Apps that help parents protect kids from cybercrime may be unsafe too

Children, like adults, are spending more time online. At home and school pre-schoolers now use an array of apps and platforms to learn, play and be entertained. While there are reported benefits, including learning through exploration, many parents are still concerned about screen time, cybersafety and internet addiction. An increasingly popular technical solution is parental control apps. These enable parents to monitor, filter and restrict children's online interactions and experiences. In this blog, Luci Pangrazio discusses why parent control apps might be unsafe for children and the importance of helping children self-regulate and reflect on their online behaviour.

Parental control apps that work by blocking dangerous or explicit content can be marketed as "taking the battle out of screen time" and giving parents "peace of mind". But such a quick fix is inadequate when addressing the complicated reasons behind screen time. Much worse though, the apps expose users to privacy and other safety issues most people aren't aware of.

What apps do parents use?

Research by Australia's eSafety Commission shows 4% of preschoolers' parents use parental control apps. This increases to 7% of parents with older children and 8% of parents with teenagers. Global trends suggest these figures are bound to rise.

Parents download parental control apps onto a child's mobile phone, laptop or tablet. Most parental control apps enable parents to monitor or restrict inappropriate online content from wherever they are. They provide parents with insights into which sites their child has visited and for how long, as well as who they have interacted with. Qustudio, for example, claims to keep children "safer from cyber threats" by filtering inappropriate content, setting time limits on use and even monitoring text messages. Boomerang, another popular parental control app, enables parents to set time limits per day, per app.

Why they may not be safe

Parental control apps need many permissions to access particular systems and functions on devices. 80% of parental control apps request access to location, contacts and storage. While these permissions help the apps carry out detailed monitoring, some of them may not be necessary for the app to function as described. For instance, several apps designed to monitor children's online activity ask for permissions such as "read calendar", "read contacts" and "record audio" — none of which are justified in the app description or the privacy policy.

Many are considered "dangerous permissions", which means they are used to access information that could affect the user's privacy and make their device more vulnerable to attack. For example, Boomerang requests more than 91 permissions, 16 of which are considered "dangerous". The permission "access fine location" for instance, allows the app to access the precise geographic location of the user. The "read phone state" allows the app to know your phone number, network information and status of outgoing calls.

It's not just the apps that get that information. Many of these apps embed data-hungry third-party software development kits (SDKs). SDKs are a set of software tools and programs used by developers to save them from tedious coding. However, some SDKs can make the app developers money from collecting personally identifiable information, such as name, location and contacts from children and parents. Because third-party SDKs are developed by a company separate from the original app, they have different protocols around data sharing and privacy. Yet any permissions sought by the host app are also inherited by third-party SDKs.

Date originally posted: 2021-05-12

Permalink: https://blogs.lse.ac.uk/parenting4digitalfuture/2021/05/12/parent-control-apps/

Blog homepage: https://blogs.lse.ac.uk/parenting4digitalfuture/

The Google Play Store, which is used for Android phones, does not force developers to explain to users whether it has embedded third-party SDKs, so users cannot make an informed decision when they consent to the terms and conditions. Apple's App Store is more transparent. Developers must state if their apps use third-party code and whether the information collected is used to track them or is linked to their identity or device. Apple has removed a number of parental control apps from the App Store due to their invasive features. Many popular parental control apps in the Google Play Store have extensive security and privacy vulnerabilities due to SDKs. For example, SDKs for Google Ads, Google Firebase and Google Analytics are present in over 50% of parental control apps in the Google Play Store, while the Facebook SDK is present in 43%.

A US study focusing on whether parental control apps complied with laws to protect the personal data of children under 13 found roughly 57% of these apps were in violation of the law. Not all parental control apps request dangerous permissions. The Safer Kid app, for example, does not request any dangerous permissions but costs US$200 per year.

Why should I worry?

Personal data has become a valuable commodity in the digital economy. Huge volumes of data are generated from our digital engagements and traded by data brokers (who collect information about users to sell to other companies and/or individuals) and tech companies. The value is not in a singular data point, but the creation of huge datasets that can be processed to make predictions about individual behaviours.

While this is a problem for all users, it is particularly problematic for children. Children are thought to be more vulnerable to online threats and persuasion than adults due to more limited digital skills and less awareness of online risks. Data-driven advertising establishes habits and taste preferences in young children, positioning them as consumers by exploiting insecurities and using peer influence. Parental control apps have also been targeted by attackers due to their insecurities, exposing children's personal information.

There are better ways to reduce screen time

It is also questionable whether parental control apps are worthwhile. Research suggests issues of screen time and cybercrime are best managed through helping children self-regulate and reflect on their online behaviour. Rather than policing time limits for screen use, parents could focus on the content, context and connections their child is making. Parents could encourage their children to talk to them about what happens online, to help make them more aware of risk and what to do about it.

Restrictive approaches also reduce opportunities for kids' growth and beneficial online activity. Unsurprisingly, children report parental control apps are overly invasive, negatively impacting their relationships with parents. Instead of a technical "quick-fix," we need an educational response that is ethical, sustainable and builds young people's digital agency. Children will not be under their parents' surveillance forever, so we need to help them prepare for online challenges and risks.

Notes

This text was originally published by The Conversation and has been re-posted with permission and small edits.

This post gives the views of the authors and does not represent the position of the LSE Parenting for a Digital Future blog, nor of the London School of Economics and Political Science.

Featured image: photo by Karolina Grabowska on Pexels

Date originally posted: 2021-05-12

Permalink: https://blogs.lse.ac.uk/parenting4digitalfuture/2021/05/12/parent-control-apps/

Blog homepage: https://blogs.lse.ac.uk/parenting4digitalfuture/