parents Around* con permisos personalizados de *Protect Your Kid*. Esto sugiere la existencia de acuerdos entre desarrolladores de aplicaciones para aprovechar la funcionalidad implementada por otras aplicaciones cuando ambas están instalados en el mismo dispositivo. También encontramos varias aplicaciones que utilizan permisos personalizados relacionados con los fabricantes de teléfonos, posiblemente habilitados por aplicaciones preinstaladas [39]. Estos permisos declarados por el proveedor permiten que la aplicación obtenga acceso a otras funciones del sistema no disponibles a través del proyecto oficial de código abierto

de Android. En algunos casos, como en el caso de Samsung KNOX API, los desarrolladores de aplicaciones deben convertirse en socios de Samsung para obtener acceso a sus API propietarias [74]. Aunque la aplicación de control parental *Parents Around* requiere acceso a permisos personalizados que pertenecen a cinco fabricantes, en general las aplicaciones de nuestro conjunto de datos tienden a declarar permisos para un proveedor o ninguno de ellos. Los permisos personalizados más frecuentes están relacionados con Samsung y son utilizados por varias versiones en 21 aplicaciones de nuestro conjunto de datos. Los permisos de proveedor más comunes son declarados por Huawei (10 aplicaciones), HTC (8 aplicaciones) y Sony y Oppo (4 aplicaciones).

**Table 2.** Clasificación, número y descripción de bibliotecas de terceros encontradas en aplicaciones de control parental.

| Categoría | Lib # | Descripción |
|---|---|---|
| Redes Sociales | 1 (60 pkgs) | Redes Sociales |
| Anuncios | 7 (82 pkgs) | Anuncios |
| Desarrollo | 56 (582 pkgs) | Herramientas de apoyo al desarrollo |
| Funcionalidad | 29 (172 pkgs) | Capacidades de la app (*e.g.,* animaciones) |
| Soporte | 43 (443 pkgs) | Librerías de soporte (*e.g.,* drivers de BD) |
| Analítica | 21 (220 pkgs) | Servicios de análisis de datos |
| Desconocido | 44 | Librerías no identificadas |

# 5 Análisis de librerías de terceros

Debido al modelo de permisos de Android, cualquier SDK integrado en una aplicación de Android hereda los privilegios y permisos de la aplicación anfitriona. Esto da a muchas organizaciones, incluidas proveedores externos que ofrecen análisis o publicidad servicios, acceso a los mismos datos que la aplicación de control parental.

Muchos proveedores de bibliotecas de terceros a menudo prohíben su uso en software para niños, como *Branch* [23] y *Appboy* (ahora renombrado como *Braze*) [24] debido a los estrictos marcos regulatorios implementados en los EE. UU. y la UE para proteger a los menores. Además, Google publicó en mayo de 2019 una lista de bibliotecas de terceros que autoverifican el cumplimiento de las disposiciones establecidas por el RGPD y COPPA [42].

En esta sección, inspeccionamos las aplicaciones de control parental—en todas las versiones de la aplicación—en nuestro conjunto de datos para encontrar librerías de terceros y clasificarlas por la funcionalidad proporcionada usando LibRadar [57]. Analizamos manualmente su salida para desinfectar los resultados y mejorar la cobertura de LibRadar, mapeándolos también a la organización real que presta el servicio. [5] Después de este proceso, pudimos identificar 157 bibliotecas únicas (44 no se pudieron clasificar debido al uso de técnicas de ofuscación de código). Luego, utilizamos información disponible públicamente para clasificar cada una de las bibliotecas por su propósito, incluidas sus propias descripciones de productos y foros de desarrolladores.

La tabla 2 se muestra para cada categoría resultante la cantidad de SDK encontrados, la cantidad total de nombres de paquetes que coinciden cada una de estas librerías, y una breve descripción de la categoría. La mayoría de las librerías de terceros integradas en aplicaciones de control parental son herramientas para soporte de desarrollo—librerías de desarrollo de propósito general,analizadores JSON, librerías de soporte de interfaz de usuario, etc—seguidos de SDK que ofrecen publicidad y servicios de análisis —por ejemplo, Flurry y AppsFlyer. La última categoría de SDK son más preocupante desde el punto de vista de la privacidad dado su comportamiento basado en datos y su negocio modelos. Por tanto, centramos nuestro análisis en las librerías que proporciona integración de redes sociales, publicidad en línea y servicios de análisis.

La figura 4 muestra que Google Ads, Google Firebase y Google Analytics están presentes en más del 50% de las aplicaciones, seguidos de Facebook SDK al 43%. Algunas de estas librerías pertenecen a la misma empresa matriz. Por ejemplo, Crashlytics, Firebase, Google Analytics y Google Ads todos pertenecen a Alphabet [3]. Por lo tanto, cuando agrupamos los SDK por su empresa matriz, podemos observar que Alphabet está presente en el 93% de las aplicaciones del conjunto de datos.

## 5.1 Apps violando los ToS de las librerías

Finalmente, estudiamos si las librerías de terceros integradas en cada aplicacióne de control parental permiten su uso en software orientado a niños en sus Térmi-

**5** Por ejemplo, LibRadar puede informar de varios nombres de paquetes para la misma biblioteca (*e.g.,* `com/paypal/.../onetouch` y `com/paypal/.../data`) por lo que agrupamos los que pertenecen al mismo proveedor: PayPal.

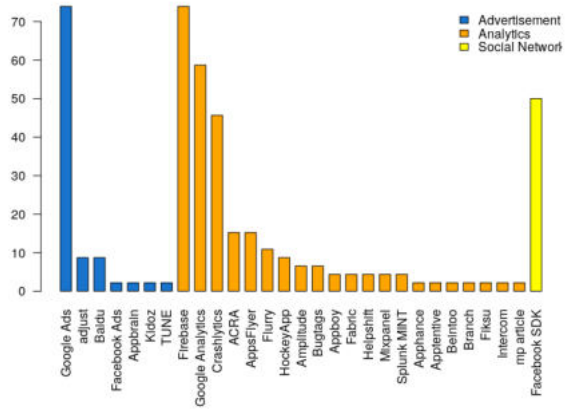


**Fig. 4.** Porcentaje de aplicaciones que utilizan librerías de publicidad, análisis y redes sociales.

nos de Servicio. Reyes *et al.* demostró que varios aplicaciones diseñadas para niños y publicadas en el programa Designed for Family de Google Play (DFF) utilizaban bibliotecas de terceros cuyos Términos de Servicio (ToS) prohíbían su integración en aplicaciones para niños [72]. Siguiendo esta información, utilizamos una canalización de análisis estático basado en Soot y Flowdroid [16, 83] para comprobar si las aplicaciones de control parental siguen un comportamiento similar. Observamos que algunos proveedores de SDK cambiaron sus ToS entre nuestro estudio y el trabajo anterior de Reyes *et al.*. También estudiamos si estas bibliotecas están incluidas en la lista de Google de SDK autocertificados como adecuados para aplicaciones para niños (a partir de mayo de 2019) [42].

Aunque tanto AppBoy como Branch aún indican que no deben incluirse en aplicaciones dirigidas directamente a los niños, nuestra canalización de análisis estático indica que están presentes en el software para niños como aplicaciones de control parental. Verificamos que dos aplicaciones en nuestro conjunto de datos (*GPS tracker* y *Qustodio*) integran estas bibliotecas en la última versión disponible de nuestro conjunto de datos (noviembre de 2018). De las siete bibliotecas de publicidad y análisis que encontramos en nuestro conjunto de datos, solo dos (AdMob y Unity) están presentes en la lista de Google. Incluimos la redacción relevante extraída de sus Términos de servicio en el Apéndice.

## 5.2 Quién maneja datos sensibles y para qué

Android no obliga a los desarrolladores a explicar a los usuarios si un permiso dado es necesario para la funcionalidad de la aplicación o si también es accedido por un SDK de terceros integrado. Por tanto, los usuarios no puede tomar decisiones informadas sobre si conceder un permiso dado a la aplicación o no en función de qué componente de software obtendrá acceso a ella. Para saber quién es el responsable de la recopilación de datos habilitada por un permiso dado, analizamos estáticamente el código de bytes de la versión más reciente de cada aplicación de control parental para buscar llamadas a la API de Android protegidas por permisos de Android y luego atribuir estas llamadas al código de la aplicación o a un SDK de terceros integrado. Para eso, actualizamos el mapeo entre permisos y llamadas a API protegidas realizadas originalmente por Au *et al.* para incorporar cambios recientes en el modelo de permisos de Android [17, 19]. Nosotros confiamos en la identificación de paquetes de LibRadar para atribuir las solicitudes de API protegidas a la aplicación real o cualquier SDK de terceros integrado.

La tabla **??** resume los resultados de este análisis. Por cada llamada de API protegida por permisos peligrosos, informamos si se usa solo en el código de aplicación, solo en el código de la librería, o por ambos. Tenemos una columna adicional que informa el porcentaje de usos para los que no podemos atribuir llamadas a la

**Table 3.** Atribución del uso de permisos al código que pertenece a aplicaciones o bibliotecas de terceros para cada permiso peligroso. La última columna informa de aquellos usos que no podemos atribuir.

| Permiso | % solo app | % solo SDK | % app & SDK | % desconocido |
|---|---|---|---|---|
| ACCESS_COARSE_LOCATION | 36 | 12 | 52 | 0 |
| ACCESS_FINE_LOCATION | 33 | 9 | 55 | 3 |
| CAMERA | 14 | 7 | 7 | 72 |
| GET_ACCOUNTS | 25 | 12 | 4 | 59 |
| PROCESS_OUTGOING_CALLS | 12 | 0 | 0 | 88 |
| READ_CALENDAR | 33 | 0 | 0 | 67 |
| READ_CONTACTS | 8 | 0 | 0 | 92 |
| READ_PHONE_STATE | 39 | 26 | 18 | 17 |
| READ_SMS | 19 | 0 | 6 | 75 |
| RECEIVE_MMS | 0 | 25 | 0 | 75 |
| RECORD_AUDIO | 20 | 20 | 0 | 60 |
| SEND_SMS | 27 | 27 | 18 | 28 |
| WRITE_CALL_LOG | 12 | 12 | 0 | 76 |
| WRITE_CONTACTS | 22 | 11 | 0 | 67 |
| WRITE_EXTERNAL_STORAGE | 6 | 41 | 47 | 6 |

API a cada componente de software por motivos tales como: *i*) el permiso solicitado por el desarrollador de la aplicación está en el archivo de manifiesto de Android pero no se invoca en el código; *ii*) nuestro método se pierde llamadas API relevantes debido a información incompleta en el mapeo de Au [17] [6]; y *iii*) el uso de técnicas de ofuscación de código. [7]

Un número significativo de llamadas a los métodos protegidos por permisos son invocados **solo por librerías de terceros**. Por ejemplo, las SDK integradas acceden el permiso de ubicación y el permiso de lectura de estado de teléfono, [8]—9% y 26% de las veces respectivamente—cuando la aplicación de host no requiere acceso a ellos. En otros casos, los SDK se aprovechan del conjunto de permisos ya solicitados por la aplicación anfitriona: *e.g.,* , el 55% de las veces que la aplicación solicita una ubicación precisa, una biblioteca de terceros también accede al permiso. Esto sugiere que los datos personales de los usuarios pueden recopilarse y procesarse para usos secundarios más allá de los ofrecidos por la aplicación.

Por aplicación, las aplicaciones *MMGuardian* y *Mobilefence* solo acceden a la ubicación geográfica de los usuarios en el código de la aplicación pero, para otras aplicaciones, solo en el código de terceros. Específicamente, observamos que la biblioteca *com.proximity*—la baliza de proximidad de Google— está incluída en la aplicación *ShieldMyTeen*. Este caso podría estar justificado por la necesidad de localizar al niño. La aplicación *GPS Tracker* filtra la ubicación en el código que pertenece a la biblioteca *Arity* [15], que es una plataforma que recopila información de ubicación para comprender mejor y mejorar la movilidad. Si bien encontramos esta biblioteca muy inusual para las aplicaciones de control parental, encontramos que esta aplicación es un "rastreador GPS familiar" que puede ser utilizado por los padres también. Los desarrolladores son muy explícitos en su política de privacidad sobre compartir datos con esta empresa para características de conducción presentes en la aplicación.

**6** A pesar de nuestros esfuerzos manuales para complementar el mapeo e incorporar cambios recientes en el modelo de control de permisos de Android, no podemos garantizar su integridad, ya que algunas asignaciones aún no están debidamente documentadas en la API de Android.

**7** Siete casos de aplicaciones que leen identificadores únicos como la dirección MAC, SSID e IMEI se identificaron en un código ofuscado, por lo que no se pudieron atribuir.

**8** Un permiso que permite leer identificadores de dispositivos únicos.

En la siguiente sección usamos análisis dinámico para omitir algunas de las limitaciones del análisis estático, reportando evidencias de la recopilación y difusión de datos personales de niños por parte de estas librerías de terceros.

# 6 Análisis dinámico

Los resultados de nuestro análisis estático muestran que algunas aplicaciones de control parental y los SDK de terceros integrados pueden recopilar y difundir datos personales de niños a Internet. En esta sección, utilizamos métodos de análisis dinámico para complementar nuestro análisis estático y recopilar pruebas reales de la difusión de datos personales a Internet. Con ese fin, realizamos las siguientes acciones de usuario para ejecutar y probar cada aplicación—o un par de aplicaciones si hay una versión para padres o una version acompañante— en nuestra base de datos:

A. Instalamos la aplicación y realizamos el proceso de configuración. Creamos una cuenta para padres cuando es necesario y otorgamos consentimiento para recopilar datos sensibles cuando se le solicite. Para realizar una comparación justa, cuando se nos solicita, configuramos cada aplicación para monitorear (o bloquear) las actividades de un niño menor de 13 años. También es importante tener en cuenta que ejecutamos todas las pruebas desde un país europeo (España) y que al crear la cuenta estamos consintiendo a la política de privacidad y los términos de servicio de la aplicación.
B. Debido a problemas de escalabilidad, no podemos probar todo el espectro de acciones de los niños que pueden ser bloqueados o supervisados por una aplicación de control parental. Por tanto, decidimos centrarnos en aquellos que tienen más probabilidades de ser bloqueados en función de sus solicitudes de permiso o caracteristicas anunciadas. Específicamente, interactuamos manualmente con el dispositivo de los niños durante cinco minutos de la siguiente manera: (*i*) visitamos un periódico en el navegador (esta acción suele estar permitida para niños), y también un sitio web pornográfico y un servicio de juegos de azar (este tipo de tráfico normalmente debería estar prohibido); (*ii*) abrimos un juego infantil permitido y una aplicación de citas potencialmente incluida en la lista negra; (*iii*) instalamos y desinstalamos un juego; (*iv*) tomamos una foto con la aplicación de cámara predetermi-

nada y ($v$)— mientras que el teléfono de prueba no tiene una tarjeta SIM— vamos a las aplicaciones de teléfono y SMS e intentamos hacer una llamada telefónica y enviar un mensaje.

Nuestro análisis estima un límite inferior de todos los posibles casos de difusión de datos personales que puedan existir en nuestro conjunto de datos de aplicaciones de control parental en comparación con nuestro análisis estático. Además, dado que la API de VPN de Android solo permite que una aplicación cree una interfaz en un momento determinado [9], nuestro método no nos permite probar completamente las 3 aplicaciones de control parental que requieren acceso a la interfaz VPN para monitorear la red de los niños. Seguimos informando sobre cualquier difusión de datos que suceden antes o durante la configuración de la interfaz VPN.

## 6.1 Servicios de terceros

Nuestros resultados confirman la alta presencia de componentes de terceros en aplicaciones para niños como se resume en la Tabla4. Observamos conexiones de red a una variedad de destinos en el registro flujos de red. Encontramos 49 diferentes dominios de segundo nivel en todas las aplicaciones, 18 de los cuales están asociados con Servicios de seguimiento y de anuncios de terceros de acuerdo con la lista desarrollada por Razaghpanah*et al.* [68]. El dominio más contactado es *Crashlytics*—ahora Firebase—que es un servicio de informe y análisis de errores propiedad de Google contactado por 54.8% de aplicaciones. Todos los dominios de terceros que se encuentran en nuestros experimentos de análisis dinámico pertenecen a SDK anteriormente informadas por nuestro método de análisis estático. Esto también verifica algunas de nuestras afirmaciones. Por ejemplo, el análisis dinámico confirma que la aplicación *GPS Tracker* contacta con el servicio *Branch*, una plataforma de análisis para aumentar los ingresos a través de "enlaces creados para adquirir, participar y medir en todos los dispositivos, canales y plataformas" [22] que no se supone que se use en software orientado a niños según sus propias Condiciones de servicio.

## 6.2 Recopilación y difusión de datos personales

Usando Lumen identificamos 513 flujos que contienen datos personales (*i.e.,* identificadores únicos persistentes y reiniciables, información de geolocalización, del punto de acceso WiFi que se puede utilizar como proxy para obtener la ubicación geográfica, y lista de paquetes instalados) generados por 42 (91%) diferentes aplicaciones. Observamos que el acceso al punto de acceso WiFi es un canal lateral conocido que ha sido utilizado como proxy para acceder a la ubicación geográfica de los usuarios [70].

El hecho de que veamos datos privados en el tráfico de la red no implica necesariamente una violación de la privacidad. Esta información puede cargarse en la nube para prestar el servicio previsto y para informar a la aplicación complementaria o el padre directamente a través de un panel web. De hecho, 74% de estas aplicaciones caen en la categoría de monitoreo, que son aquellas que solicitan un mayor conjunto de permisos. Sin embargo, algunos tipos de datos, como ID únicos y ubicación son extremadamente sensibles y no deben ser compartido con servicios de terceros, en particular los que ofrecen servicios de publicidad y seguimiento que no cumplen con las reglas de privacidad infantil. Observamos que 4 aplicaciones difunden la ubicación a un tercer dominio. Ejemplos de terceros que recopilan información de ubicación son SDK de análisis utilizados para la captación de clientes y el crecimiento de la aplicación (*Amplitude*) y servicios de notificaciones push (*OneSig-*

**Table 4.** Terceras partes más populares en referencia al número de apps que las contactan

| Servicio | Tipo | # apps |
|---|---|---|
| Crashlytics | Reporte de errores, Analítica | 23 |
| Facebook Graph | Red social, Anuncios, Analítica | 15 |
| Appsflyer | Analítica | 5 |
| Adjust | Fraude de anuncios, Marketing, Analítica | 3 |
| Google ads | Anuncios | 3 |
| OneSignal | Notificaciones push | 3 |

**Table 5.** Difusión de datos sin consentimiento

| Tipo de dato | Número de SLDs unicos | |
|---|---|---|
| | 1as partes | 3as partes |
| Android Advertisement ID | 2 | 8 |
| Android ID | 4 | 11 |
| Dirección MAC del AP | 1 | 0 |
| WiFi SSID | 2 | 0 |
| IMEI | 4 | 1 |
| Geolocalización | 0 | 1 |
| Email | 2 | 0 |

*nal*). Otros usos pueden ser para proporcionar un servicio a el padre, como en el caso de las API de mapeo (*Google Maps*). Ninguno de esos proveedores están en la lista de SDK de Google adecuados para aplicaciones orientadas a niños [42].

Google anima a los desarrolladores a utilizar el ID de publicidad de Android (AAID) como identificador único de usuario [5]. El AAID no es persistente y los usuarios puede restablecerlo u optar por no participar en la "personalización de anuncios" en su dispositivo. La combinación del AAID con otros identificadores persistentes sin el consentimiento explícito del usuario también es una violación de los Términos de Servicio [4]. A pesar de esto, encontramos 24 aplicaciones que recopilan y comparten identificadores persistentes como el IMEI y 58% aplicaciones que cargan el AAID junto con otros identificadores persistente, lo que anula el propósito de las ID reiniciables. Este comportamiento fue reportado anteriormente para aplicaciones infantiles regulares publicadas en el programa DFF [72]. Analizando más a fondo este problema, encontramos que la mitad de las aplicaciones que envían el AAID junto con otro identificador único lo hacen a una librería de terceros.

## 6.3 Consentimiento

Tanto COPPA como la RGPD establecen que las empresas deben obtener consentimiento de los padres antes de recopilar datos de niños por debajo del límite de edad (13 años para COPPA, 16 para GDPR) [29, 35]. Los desarrolladores de aplicaciones deben obtener consentimiento verificable por parte de un padre o tutor legal antes de recopilar datos personales sensibles del menor utilizando técnicas como enviar un correo electrónico, responder una serie de preguntas o proporcionar un documento de identificación o los detalles de la tarjeta de crédito en tiempo de ejecución [34]. Este requisito legal implica que simplemente informar a los padres o tutores legales sobre las prácticas de recopilación de datos en la política de privacidad no es suficiente, especialmente si la aplicación difunde información confidencial datos a servicios de terceros como se discutió anteriormente.

En nuestro análisis anterior, accedimos a la recopilación de datos en todos nuestros experimentos creando un cuenta y operando la aplicación haciéndonos pasar por un niño. Sin embargo, queremos determinar si las aplicaciones recopilan datos privados sin el consentimiento de los padres. Para ello, nos apoyamos en el método automático propuesto previamente por Reyes*et al.* [72]: lanzamos cada aplicación y la ejecutamos durante cinco minutos *sin* interactuar con ella. Esto implica que *no* damos nuestro consentimiento activo para la recopilación de datos y no realizamos ninguna de las acciones de los niños, optando en cambio por dejar la aplicación ejecutándose sin entrada. Como resultado, cualquier dato sensible o personal—particularmente identificadores únicos y geolocalización—cargados por la aplicación a terceros puede ser una posible violación de COPPA y GDPR.

Encontramos 67% aplicaciones que difunden datos personales sin consentimiento explícito y verificable. La información compartida por estas aplicaciones incluye identificadores únicos (es decir, el número de serie de Android, el AAID o el IMEI) y la ubicación de el usuario (incluidos métodos de ubicación alternativos como como el SSID o la dirección MAP del AP que han sido procesados por el FTC antes [36, 70, 72]). El 47% de todos los casos de divulgación de datos sin consentimiento van a un tercero. La tabla5 resume los tipos de datos difundidos por las aplicaciones probadas, agrupados por el tipo de datos que se difunden. Observamos que ninguna de estas librerías está en la lista de Google de certificadas adecuadas para niños SDK [42]. Creemos que algunas de estas instancias pueden corresponder a desarrolladores ser descuidado en la forma en que se integran librerías de terceros, sin asegurarse de que el usuario haya leído y aceptado su métodos de recopilación de datos antes de comenzar a recopilar datos.

## 6.4 (Falta de) Comunicaciones seguras

Tanto la regla COPPA [35] como la RGPD [29] tienen claras disposiciones que establecen que los desarrolladores deben tratar los datos sobre niños con un grado apropiado de seguridad [40, 47]. Para evaluar que este es el caso, estudiamos si las aplicaciones de control parental utilizan el cifrado (por ejemplo, TLS) para cargar los datos a la nube. La tabla6 resume los flujos no cifrados, ordenados por pares de aplicaciones y dominios, así como el tipo de datos sensibles que se transmiten de forma clara. Encontramos instancias de identificadores persistentes que permiten el seguimiento de usuarios, por ejemplo, el IMEI y el AAID, o información de geolocalización, siendo enviados en claro. Por último, observamos una aplicación (*Secure Kids*) envía sin cifrar la lista de paquetes instalados (utilizada en el servidor para permitir a los padres bloquear aplicaciones no deseadas) junto con una cadena similar a un identificador (DEV_ID). La aplicación *com.kiddoware.kidsafebrowser* aparece en nuestros re-

**Table 6.** Apps enviando información sensible sin cifrar

| Aplicación | Tipo de dato | Destino |
|---|---|---|
| com.kidoz | AAID | kidoz.net |
| ru.kidcontrol.gpstracker | IMEI & Localización | 85.143.223.160 |
| com.parentycontrol | Email | parentycontrol.com |
| com.safekiddo.kid | IMEI | safekiddo.com |
| com.kiddoware.kidsplace | Android ID | kiddoware.com |
| com.kiddoware.kidsafebrowser | Android ID & Hardware ID | kiddoware.com |

sultados porque se instala como el navegador web predeterminado por una de las aplicaciones en el conjunto de datos.

# 7 Análisis de Políticas de Privacidad

Tanto la RGPD como COPPA requieren que los desarrolladores de aplicaciones proporcionen condiciones claras de uso y políticas de privacidad para el usuario final. Sin embargo, se sabe que las políticas de privacidad puede ser difícil de entender—incluso produciendo diferentes interpretaciones— por el usuario promedio [52, 65, 77, 86]. Inspeccionamos manualmente las políticas de privacidad indexadas por Google Play Store para cada aplicación de nuestro corpus para analizar en qué medida los desarrolladores de aplicaciones de control parental respetan las obligaciones de transparencia exigidas por la normativa. Para evitar sesgos introducidos por interpretaciones ambiguas de las políticas, dos autores conducen análisis manual de cada política, y discuten con un tercer autor en caso de desacuerdo. Observamos que solo el 89% de los desarrolladores de aplicaciones había publicado una política de privacidad en su perfil de Google Play en el momento de realizar nuestro estudio en febrero de 2018. Discutimos los resultados de nuestro análisis de política de privacidad a lo largo de cuatro eje, incluidos ejemplos de redacción que se encuentran en el políticas de privacidad como ejemplos:

**Consideraciones generales:** Primero, analizamos si la política se puede encontrar fácilmente en Google Play, si proporciona información clara sobre la empresa (*i.e.,* ubicación de la empresa, propósito principal, otras aplicaciones) y si los usuarios son notificados sobre los cambios en la política. Descubrimos que 95% de aplicaciones proporciona un enlace directo a sus políticas en su perfil de Google Play, y 10% de las aplicaciones proporcionan información sobre las empresas (*e.g., La "Compañía" o "Nosotros", con domicilio en [...]*). Sin embargo, a pesar de que los cambios en ñas políticas de privacidad a lo largo del tiempo son difíciles de controlar por parte de los usuarios, solo 20% de las aplicaciones notifican activamente a los usuarios sobre cambios en las políticas.

**Prácticas de recolección de datos:** Encontramos que la mayoría de las políticas de privacidad (92.6%) informan del tipo de datos que se recopilan de los menores. Sin embargo, sólo algunos de ellos (54%) informan claramente a los usuarios de cómo se procesan estos datos y con qué finalidad (*e.g., Su cuenta y sus datos de contacto se utilizan para administrar nuestra relación contigo*). También vemos que solo aproximadamente la mitad (56%) de las políticas describen cuánto tiempo se almacenarán los datos recopilados en los servidores del desarrollador.

**Prácticas de envío de datos:** Verificamos si las aplicaciones son transparentes cuando se refieren al uso de servicios de terceros en sus políticas cotejando estas políticas con nuestros hallazgos empíricos sobre el uso de bibliotecas de terceros y difusión de datos (§ **??**). Dado que la RGPD introdujo la necesidad de nombrar a las empresas de terceros que reciben datos personales, lo comprobamos en las 25 aplicaciones para las que tenemos políticas de privacidad recopilados después de que el GDPR entró en vigencia en el 25 de mayo de 2018. La tabla 7 muestra la cantidad de aplicaciones que utilizan un servicio de terceros y cuántos de ellos realmente informan esto en su política de privacidad (*e.g., Google puede usar los Datos recopilados para contextualizar y personalizar los anuncios de su propia red publicitaria*). Sólo 28.0% de ellas nombran todos los servicios de terceros que encontramos durante el tiempo de ejecución, mientras 79% de las aplicaciones estudiadas no nombran ninguna tercera parte con las que comparten datos privados. Observamos que estas últimas están potencialmente en violación de COPPA y GDPR por no ser claros sobre las política de intercambio de datos con sus socios. Además, encontramos una aplicación que comparte datos de ubicación con un servicio de terceros, also que puede constituir un potencial violación de la regla COPPA de la FTC que prohíbe la recolección de la geolocalización de los niños (a nivel suficiente para identificar el nombre de una calle y una ciudad o pueblo). Si bien esta aplicación no está dirigida solo a niños, su nombre de empresa es *Family Safe Productions*, lo que sugiere que se puede usar para monitorear ubicaciones secundarias. Sin embargo, dicen abiertamente en su política que pueden compartir datos de ubicación con

**Table 7.** Presencia de terceras partes en la política de privacidad de las app

| Servicio | Tipo | # apps | # apps nombrandolo en la política |
|---|---|---|---|
| Crashlytics | Reporte de errores y Analítica | 23 | 5 |
| Facebook Graph | Redes Sociles, Anuncios y Analítica | 15 | 3 |
| Appsflyer | Analítica | 5 | 1 |
| Adjust | Fraude de anuncios, Marketing, Analítica | 3 | 0 |
| Google ads | Anuncios | 3 | 1 |
| OneSignal | Notificaciones Push | 3 | 1 |
| Amplitude | Analítica | 2 | 0 |
| Help Shift | Servicio de usuarios | 1 | 0 |
| Apptentive | Analítica, Participación del usuario | 1 | 0 |
| Branch | Analítica | 1 | 0 |
| Splunk | Analítica | 1 | 0 |

terceros (como se informa en § 5.2). Observamos que no encontramos este comportamiento en nuestros experimentos de análisis dinámico.

**Cumplimiento de la regulación:** También estudiamos el conocimiento de los desarrolladores sobre diferentes regulaciones. Solamente 22% de aplicaciones reclaman el cumplimiento de COPPA en su política; mientras que solo 10% de políticas habla de la legislación europea, 37% mencionan su cumplimiento de las leyes locales (*e.g., Nuestra Política de privacidad y nuestras prácticas de privacidad se adhieren a las Ley de protección de la privacidad en línea de los niños de los estados ("COPPA"), así como otras leyes aplicables*).

**Derechos de los usuarios**: Finalmente, verificamos los derechos y opciones que los usuarios tienen sobre sus datos. Para hacerlo, analizamos la cantidad de aplicaciones que permiten a los usuarios optar por no participar en las prácticas de recopilación de datos sin tener que dejar de usar la aplicación, y cuántas aplicaciones le dan al usuario la oportunidad de corregir, eliminar o acceder a sus datos. Encontramos que en 46% de aplicaciones, los usuarios pueden optar por no participar en la recopilación de datos, donde 63% de aplicaciones les da a los usuarios al menos una de los opciones anteriores (*e.g., Según los datos aplicables de la RGPD, los interesados tendrán derecho a acceder a datos, rectificación, supresión, limitación del tratamiento [...]*).

## 7.1 El efecto RGPD

Primero analizamos las políticas de privacidad al comienzo de nuestro estudio, unos tres meses antes de que el RGPD entrara en vigor en mayo de 2018. Si bien no revisamos todo el análisis, usamos los resultados de nuestro estudio para evaluar la evolución de las políticas de privacidad para las 25 aplicaciones que comparten datos con terceros y que todavía están disponibles después del 25 de mayo de 2018. Nuestro objetivo es saber si las empresas cambiaron sus políticas, y comprenden el impacto de la ley en el caso específico de las aplicaciones de control parental. Al comparar las políticas más nuevas con las de nuestro análisis anterior, encontramos que 2 tiene cambios importantes en su política de privacidad después de RGPD. Mirando con más detalle los casos específicos, encontramos que una aplicación inicialmente no nombró a sus socios de intercambio de datos en la política de privacidad, y luego agregó esta info. Otra aplicación no explicaba claramente el tipo de datos que se recopilaban, y ahora ha cambiado su política para ser más claro. Sin embargo, vemos que la mayoría de las políticas aún no son claras, ya que a menudo omiten los nombres de los servicios de terceros utilizados por la app. Por lo tanto, incluso cuando los marcos regulatorios presionan para arrojar luz sobre el ecosistema móvil de terceros, vemos la necesidad de auditar las aplicaciones móviles de control parental más allá de los aspectos referentes a la usabilidad y sus capacidades.

# 8 Discusión y Limitaciones

Nuestro análisis multilateral de las aplicaciones de control parental saca a la luz una gran cantidad de comportamientos indeseables con respecto a la privacidad de los niños. Primero, las aplicaciones de control parental solicitan una gran cantidad de permisos invasivos. Esto, combinado con el número de análisis y las SDK de publicidad integrados en estas aplicaciones representan una grave amenaza para los niños. Estas librerías no solo aprovechan la gran cantidad de permisos confidenciales solicitados por aplicaciones de control parental para recopilar información personal; sino que también utilizan varios permisos solicitados únicamente por componentes de terceros. También encontramos evidencia empírica de prácticas de intercambio de datos con terceros: 72% de las aplicaciones comparten datos con un SDK de terceros y en 67% apps este intercambio ocurre sin el con-

sentimiento de los padres explícito y verificable. En algunos casos observamos que la carga de datos sensibles en línea los servidores ocurren sin cifrado. Finalmente, nuestro análisis de las políticas de privacidad de las aplicaciones revela que están lejos tener claras sus prácticas de recopilación de datos y, por lo general, no informar sobre qué datos se comparten con otros servicios. Estas prácticas ponen en duda el cumplimiento normativo de muchas de estas aplicaciones.

Dados los graves riesgos de privacidad revelados por nuestro análisis, consideramos que las implicaciones de privacidad deben ser una parte fundamental de cualquier guía diseñada para padres. Comparamos nuestros hallazgos con recomendaciones existentes de organismos públicos para ayudar a los padres a decidir si usar este tipo de software y qué herramienta es más segura. Nuestro conjunto de datos contiene 5 de las 10 aplicaciones comparadas en la prueba comparativa SIP [33] por la Comisión Europea, que se centra en la usabilidad y la resistencia a los intentos de eludir a los niños. A continuación, dos de estas aplicaciones tiene prácticas de riesgo de privacidad: *Qustodio* (también mencionada en una gran cantidad de estudios en línea que recomiendan las mejores aplicaciones de control parental [66, 73]) comparte datos con terceros sin consentimiento, y *Parentsaround* lo hace además de compartir identificadores únicos con servicios de terceros. También comparamos nuestros resultados con IS4K Cybersecurity, que enumera una serie de aplicaciones, enumerando sus funcionalidades sin cualquier juicio sobre su idoneidad. Nuestro conjunto de datos incluye 6 de las 10 aplicaciones en su lista. Tres de estas aplicaciones comparten datos confidenciales con terceros sin consentimiento apropiado, y otra aplicación envía datos sin cifrar.

Además, argumentamos que las tiendas de aplicaciones deben tomar medidas adicionales para verificar que las aplicaciones dirigidas a niños cumplen con la legislación vigente y tratan los datos de los niños con sumo cuidado, incluso si no están en el programa diseñado para familias. Si bien un análisis completo y exhaustivo de las aplicaciones sería inviable, un análisis estático que muestre la presencia de librerías de análisis y publicidad en aplicaciones que serán utilizadas por menores, incluidos los SDK que prohíben su uso en aplicaciones para niños, deberían generar inquietudes. Además, un análisis dinámico simple para verificar que estas aplicaciones usan las medidas de seguridad básicas, como el uso de cifrado, ya ayudarían a reducir los riesgos para la privacidad de los niños.

**Comparación con apps de una naturaleza diferente.** En este trabajo mostramos que las aplicaciones de control parental a menudo se comportan mal, generando amenazas a la privacidad de los niños e incluso de los padres. Sin embargo, no podemos decir que tienen un comportamiento peor que otras aplicaciones de Android, incluso las aplicaciones para niños estudiadas en la literatura [68, 72]. Estudios anteriores muestran que la mala conducta en materia de seguridad y privacidad es una tendencia común en las aplicaciones de Android: a menudo solicitan más permisos de los necesarios [**?** ], e incluyen una gran cantidad de librerías de terceros [57, 68]. En cuanto a los riesgos de privacidad de las aplicaciones para niños publicadas en En el programa Designed for Families de Google Play, Irwin*et al.* demostró que casi el 50% de las aplicaciones estaban potencialmente violadando la regla COPPA [72].

Al igual que en el caso de las aplicaciones para niños presentes en el programa DFF de Google, las aplicaciones de control parental deben cumplir con las Reglamento y disposiciones especiales. Por definición, están dirigidos a niños. Sin embargo, ninguna de las aplicaciones analizadas en este estudio figura en el programa DFF de Google Play. Mientras que trabajos anteriores han demostrado que las aplicaciones de Android tienden a recopilar una gran cantidad de datos de usuarios [64, 68], en algunos casos incluso evitando la mecanismos de seguridad implementados por la plataforma [60, 70], el hecho de que las aplicaciones de control parental potencialmente no cumplan con la regulación es mucho más preocupante, tanto para los padres como para los menores.

De hecho, existe un gran elemento de confianza de los padres hacia los desarrolladores de soluciones de control parental, que se rompe cuando estos servicios tratan los datos de los niños de forma descuidada, compartirlos con terceros o enviarlos a través de Internet sin cifrar. Esta mala conducta y la incapacidad de los padres para auditar las aplicaciones móviles llama a la acción de los investigadores y agencias de protección de datos para comprender la forma en que estas aplicaciones pueden estar violando la legislación vigente e invocar acciones regulatorias para arreglar estos asuntos. Hasta ese momento, algunos estudios proponen el uso de soluciones no técnicas para el control parental  cite livingstone2008parental.

**Limitaciones.** Nuestro método de recopilación de aplicaciones se basa en el uso de las capacidades de búsqueda gratuitas de Google Play Store, lo que significa que no exploramos todas las aplicaciones de control parental en el mercado. Sin embargo, creemos que

el conjunto de aplicaciones elegidas es representativo en popularidad, características y comportamiento del desarrollador. Además, dado que nuestra recopilación de datos inicial comenzó dos años antes a la entrega, algunas aplicaciones se eliminaron del mercado durante nuestro análisis y aparecieron nuevas aplicaciones. Repetimos el proceso de recopilación de datos más adelante en nuestro estudio. para encontrar aplicaciones recién publicadas, y descargamos la versión histórica de cada aplicación que analizamos para cubrir siempre el mismo período de tiempo.

A pesar de combinar análisis estático y dinámico, reconocemos que nuestro análisis no puede garantizar una cobertura completa del código, características de la aplicación o los flujos de datos. Primero, el análisis estático perderá rutas de código implementado en código nativo u ofuscado. En segundo lugar, LibRadar utiliza un base de datos para identificar bibliotecas de terceros y no puede detectar bibliotecas que no están presentes en esta base de datos. En tercer lugar, Lumen puede fallar flujos que no son activados por nuestras acciones predefinidas. Además, realizamos nuestro análisis dinámico en la aplicación para niños, y puede ser que la aplicación para padres complementaria difunda datos sensibles a través de la red. Además, nuestro proxy Man-in-the-middle es incapaz de interceptar los flujos de TLS para 2 aplicaciones que podrían usar técnicas como Fijación de certificados TLS [67]. Finalmente, nuestro análisis dinámico ha sido ejecutado desde un banco de pruebas geolocalizado en la Unión Europea. Sería necesario verificar nuestras afirmaciones en EE. UU. para investigar más a fondo las posibles violaciones de la COPPA.

# 9 Trabajo relacionado

Los investigadores recurren al análisis estático o dinámico, o una combinación de ambos, como en nuestro estudio, para analizar el comportamiento de aplicaciones móviles. Se han utilizado técnicas de análisis estático para identificar posibles fugas de información en Android [16, 54], para extraer características de comportamiento para malware detección [18, 37], o para estudiar la evolución de Android ecosistema [25, 70, 80, 85**?** ]. Del mismo modo, se han utilizado muchas técnicas de análisis dinámico para la propósitos iguales o similares [32, 51, 64, 69, 78], a pesar de los desafíos para escale y automatice el análisis a grandes conjuntos de datos [28, 72]. Si bien confiamos en técnicas estáticas y dinámicas similares para nuestro estudio, el objetivo final es bastante diferente, ya que ninguno de estos trabajos se centra en los aspectos de privacidad de las aplicaciones de control parental.

Nos basamos en trabajos anteriores sobre el dominio de aplicaciones de control parental y la privacidad de los niños. Ha habido estudios sobre la efectividad de las soluciones de control parental: Mathiesen argumentó que tales políticas son una violación del derecho de los niños a privacidad [59] mientras Wisniewski *et al.* presentó un estudio completo de las características ofrecidas por las aplicaciones de control parental y concluyó que las características de monitoreo invasivo de la privacidad son más comunes que las que se centran en autoregulación del adolescente [87]. Además, Eastin *et al.* demostró que el estilo de crianza tiene un efecto sobre el tipo de las restricciones que los padres establecen en el teléfono de sus hijos [31].

Creemos que este es el primer estudio que analiza el implicaciones de privacidad de las aplicaciones de control parental de un tecnológico punto de vista. Otros han estudiado las implicaciones de privacidad para los niños en dominios como las redes sociales [58] y juguetes inteligentes [82, 88]. Reyes *et al.* [72] es el trabajo más cercano al nuestro desde un punto de vista metodologico. Analizan el cumplimiento de las aplicaciones móviles con la normativa COPPA. Mientras algunos de sus hallazgos son similares a los que presentamos en este artículo, nuestro trabajo es un análisis más completo del control parental móvil ecosistema de aplicaciones. Chatterjee*et al.* también estudió a los padres ecosistema de control. Sin embargo, se centran en evaluar cómo se pueden utilizar dichas aplicaciones para otros fines (por ejemplo software espía y violencia de pareja) [27].

# 10 Conclusiones

Hemos presentado el primer estudio multidimensional del ecosistema de aplicaciones de control parental desde una perspectiva de privacidad. Nuestros hallazgos abren un debate sobre los riesgos de privacidad introducido por estas aplicaciones. ¿El potencial del control parental aplicaciones para proteger a los niños justifica los riesgos relacionados con la colección y tratamiento de sus datos?

Esperamos que nuestro estudio cree conciencia en los padres y las autoridades reguladoras sobre los riesgos planteados por algunas de estas aplicaciones. Recalcamos que es fundamental para complementar las ini-

ciativas actuales de evaluación comparativa [1, 33] con una seguridad y análisis de privacidad para ayudar a los padres a elegir la mejor aplicación mientras teniendo en cuenta estos aspectos.

# References


[1] https://www.is4k.es/.

[2] R. Alexander, "How to protect children from internet predators: a phenomenological study," *ANNUAL REVIEW OF CYBERTHERAPY AND TELEMEDICINE 2015*, p. 82, 2016.

[3] Alphabet, "Alphabet - Home Page," https://abc.xyz/.

[4] Android, " Usage of Android Advertising ID," https://play.google.com/intl/en-GB/about/monetization-ads/ads/ad-id/index.html.

[5] ——, "Best practices for unique identifiers," https://developer.android.com/training/articles/user-data-ids.

[6] ——, "Permissions overview," https://developer.android.com/guide/topics/permissions/overview.

[7] ——, "Play Protect," https://www.android.com/play-protect/.

[8] ——, "UI/Application Exerciser Monkey," https://developer.android.com/studio/test/monkey.

[9] ——, "VpnService," https://developer.android.com/reference/android/net/VpnService.

[10] ——, "Android developer manual: permission model," 2018, https://developer.android.com/guide/topics/permissions/overview.

[11] Android Developers, "App Manifest Overview," https://developer.android.com/guide/topics/manifest/manifest-intro.

[12] ——, "Privacy changes in Android 10," https://developer.android.com/about/versions/10/privacy/changes.

[13] ——, "VPN Service," https://developer.android.com/reference/android/net/VpnService.

[14] APKPure, "Homepage," https://apkpure.com/.

[15] Arity, "Arity," https://www.arity.com.

[16] S. Arzt, S. Rasthofer, C. Fritz, E. Bodden, A. Bartel, J. Klein, Y. Le Traon, D. Octeau, and P. McDaniel, "FlowDroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for Android apps," in *PLDI 2014*, 2014.

[17] K. W. Y. Au, Y. F. Zhou, Z. Huang, and D. Lie, "Pscout: Analyzing the android permission specification," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, ser. CCS '12. ACM, 2012.

[18] V. Avdiienko, K. Kuznetsov, A. Gorla, A. Zeller, S. Arzt, S. Rasthofer, and E. Bodden, "Mining apps for abnormal usage of sensitive data," in *ICSE '15*, 2015, pp. 426–436.

[19] M. Backes, S. Bugiel, E. Derr, P. McDaniel, D. Octeau, and S. Weisgerber, "On demystifying the android application framework: Re-visiting android permission specification analysis," in *USENIX Security 2016*, 2016, pp. 1101–1118.

[20] BBC News, "Web porn: Just how much is there?" 2013, https://www.bbc.com/news/technology-23030090.

[21] Boomerang, "Spin Browser," https://useboomerang.com/spin/.

[22] Branch.io, "Homepage," https://branch.io.

[23] ——, "Terms of Service," https://branch.io/policies/#terms-and-conditionss.

[24] Braze (formerly AppBoy), "Privacy," https://www.braze.com/privacy/.

[25] P. Calciati and A. Gorla, "How do apps evolve in their permission requests?: A preliminary study," in *MSR '17*. IEEE Press, 2017.

[26] P. Calciati, K. Kuznetsov, X. Bai, and A. Gorla, "What did really change with the new release of the app?" in *MSR 2018*, 2018.

[27] R. Chatterjee, P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy, and T. Ristenpart, "The spyware used in intimate partner violence," in *2018 IEEE Symposium on Security and Privacy (SP)*, 2018.

[28] S. R. Choudhary, A. Gorla, and A. Orso, "Automated test input generation for android: Are we there yet?" *arXiv preprint arXiv:1503.07217*, 2015.

[29] Council of European Union, "General Data Protection Regulation 679/2016," 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[30] Cyberbullying Research Center, "Summary of Our Cyberbullying Research (2004-2016)," https://cyberbullying.org/summary-of-our-cyberbullying-research.

[31] M. S. Eastin, B. S. Greenberg, and L. Hofschire, "Parenting the internet," *Journal of communication*, vol. 56, no. 3, pp. 486–504, 2006.

[32] W. Enck, P. Gilbert, S. Han, V. Tendulkar, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones," *TOCS*, vol. 32, no. 2, p. 5, 2014.

[33] Europen Comission, "Benchmarking of parental control tools for the online protection of children ," 2017, https://www.sipbench.eu/index.cfm/secid.1/secid2.3.

[34] Federal Trade Comission, "Get Parents' Verifiable Consent Before Collecting Personal Information rom Their Kids." https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step4.

[35] ——, " Children's Online Privacy Protection Act, (15 U.S.C. 6501, et seq.,) ," 1998, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

[36] ——, "Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission," 2016,

https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked.

[37] Y. Feng, S. Anand, I. Dillig, and A. Aiken, "Apposcopy: Semantics-based detection of android malware through static analysis," in *FSE 2014*. New York, NY, USA: ACM, 2014, pp. 576–587. [Online]. Available: http://doi.acm.org/10.1145/2635868.2635869

[38] Y. Fratantonio, C. Qian, S. Chung, and W. Lee, "Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop," in *S&P*, 2017.

[39] J. Gamba, M. Rashed, A. Razaghpanah, J. Tapiador, and N. Vallina-Rodriguez, "An analysis of pre-installed android software," in *S&P*, 2020.

[40] S. Gambs, M.-O. Killijian, and M. N. n. del Prado Cortez, "Show me how you move and i will tell you who you are," in *Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*, ser. SPRINGL '10. ACM, 2010.

[41] Google, "Families," https://play.google.com/about/families/.

[42] ——, "Google Play certified ad networks program," https://support.google.com/googleplay/android-developer/answer/9283445.

[43] ——, "Providing a safe and secure experience for our users ," https://android-developers.googleblog.com/2018/10/providing-safe-and-secure-experience.html.

[44] Google Play, "Kid Control Dev profile," https://play.google.com/store/apps/dev?id=6687539553449035845.

[45] ——, "Yoguesh Dama profile," https://play.google.com/store/apps/dev?id=5586168019301814022.

[46] Google Play Store — FamilySafety Production, "GPS Phone Tracker," 2018, https://play.google.com/store/apps/details?id=com.fsp.android.c.

[47] Herald Sun, "Police warn photos of kids with geo-tagging being used by paedophiles," 2012, https://www.heraldsun.com.au/technology/news/photograph-uploads-put-kids-at-risk/news-story/9ef00e4105cb1d38d8f5acb77d6c7433.

[48] IAPP, "GDPR Article 8," https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A8.

[49] ——, "GDPR Recital 38," https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#R38.

[50] Internet Safety 101, "Internnet Safety," https://internetsafety101.org/.

[51] S. Jain, M. Javed, and V. Paxson, "Towards mining latent client identifiers from network traffic," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 2, pp. 100–114, 2016.

[52] C. Jensen and C. Potts, "Privacy policies as decision-making tools: an evaluation of online privacy notices," in *SIGCHI*. ACM, 2004.

[53] Kiddoware, "Kiddoware homepage," https://kiddoware.com/.

[54] L. Li, A. Bartel, T. F. Bissyandé, J. Klein, Y. Le Traon, S. Arzt, S. Rasthofer, E. Bodden, D. Octeau, and P. McDaniel, "Iccta: Detecting inter-component privacy leaks in android apps," in *ICSE '15*, 2015, pp. 280–291.

[55] S. Livingstone, L. Haddon, A. Goerzig, and K. Ólafsson, "Risks and safety on the internet: The perspective of european children. full findings," 01 2011.

[56] S. Livingstone, L. Haddon, A. Görzig, and K. Ólafsson, "Risks and safety for children on the internet: the uk report," *Politics*, vol. 6, no. 1, 2010.

[57] Z. Ma, H. Wang, Y. Guo, and X. Chen, "Libradar: Fast and accurate detection of third-party libraries in android apps," in *ICSE 2016*. ACM, 2016.

[58] M. Madden, A. Lenhart, S. Cortesi, U. Gasser, M. Duggan, A. Smith, and M. Beaton, "Teens, social media, and privacy," *Pew Research Center*, vol. 21, pp. 2–86, 2013.

[59] K. Mathiesen, "The internet, children, and privacy: the case against parental monitoring," *Ethics and Information Technology*, vol. 15, no. 4, pp. 263–274, 2013.

[60] Y. Michalevsky, D. Boneh, and G. Nakibly, "Gyrophoone: Recognizing speech from gyroscope signals," in *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, 2014, pp. 1053–1067.

[61] Monica Anderson, "Parents, Teens and Digital Monitoring," https://stirlab.org/wp-content/uploads/2018/06/2017_Wisniewski_ParentalControl.pdf.

[62] New York Times, "Uber hid 2016 breach, paying hackers to delete stolen data," 2017, https://www.nytimes.com/2017/11/21/technology/uber-hack.html.

[63] Ofcom: UK broadband, home phone and mobile services regulator, "Children and parents: Media use and attitudes report 2018," 2018, https://www.ofcom.org.uk/___data/assets/pdf_file/0024/134907/Children-and-Parents-Media-Use-and-Attitudes-2018.pdf.

[64] E. Pan, J. Ren, M. Lindorfer, C. Wilson, and D. Choffnes, "Panoptispy: Characterizing audio and video exfiltration from android applications," *Proceedings on Privacy Enhancing Technologies*, 2018.

[65] H. J. Pandit, D. O'Sullivan, and D. Lewis, "Queryable provenance metadata for gdpr compliance," 2018.

[66] PCMag, "The Best Parental Control Software of 2019," https://uk.pcmag.com/parental-control-monitoring/67305/the-best-parental-control-software.

[67] A. Razaghpanah, A. A. Niaki, N. Vallina-Rodriguez, S. Sundaresan, J. Amann, and P. Gill, "Studying tls usage in android apps," in *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*. ACM, 2017, pp. 350–362.

[68] A. Razaghpanah, R. Nithyanand, N. Vallina-Rodriguez, S. Sundaresan, M. Allman, C. Kreibich, and P. Gill, "Apps, Trackers, Privacy and Regulators: A Global Study of the Mobile Tracking Ecosystem," in *Network and Distributed System Security Symposium*, Feb. 2018.

[69] A. Razaghpanah, N. Vallina-Rodriguez, S. Sundaresan, C. Kreibich, P. Gill, M. Allman, and V. Paxson, "Haystack: In situ mobile traffic analysis in user space," *CoRR*, 2015.

[70] J. Reardon, Á. Feal, P. Wijesekera, A. E. B. On, N. Vallina-Rodriguez, and S. Egelman, "50 ways to leak your data: An exploration of apps' circumvention of the android permissions system," in *28th {USENIX} Security Symposium ({USENIX}*

*Security 19)*, 2019, pp. 603–620.

[71] J. Ren, M. Lindorfer, D. J. Dubois, A. Rao, D. Choffnes, and N. Vallina-Rodriguez, "Bug fixes, improvements,... and privacy leaks," *NDSS*, 2018.

[72] I. Reyes, P. Wijesekera, J. Reardon, A. E. B. On, A. Razaghpanah, N. Vallina-Rodriguez, and S. Egelman, ""won't somebody think of the children?" examining coppa compliance at scale," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 3, pp. 63–83, 2018.

[73] SafeWise, "Best Parental Control Apps and Software Buyers Guide," https://www.safewise.com/resources/parental-control-filters-buyers-guide/.

[74] Samsung, "Knox SDK," https://seap.samsung.com/sdk/knox-android.

[75] Screentime Labs, "Screentime homepage," https://screentimelabs.com/.

[76] B. Shmueli and A. Blecher-Prigat, "Privacy for children," *Colum. Hum. Rts. L. Rev.*, vol. 42, p. 759, 2010.

[77] R. Slavin, X. Wang, M. B. Hosseini, J. Hester, R. Krishnan, J. Bhatia, T. D. Breaux, and J. Niu, "Toward a framework for detecting privacy policy violations in android application code," in *International Conference on Software Engineering*. ACM, 2016.

[78] S. Son, D. Kim, and V. Shmatikov, "What mobile ads know about mobile users." in *NDSS*, 2016.

[79] Statista, "Mobile Internet," 2018, https://www.statista.com/topics/779/mobile-internet/.

[80] V. F. Taylor and I. Martinovic, "To updae or not to update: Insights from a two-year study of android app evolution," in *ASIA CCS '17*. ACM, 2017.

[81] G. S. Tuncay, S. Demetriou, K. Ganju, and C. Gunter, "Resolving the predicament of android custom permissions," 2018.

[82] J. Valente and A. A. Cardenas, "Security & privacy in smart toys," in *IoTS&P '17*. ACM, 2017.

[83] R. Vallée-Rai, P. Co, E. Gagnon, L. Hendren, P. Lam, and V. Sundaresan, "Soot – a Java bytecode optimization framework," in *CASCON*. IBM Press, 1999.

[84] H. Wang, Z. Liu, J. Liang, N. Vallina-Rodriguez, Y. Guo, L. Li, J. Tapiador, J. Cao, and G. Xu, "Beyond google play: A large-scale comparative study of chinese android app markets," in *IMC '18*. ACM, 2018.

[85] X. Wei, L. Gomez, I. Neamtiu, and M. Faloutsos, "Permission evolution in the android ecosystem," in *ACSAC '12*. ACM, 2012.

[86] S. Wilson, F. Schaub, A. A. Dara, F. Liu, S. Cherivirala, P. G. Leon, M. S. Andersen, S. Zimmeck, K. M. Sathyendra, N. C. Russell *et al.*, "The creation and analysis of a website privacy policy corpus," in *Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, 2016.

[87] P. Wisniewski, A. K. Ghosh, H. Xu, M. B. Rosson, and J. M. Carroll, "Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety?" in *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. ACM, 2017, pp. 51–69.

[88] B. Yankson, F. Iqbal, and P. C. K. Hung, *Privacy Preservation Framework for Smart Connected Toys*. Springer International Publishing, 2017.

[89] M. L. Ybarra, K. J. Mitchell, and J. D. Korchmaros, "National trends in exposure to and experiences of violence on the internet among children," *Pediatrics*, 2011.

[90] N. Zhong and F. Michahelles, "Google play is not a long tail market: An empirical analysis of app adoption on the google play app market," in *SAC*. ACM, 2013.

## Acknowledgment

Los autores desean agradecer a nuestros revisores anónimos y a nuestro guía, el profesor Micah Sherr (Universidad de Georgetown) por sus valiosos comentarios y su ayuda para preparar la versión final de este documento. Los autores también agradecen a Julien Gamba por su ayuda en la inspección manual de las políticas de privacidad y Juan Caballero por su contribución a la versión inicial de este trabajo. Este proyecto está parcialmente financiado por la Fundación Nacional de Ciencias de EE. UU. (Subvención CNS-1564329), Horizonte 2020 de la Unión Europea Programa de acción de innovación (Acuerdo de subvención No. 786741, SMOOTH Project), los proyectos nacionales españoles DEDETIS (TIN2015-70713-R) y SCUM (RTI2018-102043-B-I00), la subvención española TIN2017-88749-R (DiscoEdge) y la Proyecto de la Comunidad de Madrid BLOQUES (S2018 / TCS-4339).

## 3rd-party Library ToS

A continuación, enumeramos los Términos de servicio de las librerías de terceros que prohiben su uso en software para niños:

**Branch.io [23]:**

*You will not use our Services to: {...} (ix) create lists or segments of children under the age of 13 (and in certain jurisdictions under the age of 16), advertise mobile Apps that are directed to children under 13 (and in certain jurisdictions under 16), and/or knowingly market products or services to children under 13 (and in certain jurisdictions under the age of 16), without employing appropriate settings within the Branch SDKs to limit data collection for children under 13 (and in certain jurisdictions under 16), in order to comply with any applicable laws protecting children (including, but not limited to, GDPR and the U.S. Children's Online Privacy Protection Act ("COPPA");*

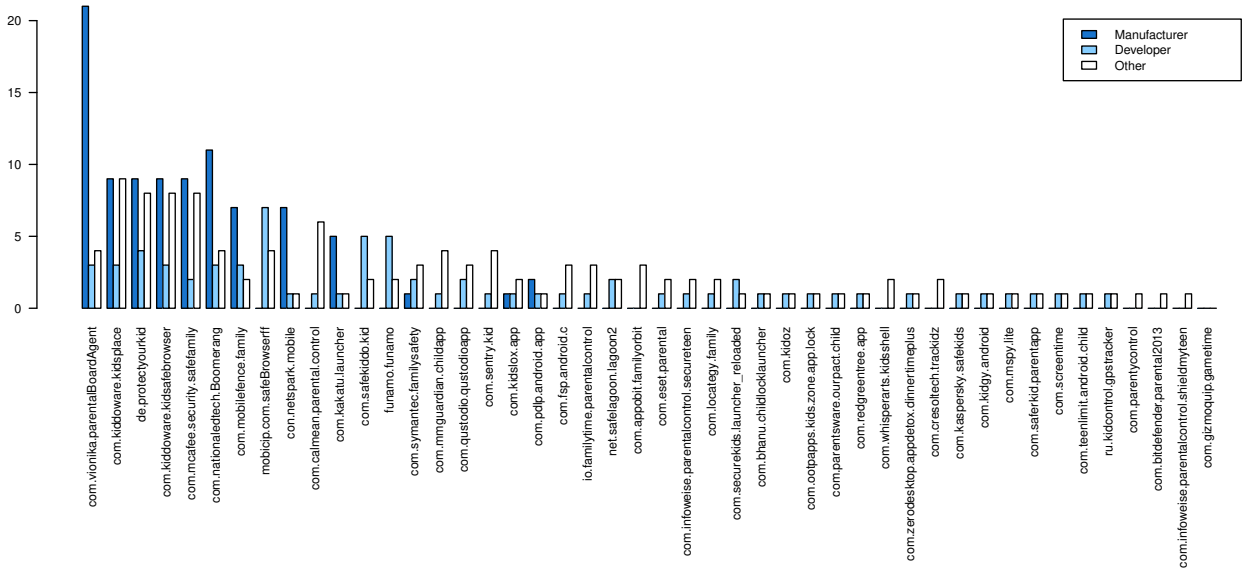


**Fig. 5.** Número y tipo de permisos personalizados encontrados en las aplicaciones en nuestro conjunto de datos

**Appboy [24]: (now branded as *Braze*)**
*Our Services are not directed to individuals under the age of 13. We do not knowingly collect personal information from such individuals without parental consent and require our Customers to fully comply with applicable law in the data collected from children under the age of 13.*

## Custom Permissions

Figure 5 dives deeper on the number and type of custom permissions for every app in our dataset.

## Permission Heatmap

La figura 6 muestra una versión apaisada de la Figura 2 que mejora la visibilidad.

## List of Analyzed Apps

La Table 8 proporciona una clasificación de cada aplicación atendiendo a si es una aplicación de supervisión o restricción, si está disponible actualmente en Google Play y si se compara con las alternativas SIP e IS4K.

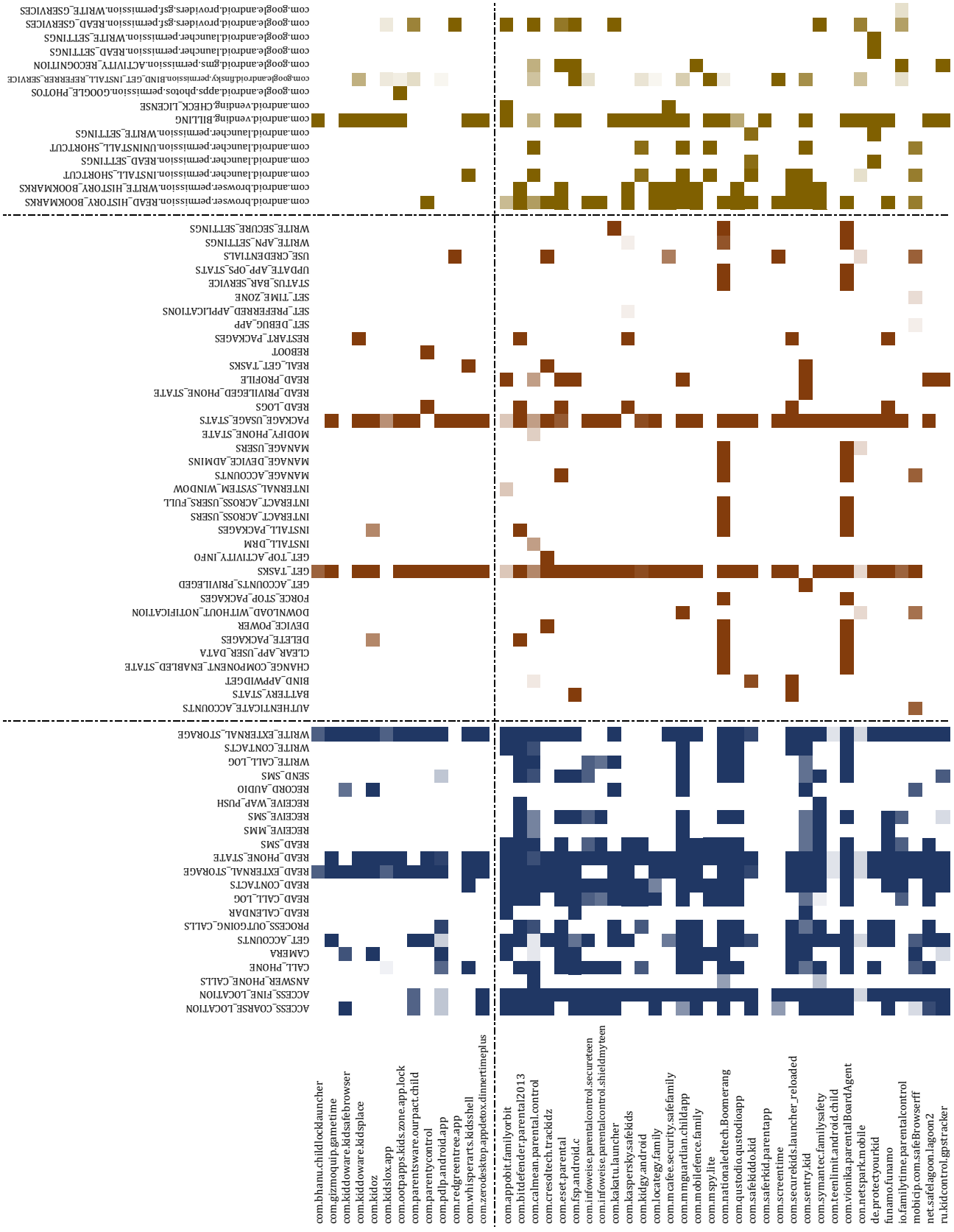


**Fig. 6.** Versión apasiada de la Figura 2

**Table 8.** Summary of our corpus of apps attending to different features. The column "benchmarked" indicates whether the app has been analyzed by [1, 33]. The values "M" and "R" stand for Monitoring and Restriction, respectively

| Name | Type | Currently listed (2019/05) | Benchmarked |
|---|---|---|---|
| com.mmguardian.childapp | M | ✓ | |
| com.infoweise.parentalcontrol.secureteen.child | M | ✓ | |
| com.qustodio.qustodioapp | M | ✓ | ✓ |
| com.kaspersky.safekids | M | ✓ | |
| com.kiddoware.kidsafebrowser | R | ✓ | |
| com.securekids.launcher_reloaded | M | ✓ | ✓ |
| com.eset.parental | M | ✓ | ✓ |
| com.symantec.familysafety | M | ✓ | |
| con.netspark.mobile | M | ✓ | |
| com.nationaledtech.Boomerang | M | ✓ | |
| com.mobilefence.family | M | ✓ | |
| com.infoweise.parentalcontrol.shieldmyteen | M | | |
| com.teenlimit.android.child | M | ✓ | |
| com.bhanu.childlocklauncher | R | ✓ | |
| com.safekiddo.kid | M | ✓ | |
| com.kidoz | R | ✓ | |
| com.cresoltech.trackidz | M | | |
| net.safelagoon.lagoon2 | M | ✓ | |
| com.screentime | M | ✓ | ✓ |
| com.kiddoware.kidsplace | R | ✓ | |
| com.mcafee.security.safefamily | M | ✓ | |
| io.familytime.parentalcontrol | M | ✓ | ✓ |
| com.vionika.parentalBoardAgent | M | | |
| de.protectyourkid | M | ✓ | |
| com.parentsware.ourpact.child | R | ✓ | |
| ru.kidcontrol.gpstracker | M | ✓ | |
| com.kidslox.app | R | ✓ | |
| com.zerodesktop.appdetox.dinnertimeplus | R | ✓ | |
| com.pdlp.android.app | R | ✓ | ✓ |
| com.redgreentree.app | R | | |
| com.sentry.kid | M | ✓ | |
| com.whisperarts.kidsshell | R | ✓ | |
| funamo.funamo | M | ✓ | |
| com.bitdefender.parental2013 | M | | |
| com.gizmoquip.gametime | R | | |
| com.kakatu.launcher | M | | |
| com.calmean.parental.control | M | ✓ | |
| mobicip.com.safeBrowserff | M | ✓ | ✓ |
| com.saferkid.parentapp | M | ✓ | |
| com.fsp.android.c | M | ✓ | |
| com.locategy.family | M | ✓ | |
| com.parentycontrol | R | | |
| com.leapteen.parent | M | | |
| com.kidgy.android | M | | |
| com.mspy.lite | M | ✓ | |
| com.appobit.familyorbit | M | | |