# MIND CONTROL

Privacy, Age-appropriateness, Deceptive Design Patterns and other Ethical issues in apps used by Adolescents

**August 2022**
**SUNDAR NARAYANAN**

# Table of contents

Copyright © 2022. All rights reserved

# I. Setting the Context

## Introduction

Smartphones have become a vital part of many children's lives due to increased access and the rise of digital learning methods such as COVID-19. Recent research shows that children spend 6-9 hours daily on smartphones [2]. The current expansion of mobile apps' use for games and online education for children requires that we examine the consequences of any ethical deviations. Children might not be as aware of the implications and risks associated with their actions when using smartphones or apps. This paper examines ethical issues, including deceptive design patterns in apps children use in adolescence (12-17 years).

## Adolescent age group

Adolescents were selected for this study. A 2019 Pew Research found that 54% of teens in the United States (US) spend too much valuable time on their cell phones [1]. In selecting adolescents for the study, three key reasons were considered: (1) Adolescents are still in their normative decision-making stages and may be susceptible to be influenced by nudges; (2) Adolescents don't have an appropriate app category. Apps on platforms are classified as "children's apps" for users aged less than 12. Some apps allow users to log into the app via their social media accounts. (3) Research shows that adolescents are more susceptible to anxiety, depression, and behaviour disorders.

## Regulatory gamut

Regulators across geographies have regulations laying out expectations regarding designing technology applications for children.

In the UK, GDPR has provisions to enhance the protection of children's data and demands that the privacy policy is laid out in plain and unambiguous language that a child can understand. It also places a requirement for transparency and accountability in dealing with the personal data of children [3].

Also, the Age-appropriate design code of the UK sets clear expectations around processing or dealing with the personal data of children. It establishes the requirement to (a) place children's best interest when processing personal data, (b) establish age-appropriate content, (c) prohibit detrimental use of data, (d) take effort towards data minimization, (e) ensure that default settings and location tracking are off, and (f) enable parental access and controls. Further, it highlights that use of the nudging technique to exploit a psychological bias of children as non-compliance to GDPR Child-specific considerations [4].

In the US, Federal Trade Commission (FTC) has provided guidelines for app developers to help them comply with Truth in advertising standards and privacy principles [5]

Advertisements shall have the truth, and demonstrable proofs shall support their objective claims. Further, FTC expects that the features and limitations of the product or service are explained clearly and conspicuously. While the law does not dictate the font or type size, FTC has clarified that they have acted against companies that buried important terms behind dense blocks of legal jargon or vague hyperlinks.

FTC insists app developers consider privacy by design, including limiting the extent of data collection, securely managing data held, allowing the user to set preferences regarding default settings, and being transparent about data processing and use practices. The app developers must make it easier for users to access the privacy features. [5].

In addition, FTC clarifies that the app developers shall ensure privacy settings and an opt-out mechanism to help users make their choice. In addition, FTC expects the app developers to comply with children’s online privacy protection rules (COPPA). COPPA, among others, requires parental consent before collecting any personal information.

Online Safety regulations emerging across geographies are also intended to protect children from harm caused by online services. These regulations ensure privacy and safety and protect the child’s best interest. Regulators are increasingly enforcing companies for violation of rules. For instance, Tiktok was penalized for violating the privacy of young children by the Dutch Data Protection Authority in 2021 [6].

### UNICEF guidance

UNICEF's Rights by Design Standard highlights five key issues. These are (1) Privacy violations, (2) Safety violations that may threaten children's morality and physical & mental integrity, (3) Economic exploitation using data-based marketing strategies, (4) Freedom violations caused by persuasive technologies, and (5) Unequal treat and discrimination. It is essential to recognize that children can be affected by data access and usage (sharing with third parties) for economic benefit. Inadequate safety design can also hurt children's well-being [7].

This white paper examines ethical issues in apps used by adolescents (12-17 years). This paper covers the methodology & critical ethical issues in Section 2, detailed outcomes in Section 3 to Section 6, way forward suggestions, and conclusion in Sections 7 & 8.

# II. Methodology

## Apps used by adolescents

The white paper examines the ethical issues in popular apps (Android and IOS) in categories including Education, Gaming, Communication, Social and Dating; used by adolescents. Apps were identified based on keyword searches on Google Play Store and Apple App Store (collectively called 'App marketplaces') and searched app marketplaces with the keywords "top apps" in each category along with the words "Children" in the app marketplaces. Thirty-nine apps were identified across five app categories, namely, education (5), communication (7), social media (8), games (10), and dating (9). These categories were identified based on the possible relevance of such apps to adolescents. Additional categories of apps, including Music & audio, entertainment, and movies & series, will be covered in subsequent parts of the study.

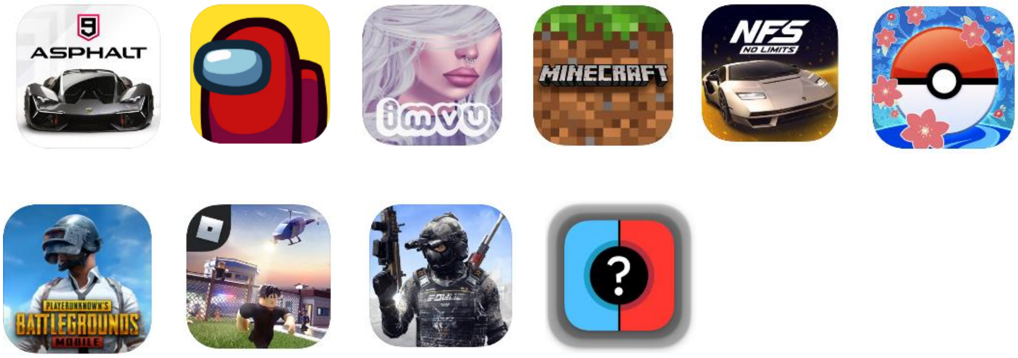
## Review of apps

Identified apps were installed on an Android device (Oneplus 7) and an IOS device (iPhone 11) for examination. Ethical issues were examined in such apps. For this research, a user id was created using an email id (ethics.test@aitechethics.com) in these apps (wherever user creation was mandatory), navigated through the user journey, and took screenshots of ethical issues in them for documenting the research.

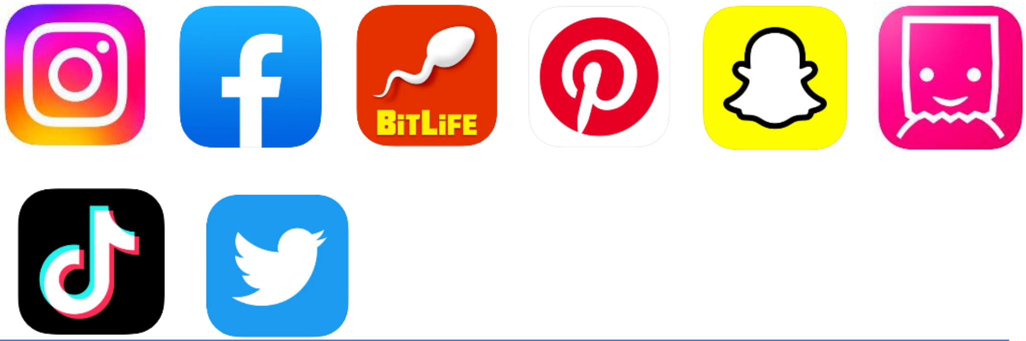
Emails received (on the email id) were also reviewed for any notifications, privacy policy changes, or other communications from the app developers. While many apps were freemium, allowing in-app purchases or subscriptions, the apps were examined on features available for free (without signing up for any subscription). Many apps were accessed using the Gmail account or Facebook account, while some required users to create an account itself. In most cases, for testing, age was declared to be 13 or 14 years and 18 in select cases (specifically in the case of dating apps) to subsequently validate if there was any age verification mechanism present in them.

## Apps used by adolescents

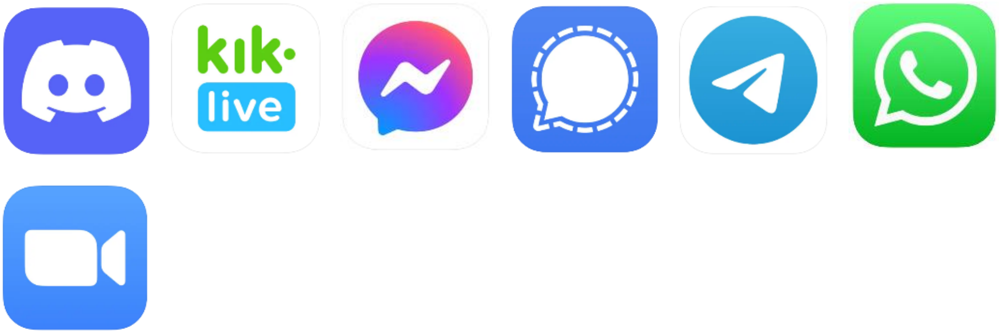
**Games**



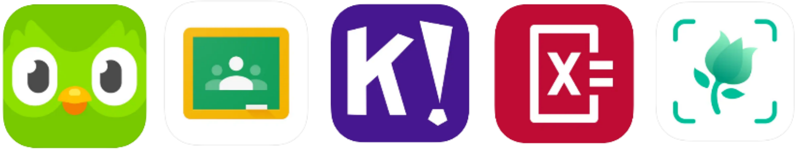
**Social Media**



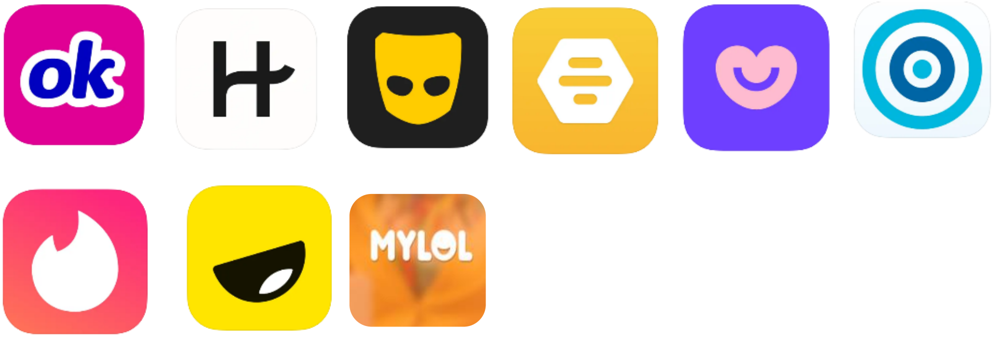
**Communication**



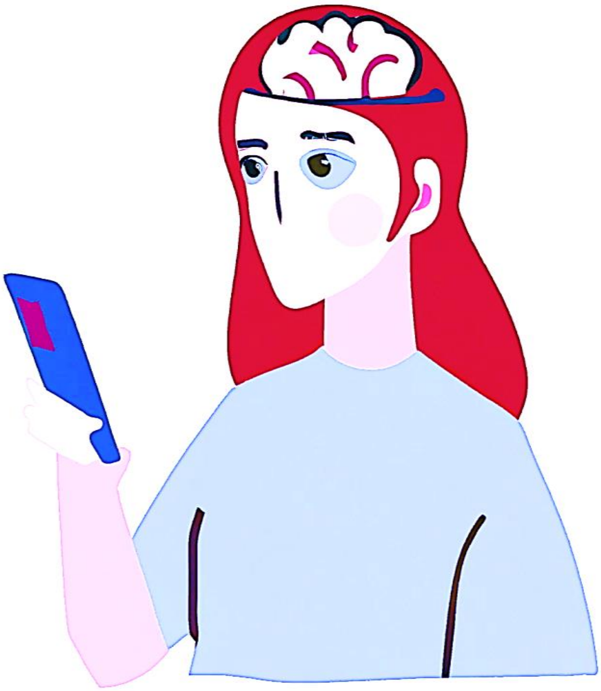
**Education**



**Dating**



In addition, secondary research was conducted by searching for (a) ethical issues regarding the apps on Twitter, Reddit, Quora, and Google and (b) instances of deceptive design patterns as published on www.deceptive.design, www.darkpattern.games and https://darkpatternstipline.org/



## Ethics in apps

Ethics of app design, development, deployment, and monitoring are essential to ensure the users' privacy, security, well-being, and fairness, in this case, adolescents.

The negative consequences of ethical deviations will impact people, society, and the environment. Ethical deviations in the context of an app include (a) constraining, limiting, and not providing an ethical choice (autonomy), (b) non-consideration of environment and social well-being, (c) discrimination, (d) exposure to privacy or unconsented use of personally identifiable data, (e) inadequate security or safety consideration, (f) non-transparent systems, and above all, (g) incorrect or inconsistent results or outputs.

Apps that (1) gathers more information than required, (2) exploits the cognitive biases of users, and (3) constrains users to avoid sharing information or deleting their information from the app, are all examples of ethical deviations in apps used by adolescents.

## Ethical issues in focus

In this white paper, we examine ethical issues associated with four key sections, namely (1) Privacy, (2) Age-appropriateness, (3) Human-in-the-Loop, and (4) User interface.

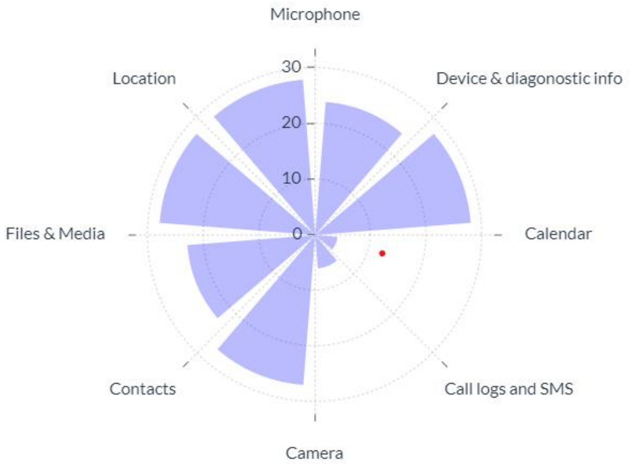
1. The privacy section covers issues associated with privacy policy, consent, data collection, data shared with third parties, and use of third-party trackers.
2. The age appropriateness section covers issues associated with age limits mentioned in the app marketplace places, age appropriateness of design and content filtering in the apps, and age verification by the apps.
3. Human-in-the-loop section covers issues associated with parental consent and parental access
4. The user interface section covers issues associated with nudges and deceptive design patterns

# III. Privacy

## Permissions - Overview

Permissions are consent requirements for collecting, processing and using data from the user by the app developer/ owner. The consents are primarily for accessing the app features (e.g., uploading photos), a personalized path within the app (e.g., game path based on choices made in the user journey), and app interactions (e.g. gathering of touch screen interactions for improving products), etc.

Count of apps that required these permissions

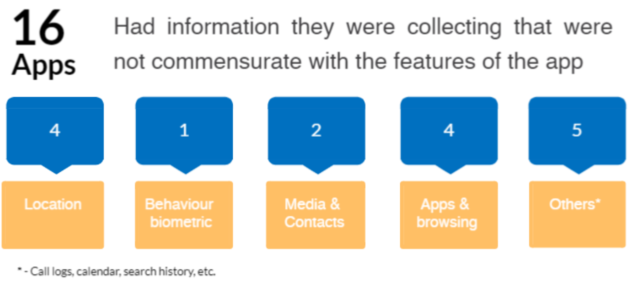


These permissions seek consent from the user at the time of registration or during the app's runtime. Analysis was done based on permissions compiled from the permission manager on an android device. The permissions were broadly relating to (a) contacts, (b) microphone access, (c) files and media, (d) camera, (e) location, (f) call logs & SMS, (g) calendar, and (h) device & diagnostic information.

Most app developers provide the details and nature of permissions sought for location in the privacy policy. Further, these permissions are at broad level and not specific. For instance, location access permission can be used for tracking a coarse location or precise location information. The location access can be used to gather personal information along with the location or just gather non-personal location data. The permissions just ask if location data can be shared as a pop-up, they do not explain the details of how location data would be used when the permission is sought. Hence, permissions need to be examined in line with the privacy policy and the app features to see the relevance of such data collection.

## Permissions not in line with features

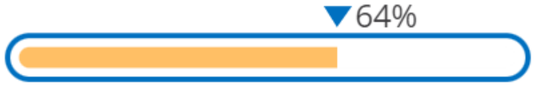
Comparing the permissions with the app's features revealed 16 apps with permissions that were more than the app's features.


16
Apps
Had information they were collecting that were not commensurate with the features of the app
4
Location
1
Behaviour biometric
2
Media & Contacts
4
Apps & browsing
5
Others*
* - Call logs, calendar, search history, etc.

The location data is used for personalizing advertisement that is targeted to the general location of the user. The collection of location information has no direct connection to the user experience or the app's features. For instance, the gaming app Asphalt 9 requires coarse/ general and precise access to location information.

## Opt-out of processing

Privacy regulations require app developers to provide an option to the user to opt-out of personal processing data.



64% of Apps had the option to opt-out of processing. However, these were tailored for one or more aspects of cookies, interest-based advertisement or for marketing communications. But not for the core purpose of processing.

A review of the apps' privacy policy revealed that 64% of apps had mentioned opt-out of processing in their privacy policy. However, these mentions are primarily related to opting out of marketing emails or opting out of personalized advertisements, instead of opt-out for the core services. For instance, none of these apps allow users to choose processing activities for which their data can be used.

## Data sharing with third party

92%

of the apps were sharing data with third party

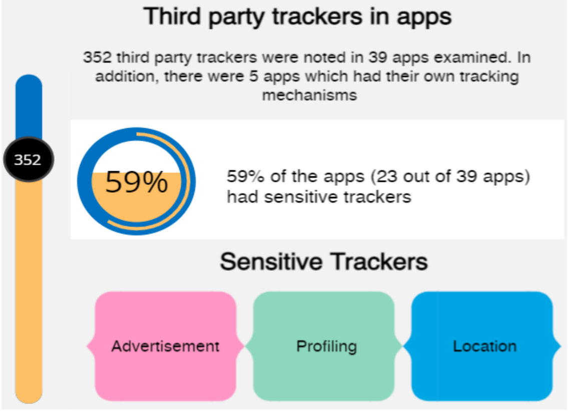
92% of the apps mentioned sharing data with a third party as part of their privacy policy. While the nature of data sharing varied (e.g., data shared with a third party engaged for support in the product), no specific data minimization was associated with sharing data of adolescents or children.

## Third party trackers

Trackers gather additional information, including app diagnostics, crash reporting, and analytics, thereby finding ways to enhance the app features. Companies can have their trackers or embed third-party trackers in the app code.

Exodus Privacy is a website dedicated to identifying privacy and third-party tracker information regarding the apps deployed in the marketplace. A review of third-party trackers available on the apps revealed the following:

1. There were over 352 third-party trackers in the apps examined, excluding apps that had their trackers (e.g., Google, Facebook)
2. 59% of apps reviewed had at least one of the three trackers (advertisement, profiling, and location) that dealt with sensitive information.



Third party trackers in apps

352 third party trackers were noted in 39 apps examined. In addition, there were 5 apps which had their own tracking mechanisms

59% of the apps (23 out of 39 apps) had sensitive trackers

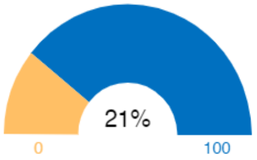
Sensitive Trackers

For apps used by adolescents, permissions beyond feature requirements, lack of an option to opt-out of processing, data sharing with third parties, and the existence of trackers expose the apps to several ethical issues.

# IV. Age Appropriateness in apps

## Age limits on app marketplaces

The age reference provided in the marketplaces (Apple App Store and Google Play Store) determines the appropriate age for accessing the app.

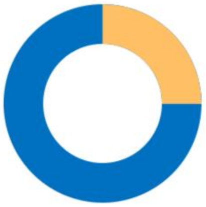


In 21% of apps, the eligible age prescribed by app marketplaces were less than the eligible age prescribed by privacy policies of such apps

In 21% of apps, the appropriate age as referred by the marketplace was less than the age appropriateness as directed in the app's privacy policy. For instance, certain apps in the marketplace had "Everyone" or "4+", indicating that the app is suitable for children; however, as per the privacy policies of these apps, the intended age of the users shall be over 13. For instance, PUBG is designed for children above 12 yrs as per the App marketplace, while the privacy policy indicates that it is intended for children above 18 yrs of age. Similarly, for the app Among Us, the intended age per the app marketplace was ten yrs+, while the privacy policy indicates that its users should be above the age of 13+. Some of the apps examined contained violence, provided access to adult content, and allowed other users (strangers) to interact with the users (in our case, adolescents).

These communications do not have age-appropriate filters concerning shared photos and videos, comments or abuses on chat messages, violence, or gore in the content shared/ displayed.

## Inappropriate content



25%

of Apps contains groups servers with adult visuals (video/ images) or games with violence

25% of apps contained content including adult visuals (videos/images) or games with violence. In some cases, the users had access to chat groups or rooms wherein pornographic contents were shared or traded. Some groups (especially in apps like Kik, Discord & Telegram) work on

1. (a) ‘Pay to play model (where the user must pay in crypto coins or gift cards to receive content), and

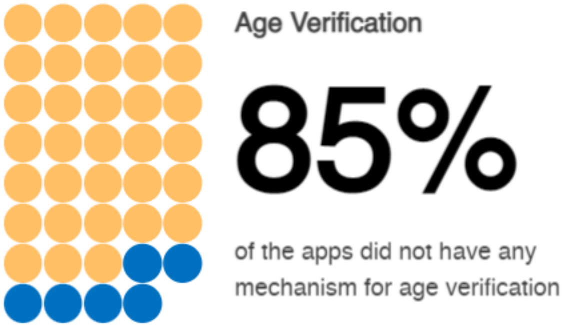
2. (b) some of them work on ‘Play for play’ model (where the user has to share pornographic content of self or curated to get access to content from others).

Game apps (e.g., Among us, IMVU, etc.), with peer-to-peer chat functionality where players chat with each other, did not have any content filters allowing abusive or inappropriate language in these communications. Particular apps also provide access to groups that trade in arms.

## Age verification

51% of the apps examined consider the age of the users based on the declaration, while they do not validate them, despite the need to register using a Gmail id or Facebook id (13-year-old can create Gmail and Facebook accounts).

Age declarations are not cross-verified with the content searches performed by the users.



Some the apps like Twitter banned the user id for searching content that was not age-appropriate, while apps like Telegram, Facebook, Instagram, Snapchat, Tiktok, Pinterest, and IMVU do not have any such age-appropriate content filter.

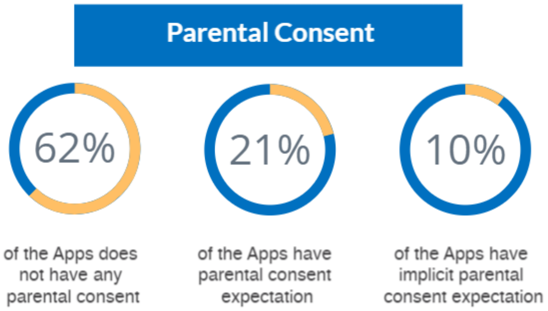
Some apps (e.g., Tiktok and Instagram) perform age verification if there are attempts to change the age from minor to primary. However, this does not apply to incorrect or false age declarations in the first instance.

App developers, UX designers, and behavioral economists have long interrogated how design influences human interaction. Apps vie was engagement with the user to make the app usable and relevant. However, measuring engagement without consideration of age-appropriateness or age verification results in systemic social impacts on adolescents using such apps.

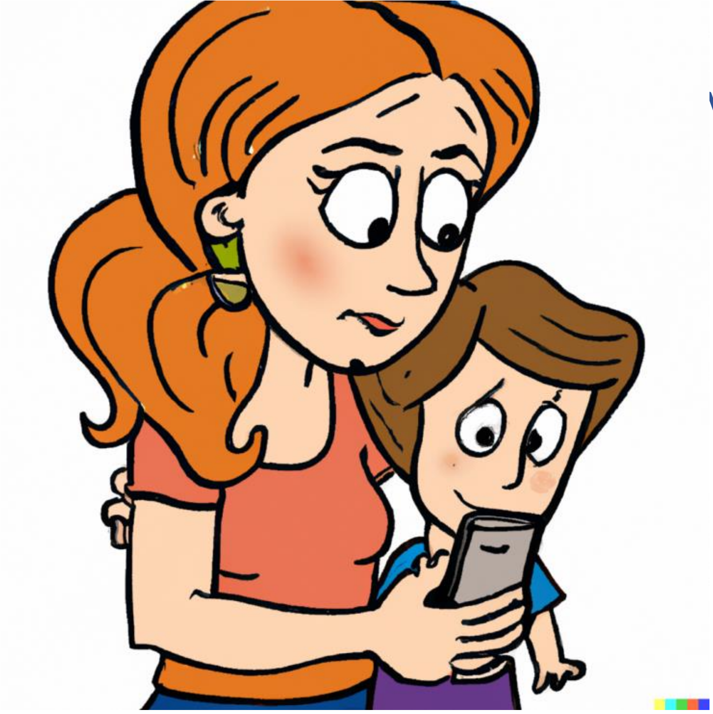
## V. Human-in-the-Loop

### Parental consent

21% of apps had parental consent requirements as part of their privacy policy and app registration journey. Another 10% of apps assumed parental consent, as explained in their privacy policy. Parental consent requirements do not apply if the user (adolescent) falsely declares age as an adult or if the adolescent uses the app without registering.



* - for 8% of the apps the parental consent reference is unclear



## VI. Interface Design

### Ethical design

Ethical interface design in apps is essential to ensure that it encourages, enriches, and empowers children and their welfare.

Digital Nudging is the use of user-interface design elements to guide people's behaviour in digital choice environments (10]. A nudge is a function of any attempt at influencing people's judgment, choice, or behavior in a predictable way. The underlying choice architecture (of nudges) that predictably alters people's behaviour shall not limit any options or shall not significantly change economic incentives. [8]. Thaler, one of the co-authors of "Nudge" (book), mentions in one of his posts in the New York Times, details three critical principles of nudges. They are (1) Nudging shall be transparent, (2) It should be accessible to opt-out of the nudge, and (3) Reason to believe that behavior influenced is for the welfare of those being nudged [8].

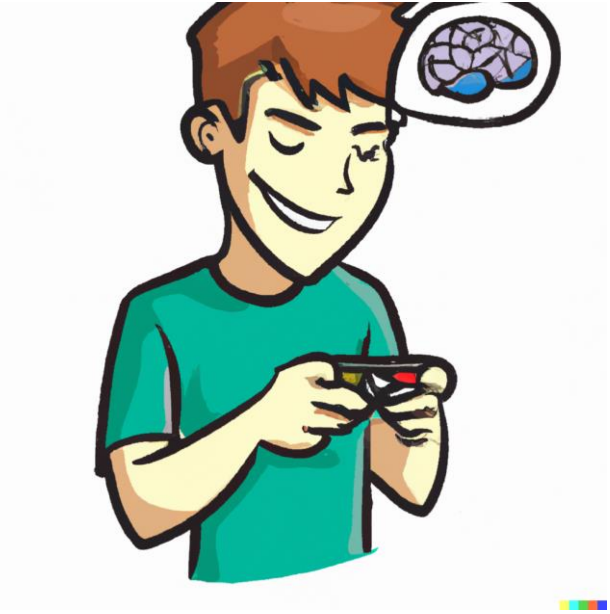
It is necessary to understand that not all nudges are effective, and some of the nudges may harm the users due to their behavioral economics informed manipulative nature (also called budges or deceptive design patterns) [9]. Deceptive Design Patterns may cause emotional or cognitive harm besides financial harm. These harms are known to contribute to depression or anxiety, or other mental health [10].

### Parental controls

Only 21% of apps had parental controls, wherein the parents had the opportunity to control and manage the children's access to the app. However, most apps consider an age threshold of 13 years for parental controls, as guided by the regulations. Further, the apps require the parent's email ID to be provided for enabling parental controls; however, it does not validate such email. For instance, even if the adolescent provides another email id of theirs as the parent's email id, it will accept them. During the validation process, an alias email id was used for the registered email id for creating an account as a parental email id, and the app sent notifications for parental controls and consent.

Deceptive design patterns exploit the cognitive bias of the user to persuade them to do things they would not otherwise do, using design tactics and persistent attention-seeking behavior. The ethics of deceptive design patterns are widely discussed in academia and business. However, would the degree and sensitivity of such discussion change if the user in question was a Child?

Deceptive design patterns drive users (children) to make accidental or uninformed decisions against their best interests [11]. The design inherently has a purpose of persuasion embedded in it; however, some techniques can be exploitative or harmful to the users. Avoiding making a harmful persuasive design is in the hands of the app / UX designer. With recent awareness of the implications of deceptive design patterns and bad UX designs, more researchers in the Human-Computer Interface community are exploring a moral and ethical approach to design.



Deceptive design patterns appear as (a) a dialog or pop-up when launching the app, (b) as a guided flow in user journey design or navigation layout, (c) as a notification or a highlight in the app bar that brings users' attention to the app, and (d) as a hidden feature that hides or ignores to disclose essential information to the user.

### Implications of deceptive designs

The implications of deceptive design patterns, specifically the long-term impacts of exploiting cognitive biases, have not been studied extensively. The short-term consequences of deceptive design patterns include exposure to privacy, unnecessary monetary spend, spending significant time with the app, change in belief systems including more weightage to social validation, etc. The questions that require examination in this context are:

1. What is the privacy trade-off for children (including adolescents) caused by the inconvenience of deleting the account?
2. What is the long-term economic behavior of children (including adolescents) who tend to buy premium subscriptions influenced by a dark pattern?
3. What kind of emotional influence that children go through due to social validation or social pressure induced by the deceptive design patterns?
4. What psychological impacts are caused to children (including adolescents) by consistently falling prey to deceptive design patterns?

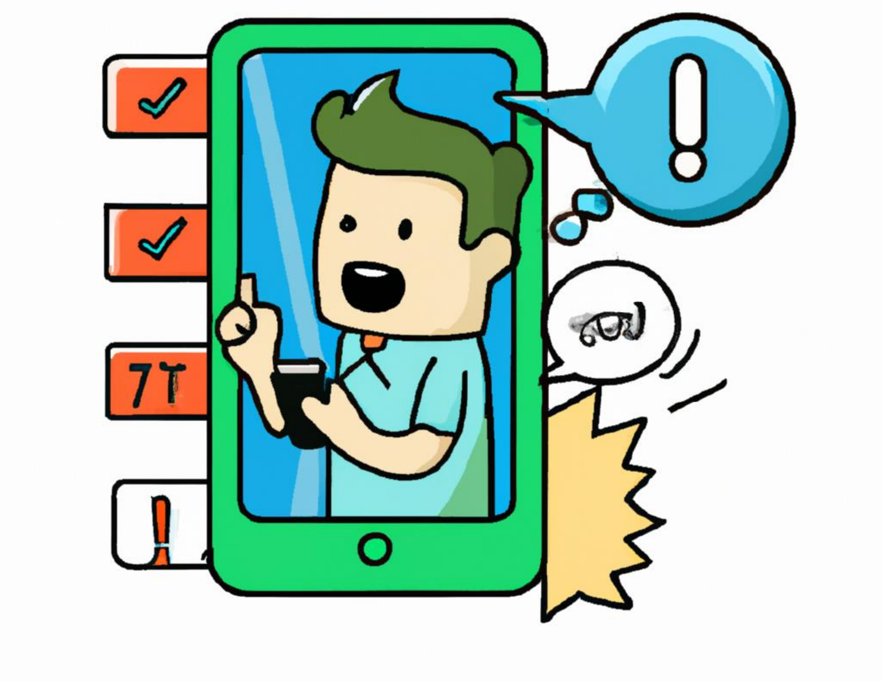
These physical, economic, emotional, and psychological implications of deceptive design patterns can throw numerous questions requiring detailed research. More than anything else, they need conscious and thoughtful, ethical solutions.

### Stages of the user journey

While classifying deceptive design patterns into taxonomies has been extensively studied in the research, exploring where such design patterns occur in the user journey is also critical. For instance, the maximum number of deceptive design patterns found in games played by children were all in the stage where the user is engaging with the app (i.e., playing the game) and not necessarily at the time of signing up, subscription or even deleting the account.

User journey stages and examples of the deceptive design patterns are used to simplify understanding of such design patterns.

This white paper attempts to explain the kind of deceptive design patterns that appear at every stage of the user journey to understand the potential implications of such deceptive design patterns. These deceptive design patterns cannot be identified entirely based on research studies alone. The study revealed over 270 deceptive patterns in the apps examined. However, these are non exhaustive, given that more deceptive patterns may emerge as the user journey deepens within the app. Needless to say, deceptive design patterns associated with the engagement stage with the user can be complex and very contextual.



## Deceptive Design Patterns across User Journey Points

- Initial access & sign-up
- Default settings
- Subscription
- Attention triggers to bring user into the app
- User engagement within the app
- Trading within the app
- Removing or deleting the account
- Others

Focussed UX risk assessments, independent audits, and disclosure requirements are some of the actions that can help limit the deceptive design patterns in the engagement stage with the user and develop trust with the stakeholders. Also, establishing a repository of deceptive design patterns or supporting existing ones can significantly contribute to future research and UX risk assessments and audits in this space.

User journey stages considered for this white paper are (a) Initial access and Sign-up, (b) Default settings within the app, (c) Attention triggers to bring the user to the app, (d) User engagement within the app, (e) Trading within the app (e.g., use of in-app coins), (e) Subscription, (f) Removing or deleting data or account and (g) others.

### Examples of deceptive designs

*Initial access & sign-up*

No of deceptive patterns 63

At the 'initial access and sign-up stage, the users come across deceptive design patterns like (a) providing privacy policy in small font, (b) seeking access to contacts by constantly nagging, and (c) prompting users to "allow" all subsequent permissions, (d) displaying an offer to avail credits that can be used within the app prominently while the price for such credits are given in small font, (e) only one action option ("accept") for community guidelines, (f) option to bulk add connections or people to follow within the app, and (g) allowing the user below 16 yrs to make their profile public.

## *Default settings*

51%

of the Apps had notifications settings pre-selected as default

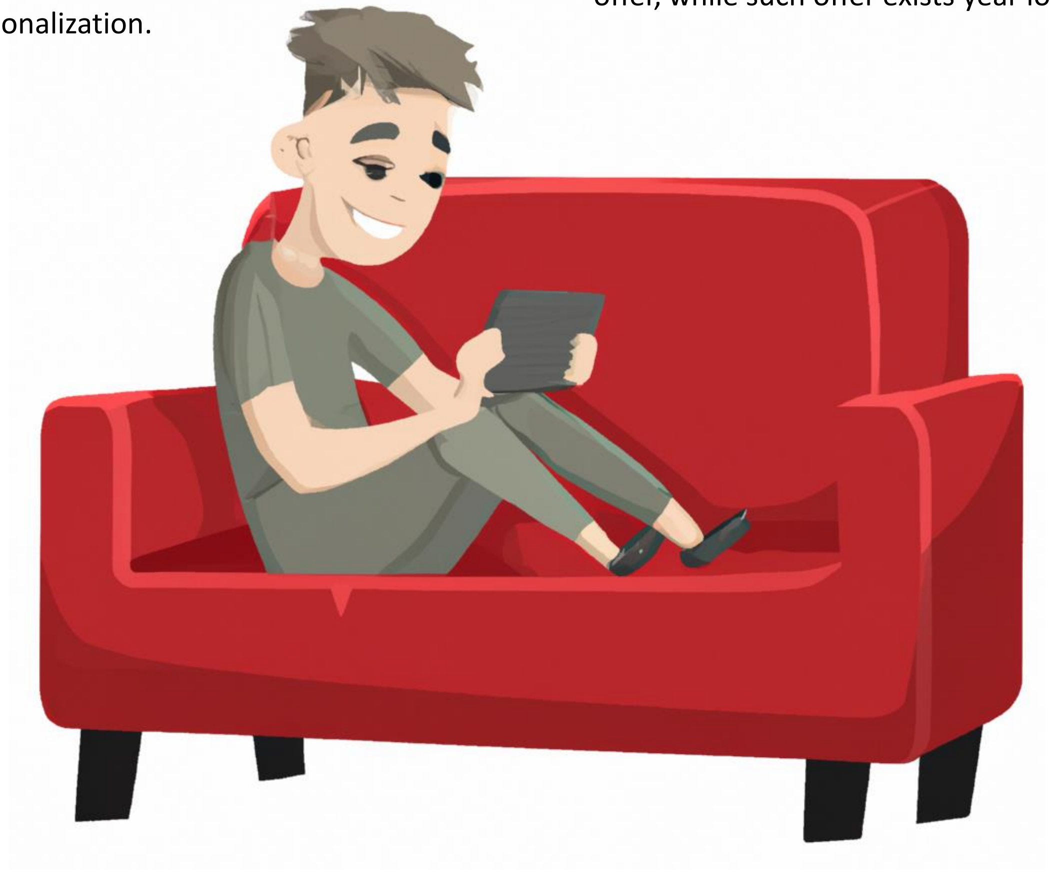
33 No of deceptive patterns

The ‘default settings’ stage has deceptive design patterns that are (a) activating all push notifications, (b) allowing to download videos and media using mobile network data (instead of wifi), (c) permissions to continuously sync contacts, and (d) settings for advertisement personalization.

## *Subscription*

15 No of deceptive patterns

The ‘subscription’ stage has deceptive design patterns that (a) preselecting high value or long-term subscription plan for the user, (b) show up subscription page without the option to move back into the app, and (c) upgrading to ensure additional features or availed or option to correct the actions within the app (revisiting profiles that were swiped left), (d) showing only one subscription while multiple subscription plans exist, (d) raise a ticket and wait for 24 hrs to cancel the app subscription, and (e) displaying an urgency to subscribe at a discount price exhibiting it to be one time offer, while such offer exists year long.



### *Attention triggers to bring user into the app*

23 No of deceptive patterns

The ‘attention triggers to bring the user into the app’ stage has deceptive design patterns that are (a) rewarding daily access to the app, (b) reminders and notifications to nudge the user into the app (e.g., “you have not swiped in a while” messages in Tinder, (c) false/phantom notifications wherein the user believes he has got new content or communication from another user, and (d) insults or emotional triggers to bring attention to the app.

### *User engagement within the app*

No of deceptive patterns 97

The ‘user engagement within the app’ stage has deceptive design patterns that are (a) advertisements being disguised in between posts within the app and (b) communications from the app provider within the app classified under chats, thereby creating an impression that there are messages from another user, (c) seeking run-time permissions while the user is in the middle of an action, to access the gallery, record video and capture photographs, (d) design changes to place “shopping” button at the place where there was “notification” button earlier, thereby attempting to influence muscle memory of users, (e) making syncing contacts and sharing of profile as an essential action for profile update within the app and showing them as incomplete till the time these actions are done, and (f) influencing to spend real money to get more in-app coins that can be used during a game.

### *Trading within the app*

22 No of deceptive patterns

The ‘trading within the app’ stage has deceptive design patterns that are (a) in-app coins being charged for skipping an action within the app, (b) opportunity to boost one’s profile by using in-app coins, (c) providing users with an option to purchase virtual outfits or gifts or in-app virtual merchandise, and (d) influence to gain in-app currency by watching videos (some of it would be advertisements).

### *Removing or deleting account or data*

19 No of deceptive patterns

‘Removing or deleting an account or data from the app’ stage has deceptive design patterns that are (a) removing or deleting account feature inaccessible within the app, (b) requiring the user to send an email to request for deletion, (c) providing alternative option to pause instead of deleting account, (d) delete feature adds a condition to wait for a minimum of a certain period (1 month in some cases) without accessing the app to ensure deletion of the account, and (e) claiming that deletion of data can be done, but not the deletion of account for record-keeping reasons.

### *Others*

7 No of deceptive patterns

The 'Others' stage is a miscellaneous category of deceptive design patterns not covered in other stages. They include (a) UX design wherein the actions buttons are placed at the place where some of the mobile devices (android) will have a back button, thereby engaging users with content even when they want to go back from the page, and (b) feedback or grievance reporting feature takes the user to frequently asked questions, (c) requiring the user to download additional data soon after installation for running the app to disguise the size of the app on app marketplaces, and (d) parents who are required to provide consent for their child's privileges within the app, have to consent to all cookie setting in the webpage without an option to disagree/ consent to a part of them.

All these are used to exploit for creating engagement, continuing the service, making a financial commitment/ purchase, or using the user's data for business purposes.

# VII. Way Forward

### Ethics by design

The ethical design of apps must become a primary expectation in how apps are designed, developed, and deployed in the marketplaces. This shall include the adoption of Standards and Principles or a Code of conduct for designers and developers to demonstrate commitment to ethics in the app development lifecycle.

### Platform based governance

App marketplaces are the primary gateway for apps to be accessed by children and adolescents. App marketplaces like Google Play Store and Apple App Store currently have conditions that an app shall comply with. This includes requiring disclosure of privacy consents needed within the app and requiring the app to go through a process of app listing to ensure the broad level expectations are met. However, these requirements by the marketplaces do not limit the apps to avoid any of the ethics issues highlighted here. It is pertinent to note that the problems highlighted are for most used apps; there may be apps that children and adolescents use with serious ethical issues beyond the ones highlighted here. Hence, there is a need for policy expectations, hosting requirements, oversight, and enforcement mechanism to act on reports or complaints from users for violations regarding apps designed for children. These violations could be aligned to the relevant jurisdictional legal frameworks, thereby avoiding unscrupulous and unethical apps being deployed on the marketplace.

### Audit requirement

The age-appropriate Design Code of the UK lays out clear expectations for apps falling under Information Society Services (ISS). Similar regulations are emerging across geographies, including the California Age-appropriate code. Beyond just a compliance regulation, a mandate to publish annual audit reports for the apps deployed on the marketplace brings an opportunity for children and parents to have mechanisms to be aware of these apps' compliance status. These audits shall demand (1) Independence of auditors, (2) Clearly defined audit criteria, (c) Trained auditors, and (d) audit conducted on behalf of the public, not on behalf of the app developer, and (e) Transparent disclosure of audit report on the marketplace or within the app. ForHumanity (a non-profit) working to build audit criteria for audit of AI systems is developing such an infrastructure of trust. Such an action would enhance trust and bring uniformity of consideration for preserving and protecting the rights of children and adolescents.

### Privacy-preserving technology

Privacy threats associated with apps used by children and adolescents may significantly impact their life and well-being. They may also have long-term effects (privacy exposure or data breach) and psychological or financial distress. Adopting privacy-preserving technologies (Differential Privacy, Federated Learning, etc.) could be an alternative for managing privacy risks to children and adolescents, providing adequate privacy for users to engage with the app.

### Regulatory enforcement

Regulators in select geographies (the UK and the Netherlands) are beginning to enforce Corporations for violation of Children’s rights and age-appropriate design expectations [6]. Practical enforcement actions and financial penalties deter corporations from adopting approaches that may violate the relevant jurisdictional regulation.

## VIII. Conclusion

In conclusion, ethical considerations in developing and deploying apps for children and adolescents are necessary and cannot be undermined, considering mobile apps' influence on them. While regulatory requirements are making clear expectations on privacy and children's rights, there is a heightened need for operating responsibly. Responsible development and deployment of apps used by children and adolescents must move beyond regulatory expectations to minimum levels of public technology, establishing the baseline for responsible apps.

# Bibliography

1. Jiang, Jingjing. “How Teens and Parents Navigate Screen Time and Device Distractions.” *Pew Research Center: Internet, Science & Tech*, Pew Research Center: Internet, Science & Tech, 22 Aug. 2018, www.pewresearch.org/internet/2018/08/22/how-teens-and-parents-navigate-screen-time-and-device-distractions/
2. Jacobo, Julia. “Teens Spend More than 7 Hours on Screens for Entertainment a Day: Report.” *ABC News*, ABC News, 29 Oct. 2019, abcnews.go.com/US/teens-spend-hours-screens-entertainment-day-report/story?id=66607555.
3. “Children and the UK GDPR.” *Ico.org.uk*, ICO, 27 May 2022, ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/. Accessed 16 Aug. 2022.
4. “Age Appropriate Design: A Code of Practice for Online Services.” *Ico.org.uk*, ICO, 28 July 2022, ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/.
5. “Mobile Apps.” *Federal Trade Commission*, 11 Feb. 2022, www.ftc.gov/media/71318. “Dutch DPA: TikTok Fined for Violating Children’s Privacy | European Data Protection Board.” *Europa.eu*, 2021, edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en. Accessed 16 Aug. 2022.
6. Hartung, Pedro. *The Children’s Rights-By-Design Standard for Data Use by Tech Companies*. 2020, [www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf](www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf).

7. Nesterak, Evan. “Five Takeaways from Our Conversation with Richard Thaler about the Past, Present, and Future of Nudge - Evan Nesterak - Behavioral Scientist.” Behavioral Scientist, 21 Sept. 2021, behavioralscientist.org/five-takeaways-from-our-conversation-with-richard-thaler-about-the-past-present-and-future-of-nudge/.

8. Jonas, et al. “The Effectiveness of Nudges in Improving the Self-Management of Patients with Chronic Diseases: A Systematic Literature Review.” Health Policy, vol. 123, no. 12, 2019, pp. 1199–1209, econpapers.repec.org/article/eeehepoli/v_3a123_3ay_3a2019_3ai_3a12_3ap_3a1199-1209.htm.

9. Wang, Jin-Liang, et al. “The Association between Mobile Game Addiction and Depression, Social Anxiety, and Loneliness.” *Frontiers in Public Health*, vol. 7, 6 Sept. 2019, www.frontiersin.org/articles/10.3389/fpubh.2019.00247/full, 10.3389/fpubh.2019.00247.

10. Schneider, Christoph, et al. “Digital Nudging–Guiding Choices by Using Interface Design.” *Ssrn.com*, 13 Oct. 2017, papers.ssrn.com/sol3/papers.cfm?abstract_id=3052192.

11. Kernaghan, Chris. “The Dark UX Patterns Targeting Children - UX Collective.” *Medium*, UX Collective, 19 Mar. 2021, uxdesign.cc/the-dark-ux-patterns-targeting-children-6c6cb1f0624d. Accessed 18 Aug. 2022.

© 2022. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system, except by providing due credit to the work.

This document is published as a white paper based on research conducted by Sundar Narayanan. The findings, interpretations and conclusions expressed herein are a result of research conducted between 01 January 2022 to 15 August 2022.

This material is based upon work supported in whole or in part by The Notre Dame-IBM Tech Ethics Lab. Such support does not constitute an endorsement by the sponsor of the views expressed in this publication.

Image credit: All images in this report were generated using text prompts in DALL-E (OPEN AI)

Note: As part of the project a workshop was conducted to gather multi-stakeholder feedback on deceptive design patterns identified. However, the participation in the workshop was less representative and hence the results of the workshop is not considered inthis report.