Agency for Digital Government

Educational apps: What are you paying with?

Data collection from educational apps for children

Disclaimer: This translation is provided for information purposes only. The Agency for Digital Government do not guarantee the accuracy of the translated text. In case of doubt, the Danish version prevails.

January, 2025

Table of content

1. Executive Summary

This report is based on an analysis of 40 popular educational apps that you pay for. Twenty apps were selected and tested in their iOS and Android versions. The primary target group for these apps is children of 0-14 years of age. The 40 apps were analysed to assess the extent of data collection by third-party services from apps after they have been paid for. Two types of apps with different payment methods were included in the analysis: 1) Apps that require payment before download. 2) Apps offering full access after download, either through a one-time payment or through a subscription.

Additionally, information was gathered on the use of consent forms in the analysed apps to understand how user consent for data collection is obtained across these educational apps.

The report at hand serves as a continuation of a previous publication, *What Does a Free Mobile Game Cost*? released by the Danish Agency for Digital Government in March 2024. This report analysed data collection by third-party services from 24 free mobile games. The current report incorporates a comparative analysis, juxtaposing individual findings from the current analysis with those from the earlier publication.

The key insights from the report are organized under the following headings:

Big difference in data collection from the two types of paid-for apps

The analysis reveals a notable disparity between the two types of payment methods in the amount and purpose of data collection from the apps. Third parties collect significantly less data from the apps that require payment before download, compared to those where full access is purchased post-download. This means users may effectively "pay" for their apps with both money and personal data in cases where they initially download a free version and later purchase full access or additional features.

Lack of consent forms, even when required

According to the Danish Cookie Order, explicit consent must be obtained from users if data is collected by third-party services that use the data for marketing and/or statistical purposes. None of the apps analysed have an explicit consent form, such as a cookie banner, and thus the user does not have the option to reject data collection by third-party services. It is worth noting, that the lack of a consent form is not necessarily problematic. From 52.5% of the analysed apps, third parties do not collect any data, or only collect data for purposes that are technically necessary.
In these cases, law does not require a consent form. However, from 47.5% of the apps, third parties collected data for either marketing and/or statistics – purposes that, per the law, require the app providers to collect valid consent from the users.

Significantly less data collection than from free mobile games

In total, third-party services collect data from 27 of the 40 apps analysed, corresponding to 67.5%.

In 19 of these 27 apps (47.5%), third-party services collect data for statistical and/or marketing purposes. This means that from more than half of the analysed apps (52.5%), either no data is collected or the data collection is limited to purposes that are technically necessary.
In comparison, of the 24 free mobile games analysed in the previous report, third parties who collected data for marketing purposes were present on 100% of the apps.

A particularly vulnerable group

All the analysed apps are primarily aimed at children aged 0-14, meaning they are subject to specific GDPR rules on obtaining consent from users under 15. Service providers must ensure that consent is obtained from a child's legal guardian and take reasonable precautions to verify this.

Given children's particular vulnerability to digital services—in terms of both retention mechanisms designed to keep them engaged and their ability to understand consent processes—it is crucial that developers take special care in securing valid consent from an adult.

Beyond legal compliance, figures from Statistics Denmark suggest that greater transparency in data collection can significantly enhance customer trust, making it both a regulatory and ethical priority for service providers.[1].

Recommendations

Navigating the complexities of data collection and sharing in digital services can be challenging for users. This challenge is further amplified by a lack of transparency, since most of the data collection happens behind the scenes and may not even be fully understood by the service providers themselves. Despite this, there are steps that can be taken to reduce third-party data collection.

The recommendations are divided into two categories: the first three are aimed at parents and app users, while the last two are directed at service providers. The recommendations are elaborated later in the report.

- Consider the benefits of using the app versus the consequences of data collection
- Paying for your apps can help protect your and your children’s data
- Read the privacy section in the app store before downloading an app
- Be aware that the same rules apply to apps as they do to websites
- Consider how to collect consent, if your app primarily caters to children and young adults

[1] IT-anvendelse i befolkningen 2024, Danmarks Statistik

2. Introduction

Screens have become an integral part of most people's everyday lives, influencing virtually every aspect of our routines. Particularly for children, the reliance on digital devices has sparked a growing debate on how to balance screen time, both in private settings and public institutions.

The role of digital tools to support learning frequently emerges as a topic of public discussion. The influence of technology on children's education and learning is evident both at school and at home, prompting questions about its proper extent and application. Children, especially in digital contexts, represent a particularly vulnerable group. Many parents and educators strive to make children's screen time both productive and meaningful. Schools often recommend educational apps to reinforce learning outside the classroom, leading parents to explore apps designed for educational purposes. However, this raises concerns about potential pitfalls when children engage with these tools, such as apps designed to teach the alphabet, arithmetic, or other skills.

In recent years, there has been heightened attention on protecting children's privacy as they navigate the digital world. The phrase, *If a digital service is free, you are the product*, has long underscored concerns about online privacy. Free services, including games, often generate revenue by collecting user information and sharing it with third-party services.

In March 2024, the Danish Agency for Digital Government published the report *What Does a Free Mobile Game Cost*? This report detailed how free gaming apps aimed at children had third parties extensively collecting data, raising critical concerns about these practices.

Data collection from third-party services plays a significant role in the current data economy and is used for purposes such as cross-platform targeted marketing, where advertisements can be presented at specific times when the user is more receptive to marketing.

It is important to emphasize that third-party services are not inherently problematic. They can optimize the digital user experience in many ways. However, it is also important that the rules for data collection from third parties be observed. This includes ensuring that users actively consent to data collection and sharing when it is not technically necessary.

We have grown accustomed to not paying money for the digital services we use daily. However, the study IT Usage in the Population 2024 shows that 33% of Danes are willing to pay (more) for digital services if it means that less information is collected about them[2].

This report examines whether paid educational apps for children collect less third-party data. It does this through an analysis of 40 popular educational apps.

There are numerous actors who uniquely interact with and are affected by apps and digital services from which third parties collect data. Based on the analysis, several recommendations are provided. These recommendations target parents and digital service users seeking to minimize data collection, as well as developers and service providers needing clarity on data regulations.

[2] IT-anvendelse i befolkningen 2024, Danmarks Statistik

3. Method

3.1 Data and approach

In addition to investigating the collection of data from educational apps by third parties, the purpose of this report is to investigate whether a business model based on monetary payment is more protective of user data and privacy. Thus, all apps analysed are paid apps, even in cases where a free version of the app exists. Paid apps are defined as apps that are purchased directly from an app store or for which full access is purchased after download, either as a one-time payment or as a subscription. The business models for the apps analysed are thus either subscription-based, freemium or one-time payment.

The results presented in the report are based on an analysis of 20 popular apps with educational purposes. Each app was tested in both iOS and Android versions, resulting in a total of 40 apps analysed.

Although the iOS and Android versions of each app essentially are “the same" app, we treat them as separate, individual apps. This approach is taken because differences in the development of an app for each operating system can result in variations in the amount and type of data an app shares.

iOS and Android are the two most widely used operating systems in Denmark, with iOS holding approximately 61% of the market share and Android around 38%[3]. Given this distribution, it is relevant to analyse apps developed for both platforms.

Business models behind apps include Microtransactions, data collection and advertising, subscriptions and one-off payments.

Microtransactions allow players to purchase virtual goods with real money.

Ads can appear as banners, videos or pop-ups and developers earn money when players interact with them. In this context, *data collection* can enable, for example, targeted advertisement.

Subscriptions often give players access to exclusive or extended content for a fixed fee, often removing ads or in-game restrictions.

In digital services that use *one-time payment*, the user pays once for full access with no time limit.

The primary target audience for the analysed apps is children aged 0–14. This assessment is based on the content of the app, the categorization in the app stores, and annotations in the Apple App Store, where developers can specify the intended age group for their app.

Each app was tested for 15 minutes, during which as many core features as possible were explored. Apps where a subscription or full access was purchased post-download were tested after the purchase.

[3] https://gs.statcounter.com/os-market-share/mobile/denmark/#monthly-202409-202409-bar – per 07.10.2024

3.2 Collection and data processing

Data from iOS was collected through the App Privacy Report, a built-in feature in iOS that has been available on iPhones since iOS 15.2. App Privacy Report records network activity from the device. In addition, it also records which permissions, such as microphone access or location, have been used.

Data from Android was obtained through TrackerControl. TrackerControl is an open-source tool used to detect which trackers are embedded in the source code of an app and which third-party domains are contacted when the app is in use.

The two tools differ from each other in terms of their approach to data collection and how the collected data is structured. Whereas the App Privacy Report records all network activity from the device during the time the feature is turned on, TrackerControl records activity from the individual app. To work around this difference, all other apps and programs used on the iPhone were closed before enabling the feature. During the 15-minute test, only the app being analysed was open on the iPhone to avoid capturing network activity from other programs on the device. Individual calls from system apps detected during testing were filtered out during the data cleaning process.

As mentioned, both the App Anonymity Report and TrackerControl record the domains contacted by the device or app being tested. To ensure consistency, the analysis focuses exclusively on these domain calls. Consequently, some data from TrackerControl is excluded from the study where no equivalent exists in the App Anonymity Report, and vice versa.

The tools used do not provide insight into the contents of the data being collected or shared. Every domain that was contacted has been analysed to identify whether the call was made to a third-party service, determine the company that owns the domain, and assess the possible purpose of the service.

Additionally, data was gathered to assess whether each app obtains user consent for data collection and to examine how this consent is designed across the analysed apps.

4. Results

4.1 General results

Cookies and similar tracking technologies fulfil many different purposes (Table 1). This means that the purpose of third parties collecting data can vary. The purposes can be technically necessary, statistical, personalization, and marketing. Whether to inform the user and obtain consent if data is collected depends on the purpose of the collection.

Know your purposes

When service providers use tracking technologies like cookies on their platforms, these must be categorized by purpose. This allows users to provide a more detailed consent based on the purposes for which they wish to allow their data to be used.

Does not require consent

Technically necessary purposes

- Tracking technologies for technically necessary purposes are used to ensure that the service functions correctly. For example, they may keep users logged in during their visit.

Requires consent

Statistical purposes

- Tracking technologies for statistical purposes are used to collect data on how users interact with services. For instance, they measure the number of visitors, visit duration, and navigation patterns on the website.
- Their primary aim is to improve services by providing insights into user behavior and preferences

Personalization purposes

- Tracking technologies for personalized purposes are used to customize the user experience based on individual preferences, such as language settings or products a user has shown interest in.
- Their primary aim is to create a more tailored and relevant experience for each user.

Marketing purposes

- Tracking technologies for marketing purposes are used to target ads and campaigns based on the user's online behavior. They may also track users across different websites to optimize marketing efforts.
- Their primary aim is to enhance the effectiveness of marketing by delivering more targeted and personalized advertisements.

Table 1. Purposes of tracking technologies

The report *What does a free mobile game cost?*, published by the Agency for Digital Government in March 2024, showed that third-party marketing services collected data from 100% of the free mobile games that was analysed. Compared to these results, there is a noticeable difference from the apps analysed in this report.

Out of the 40 apps analysed, third-party services collect data from 27 of these (67.5%). Of these 27, 19 (47.5%) are collecting for marketing or statistical purposes. This means that more than half (52.5%) of the apps tested do not share data with third parties or only share data for technically necessary purposes.

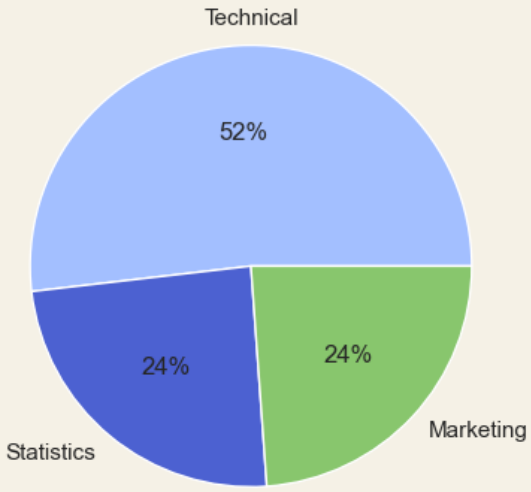

Figure 1. Overall distribution of purposes for data collection in percentage.

There is also a noticeable difference in the amount of domain calls from the two types of apps. A domain call is the request a client (for example, an app) sends to a server to request content, images or other data.

The 27 apps from which third parties collected data only made a total of 217 domain calls during the time they were tested. Of those 217 calls, 104 are for marketing or statistical purposes. This is relatively few calls considering that all apps were tested for 15 minutes each, i.e. 217 calls across 10 hours of testing time. This equates to an average of only 1 call every 3 minutes or so. In comparison, the mobile games from the previous report made more than 1600 domain calls from 24 apps.

The difference in the number of domain calls is most likely related to the two different business models used by the mobile games and the educational apps. The free mobile games rely on earnings through advertisement and therefore make far more domain calls to third parties (e.g. to download advertising material).

Across the 27 apps making domain calls to third-party services, there is also a large difference in the number of calls made by each app. The number of calls ranges from a single call by the app with the fewest interactions with third-party services to 28 calls by the app with the most, as shown in Figure 2.

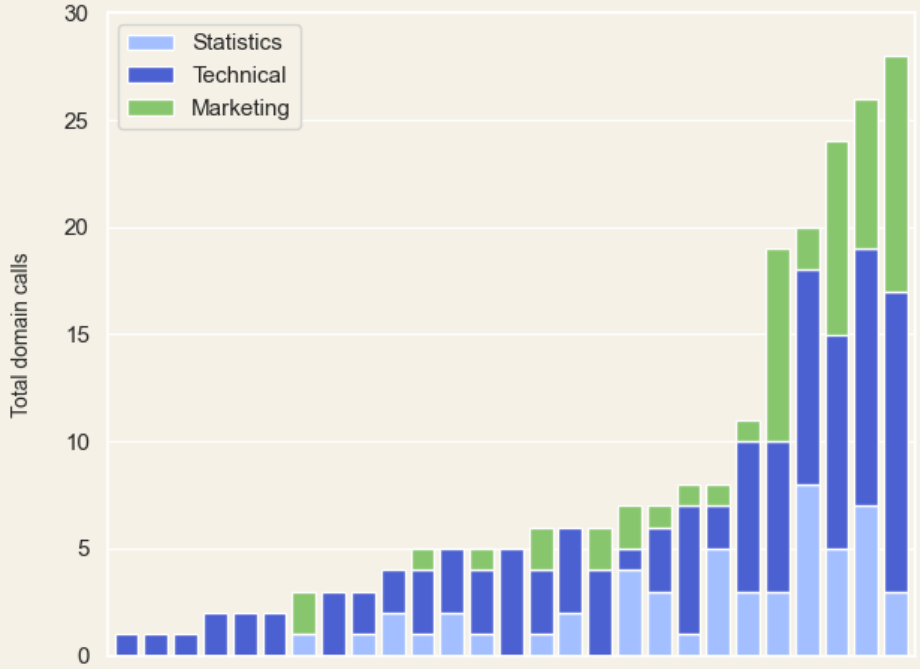

Figure 2. Domain calls per app differentiated by purpose. Each bar represents one app.

The same is true for the 19 apps that collect data from third-party services for marketing or statistical purposes. Here, the 5 apps that collect the most data from third parties account for approximately 62% of the total data collection.

Overall, the extent of data collection for third-party services in the analysed apps is significantly lower compared to the free gaming apps examined in the previous analysis.

4.2 Apps purchased before and after download

The apps analyzed in this report fall into two payment categories: those purchased before download and those requiring a one-time payment or subscription for full access after download.

When comparing the two types of paid apps, there is a significant difference in the amount of data collected by third-party services. As Figure 3 shows, apps with payment post-download account for the majority of domain calls to third-party services. This suggests that more data is likely collected for third-party services from these apps compared to apps purchased directly in the app store.

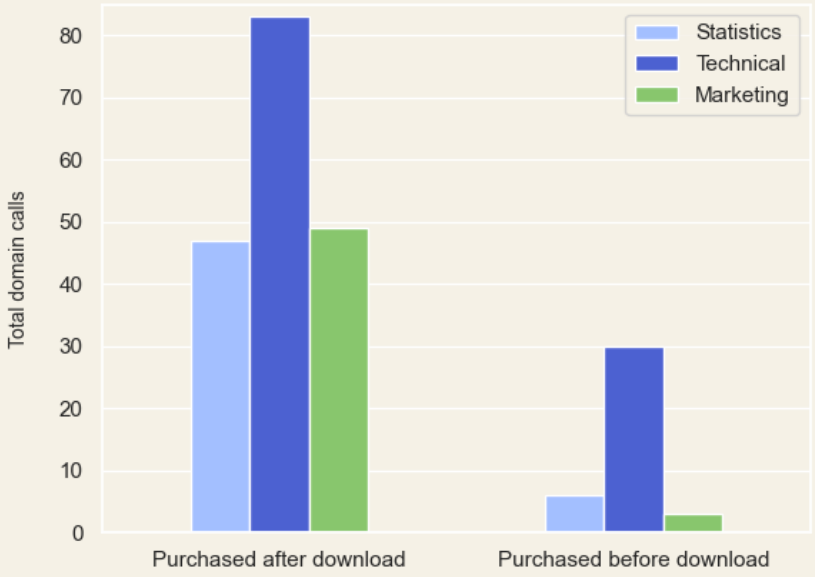

Figure 3. Total domain calls from apps purchased respectively before and after download

A significant difference also exists between the two types of paid apps regarding the purposes for which third-party services collect data. Apps with payment post-download account for 94% of the data collected for marketing purposes and 89% of the data shared for statistics and analysis (Figure 4).

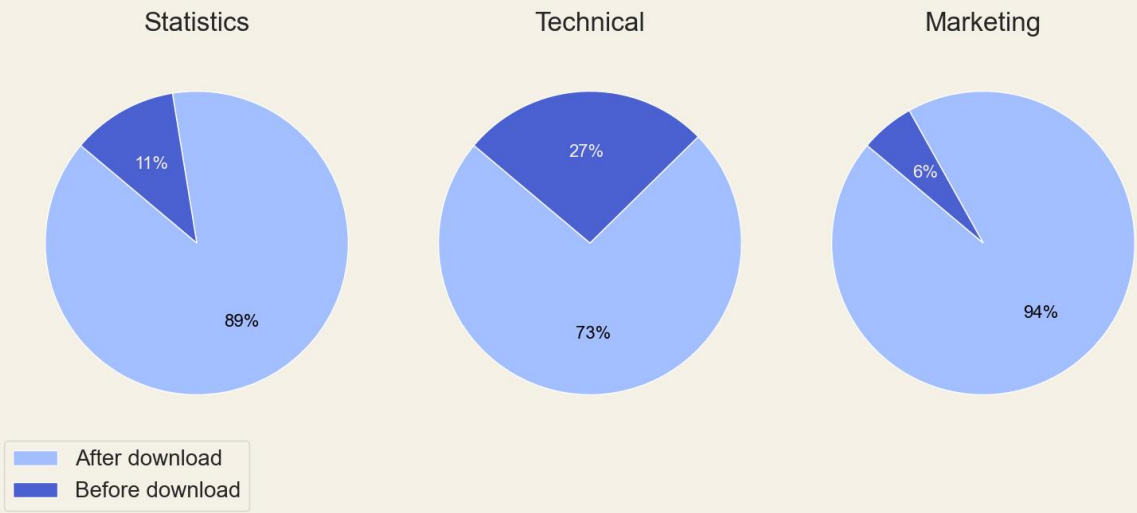

Figure 4. Distribution of purposes for data collection in percentage for apps purchased before and after download.

The difference between the two types of apps is not entirely surprising. Purchasing access to an app after it has already been downloaded essentially means paying for access to "the same app", i.e. a

new app is not downloaded that has been developed or built differently. Consequently, it is assumed that the app operates the same way as it would without payment.

In the report *What Does a Free Mobile Game Cost?* it was explained how apps adopt different business models to generate revenue. While free apps often rely on users "paying" with their data, paid business models typically eliminate advertising content and, by extension, data sharing with third-party services for marketing purposes.

The analysis in this report supports the notion that this is true in most cases. However, it also reveals that apps using a subscription-based model collect data for third-party services to a significantly greater degree than apps paid for before download. This is particularly evident in data collected by third-party services for marketing or statistical purposes. As a result, users may find themselves in a situation where they pay for an app with both money and data, potentially without providing explicit consent for their data to be used for marketing and/or statistical purposes.

4.3 Consent forms

When an app retrieves or stores data on a user's device for purposes that are not technically necessary, the app owner is responsible to obtain the user's consent per the ePrivacy Directive.

In the analysis, 47.5% of the apps had at least one third party collecting data which, based on domain analysis, was determined to primarily serve marketing or statistical purposes. Since these purposes are not considered technically necessary, these apps are not exempt from the requirement to obtain user consent.

However, none of the analysed apps included a cookie banner or similar mechanism for obtaining consent. This indicates that nearly half of the apps fail to comply with relevant regulations.

A general pattern was observed in apps where payment is made after downloading: privacy policies are typically included alongside other business terms, often presented as a link that leads to an external website. By embedding the privacy policy in this way, users cannot avoid accepting it if they want to purchase full access or a subscription. This approach leaves users without the option to opt out of specific aspects of data collection that they may not agree with.

More often than not, apps purchased directly from the app store have their privacy policies located within the menu of the app. As a result, users are neither directly presented with the privacy policies of these apps nor offered an option to decline non-technically necessary tracking.

4.3.1 Collection of consent

There are requirements for how consent must be obtained and what information the user must be presented with (see Table 2). The Danish concept of consent in the Cookie Order originates from the ePrivacy Directive that adheres to the definition of consent outlined in the GDPR. In Denmark, the Danish Data Protection Agency enforces and provides guidance on the GDPR, while the Danish Agency for Digital Government is responsible for the ePrivacy Directive, implemented in Denmark through the Danish Cookie Law.

What do the rules say?

If you as a service provider use tracking technologies for purposes other than technical necessary ones, users must consent to this. Below are the requirements on how to obtain this consent from users:

- **Obtain valid consent**
  When a user visits a service, they must be clearly and fully informed about any tracking technologies, such as cookies, used on the service, what purposes they serve, and whether any data collected through these technologies will be shared with third parties.

- **Elaborate on the tracking technologies**
  The service owner must provide clear information about the tracking technologies used on the service, including purpose, provider and duration.

- **Provide denial and revocation options**
  Users should have the option to refuse or change their consent and it should be as easy to withdraw it, as it was to give it. It should not be easier for users to give consent than to refuse.

- **Customized consent**
  Consent must be obtained for each specific purpose, such as functional, statistical, or marketing purposes, and not as a single, combined consent. The checkboxes must not be pre-selected, the user must actively make a choice.

- **Update information**
  If new tracking technologies are introduced, they must be categorized by purpose and the information must be updated. Users must be informed and new consent must be obtained.

Please note that the rules for tracking technologies only cover the collection and storage of information on the user's terminal equipment, not subsequent processing. If the data collected is personal data, the processing must be assessed under the GDPR. This may require separate consent for processing.

Table 2. Rules for the valid collection of consent

Consent is often obtained via a so-called 'cookie banner'. To comply with the provisions of the ePrivacy Directive, this now familiar pop-up must offer information about the purposes for which data is collected and give the user the option to reject or allow all or part of this collection.

The design of a cookie banner should also have a neutral messaging effect so that it does not make it easier for the user to give consent than to refuse it. Cookie banners have become a familiar part of our experience on websites. However, it is important to note that mobile apps are subject to cookie regulations on equal terms with websites.

4.3.2 Consent from children and young adults

For information society services aimed directly at children under the age of 15, specific rules govern how the service provider must obtain valid consent. An information society service refers to any commercially oriented service delivered online at the request of an individual user. This category

includes online games, e-commerce platforms, social media, and the paid educational apps analysed in this report.

If the service provider is established in Denmark and collects or stores information from users under the age of 15, the law requires that consent be obtained from the parent or legal guardian.

Given that the analysed apps target children aged 0–14, the primary users are assumed to be within this age group, i.e., under 15 years old. As a result, service providers must make reasonable efforts in accordance with the available technology to prohibit the child from giving consent. Instead, the service provider must verify and secure consent from a parent or guardian[4].

[4] Datatilsynet: Vejledning – Samtykke. https://www.datatilsynet.dk/Media/0/C/Samtykke%20(3).pdf

5. Young adults and children – a vulnerable audience

Many apps are developed with the help of third-party services, and there are several legitimate reasons for this. Using third-party services can make it easier to display content such as videos and images, collect data about app errors, send push notifications, or other useful features without the developer having to build the functionality from scratch.

Third-party data harvesting is an important component of the existing data economy, where it serves to create consumer profiles for marketing purposes. This makes it possible to follow the same user across different online platforms and services and optimize these to maximize retention time. In addition, this profiling can also be used to present advertisements at times when the user is deemed particularly receptive.

Children and young people using mobile apps are less aware of the extent to which content they encounter is marketing. In addition, they are particularly vulnerable to the retention mechanisms used in mobile apps.

Service providers must comply with cookie regulations by lawfully obtaining user consent, ensuring that users are informed about why and to what extent their data is being collected, including whether third-party data collection is involved. In addition, we are becoming increasingly critical of data collection as part of our digital lives. For example, 63% of Danes say they at some point opted out of services or websites because they were concerned about the company's use of their data[5].

The Danish Cookie Law does not place specific restrictions on the use of the data harvested, but it does emphasize the importance of allowing users to decide whether they want to consent to the collection or storage of data on an informed basis. However, in connection with subsequent processing, it is important to comply with the GDPR to the extent that personal data is involved. This is reflected in Danes' attitudes towards transparency about how their data is used: 79% partially or completely agree that it is important to them that companies clearly state whether they collect data about the user in order to profit from it[6]. Therefore, in relation to legislation and customer trust, there are several reasons for service providers to make parents aware of how data is used and for what purposes - especially when the target audience is children under the age of 15.

[5] IT-anvendelse i befolkningen 2024, Danmarks Statistik
[6] IT-anvendelse i befolkningen 2024, Danmarks Statistik

6. Recommendations

Apps, especially educational apps, can be valuable to children in many ways through play, learning, development and entertainment. They can help children improve their skills and provide access to content tailored to their learning needs. However, it is important to recognize, as previously highlighted, that apps can also collect data about children's behaviour and interactions to varying extents, enabling some level of profiling and targeted marketing. In addition, it can be confusing and opaque to navigate and understand the cookie policies of digital services and the extent to which they share data.

Here are five recommendations to consider if you or your children use apps, or if your company provides apps for children:

6.1 Parents and users of digital services

Consider the benefits of the app versus the consequences of data collection

When a parent has to decide in a specific situation whether they want to give consent to data collection on behalf of their child, they may be faced with questions like: What information is being collected? What is this information used for? Moreover, what could the consequences be? It is important to weigh the potential benefits of the app against the possible consequences of data collection. What value does the app bring to your child's learning and could this be achieved without having data collected for commercial purposes? Are there alternatives to the app in question that do not collect data for marketing?

It pays off to purchase apps if you want to protect your and your children's data

The analysis of the apps in this report indicates that paid apps generally share far less data with third-party services than free apps. If you want to avoid data harvesting and have the means to do so, paying for your apps is often worthwhile. In particular, the analysis shows that paying for the app directly in the store significantly reduces data sharing.

Read the privacy section in the app store before downloading

Both the App Store and Google Play Store provide a details section where developers specify the data collected and its usage. In the Google Play Store, the section is called 'Data safety' and in the App Store, it is called 'App Privacy'. These sections can be used for a relatively quick and easy orientation on the data collection and usage of the app. The sections provide insight into what data is collected, whether data is shared with third parties and whether it is used to track you. You can use this information to help you decide if you want to download the specific app, but are unsure about how the app addresses data collection by third parties. However, it should be noted that it is the developers themselves who provide this information.

6.2 Developers and service providers

Be aware that the same cookie rules apply to apps as they do to websites

If you are the owner of an app that collects or stores data on a device, you should be aware that the rules for the use of cookies and similar technologies also apply to apps. Please refer to the Danish Cookie Law or the Agency for Digital Government's cookie guidelines[7] if you are in doubt about which rules apply. As a service provider, it may be relevant to get an overview of the third-party services used, and have a dialog with your developers to avoid all unnecessary data collection and obtain consent when required.

Consider how to collect consent when your app has children and young adults as its audience

If your app falls under the definition of an information society service, as is the case with the educational apps analysed here, and your app directly targets children and young people under the age of 15, consent must instead be obtained from a parent or legal guardian before information can be collected or stored. Therefore, developers must make reasonable efforts to secure parental consent. This must take into account the potential intrusiveness of the data collection and the available technology. Currently, there is no perfect solution for verifying or estimating the age of a user, or ensuring that consent is obtained by a parent or guardian. However, this does not exempt service providers from their responsibilities. Examples of reasonable efforts could be self-declaration of the user's age or capacity testing by presenting the user with a problem of appropriate difficulty. What constitutes a reasonable effort depends on how potentially privacy-invasive the data being collected or stored is.

[7] https://digst.dk/sikkerhed/digitale-tilsyn/tilsyn-med-sporingsteknologiomraadet/cookievejledningen/

7. Appendix 1: Analysed apps

The following apps were selected on June 28th, 2024, and serve as the foundation for the analysis and report:

- Knæk Læsekoden
- King of Math: Hele spillet
- Lær ABC Alfons Åberg – Fulde
- Letrakid Pro Lær ABC Skolespil
- Babblarna
- Dr. Panda Handyman
- Arkæolog Istid Dinosaur
- Toca Boca Hair Salon 2
- Grow Garden: Børnespil
- Pettson's Inventions Deluxe
- Sjove Børnespil: spil for børn (BimiBoo)
- PAW Patrol Academy
- Thinkrolls 2
- Sjove læringsspil for børn (SKIDOS)
- Miniklub Lite
- DuoLingo
- Maneno
- Lingokids – Play and Learn
- LEGO DUPLO World
- Albert Junior: spil for børn

Agency for Digital Government