Integrating Dark Patterns into the 4Cs of Online Risk in the Context of Young People and Mobile Gaming Apps

Dan Fitton, Beth T. Bell, Janet C. Read

▶ **To cite this version:**

Dan Fitton, Beth T. Bell, Janet C. Read. Integrating Dark Patterns into the 4Cs of Online Risk in the Context of Young People and Mobile Gaming Apps. 18th IFIP Conference on Human-Computer Interaction (INTERACT), Aug 2021, Bari, Italy. pp.701-711, 10.1007/978-3-030-85610-6_40 . hal-04215510

HAL Id: hal-04215510

https://inria.hal.science/hal-04215510

Submitted on 22 Sep 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

Integrating Dark Patterns into the 4Cs of Online Risk in the Context of Young People and Mobile Gaming Apps

Dan Fitton[1][0000-0002-2300-5432], Beth T Bell[2][0000-0002-6587-0336], and Janet C Read[1] [0000-0002-7138-1643]

[1] ChiCI Research Group, University of Central Lancashire, Preston, UK
{DBFitton,JCRead}@UCLan.ac.uk
[2] School of Psychological & Social Sciences, York St John University, York, UK
b.bell@yorksj.ac.uk

Abstract. Mobile technologies potentially expose children and adolescents to increasing online risk. These risks take many forms and are widely categorized using the 4Cs: Content, Conduct, Contact, and Commerce. Commerce is the least developed category and, while it has significant overlap with what is known as Dark Design within the field of UX, amalgamation of Dark Design and the 4Cs has not yet been considered. Within this paper we integrate Dark Design into the 4Cs to provide a set of questions we call RIGA (Risk In Games Assessment) and use RIGA to identify potential risks to children and adolescents in free-to-play mobile gaming apps. The key contribution of this paper is the integration of contemporary understandings of Dark Design into the 4Cs framework, through the RIGA question set, which can support research and practitioner communities in identifying potential risk to young people present in mobile gaming apps.

Keywords: Dark Patterns, Dark Design, Online Risk, Games, Children.

1 Introduction

Mobile digital technologies are ubiquitous in contemporary society and are increasingly considered to be integral to the daily lives of young people (adolescents and children) [1] [2]. Young people often use their phones as a source of entertainment ([3] [4]) and particularly for mobile gaming. At the time of writing indications [5] are that the Google Play store contains almost 3.2 million apps/games and the Apple iOS app store almost 1.8 million, with tens of thousands being added monthly. Both Apple and Google require that products submitted to their app stores include an age rating to protect adolescents and children from inappropriate content, but each takes different approaches to ensuring compliance. Apple use their own staff for vetting whereas Google provide policies for developers to engage in their own vetting through a self-report process. For example, the Google Play store has a 'Restricted Content' policy [6] that developers are expected to adhere to which references child endangerment, inappropriate content, finance, gambling, illegal activities and user generated content. While Google's approach is scalable, the developer-reported content ratings may be applied inaccurately [7, 8] and are only queried when users (typically parents) report inappropriate content.

The effectiveness of the approach depends to some extent on developers understanding the wording and nuances of the guidance provided to them. At the time of writing this paper the Google Child Endangerment policy states 'Apps that appeal to children but contain adult themes are not allowed'; this raises questions of how the developer would know what age child is being referred to, or how appeal may differ between age groups, or even how appeal would be measured. It is also the responsibility of the app developer themselves, or users who identify and report breeches of policy, to ensure adherence.

Due to their limited spending power, young people often use free-to-play mobile games where there is no initial cost for download and use. The business model for such apps requires that monetization is included within the gameplay; typically implemented through adverts which the user must watch or in-app purchasing possibilities the player is encouraged to engage in. To encourage such engagement subtle 'Dark' techniques may be employed like coercion to pay or making it deliberately hard to close an advert [9]. As the free-to-play model is used in over 95% of mobile apps, not just those targeted at young people, the implementation of monetization in apps and games is commonly developed by adults for adults. It is unclear whether younger users are considered in the design of these monetization mechanisms, and the effect these mechanisms (along with their associated risk) may have on younger users compared to adults is not well understood.

The key contribution of this work is the integration of Dark Design into the 4Cs framework, achieved in this paper through the creation and application of the RIGA (Risk In Games Assessment) question set. Our work also highlights the importance of an interdisciplinary approach to topics such as technology risk, combining work from the fields of UX and Psychology. The RIGA questions provide a means for identifying potential risk to young people in mobile gaming apps which operationalizes and elucidates the motivations which underpin the guidance provided to app developers. Additionally, RIGA can potentially be used by a range of stakeholders including academics, developers, parents, educators and young people themselves.

2 RELATED WORK

Risks of harm in relation to technology use among young/vulnerable users are typically clustered around four Cs; Content, Contact, Conduct and Commerce [10].

Content risks refer to those stemming from exposure to potentially harmful digital media content (e.g., self-harm content, appearance ideals, violence [10]). Research has demonstrated how violent media content, particularly in video games, can have negative, yet small, effects on childrens' and adolescents' aggression and mood [11] though these effects are widely debated (e.g., [12]). More recently, content that alludes to self-violence (e.g. self-harm and suicide) in social media spaces has been identified as posing risks to children and young people, triggering distress or possible contagion ([13]). Sexualized media content has received considerable attention from researchers with research documenting the negative consequences of accessing both graphic sexual material (e.g., nudes, pornography) and non-graphic sexual material (e.g., revealing images; [14] [15]). Research has also highlighted how unrealistic body ideals (e.g.,

surgically enhanced or ultra-thin models) can foster negative body image and encourage unhealthy body-shaping strategies in young people ([16]), including in mobile games played by girls aged 8-9 years old ([17]).

Contact risks are those that stem from online social interactions/relationships with those who wish to bully/abuse/troll. Contact risks can take many forms, including the experience of unwanted sexual messaging (e.g., sexting), harassment, grooming, cyberbullying, hate speech, denigration, and other users pretending to be someone who they are not [18]. As contact risks stem from the misappropriation of communication tools by users rather than from the app itself, these risks can be more difficult to regulate than content risks. The Google Play policy specifies that apps that contain or facilitate threats, harassment or bullying are restricted, and app developers are responsible for ensuring that the app, including any user-generated content facilitated by it adhere to this policy [6], although this policy can be difficult to police.

Conduct risks stem from a user's own personal conduct within digital spaces. Antisocial behavior is perhaps the most prominent of these conduct risks and encompasses a diverse range of behaviors from bullying to harassment [2]. In addition to causing harm to others (i.e., the victim/receiver of the antisocial behavior), there are important negative consequences for the perpetrator including loss of reputation, criminality and potential legal repercussions e.g., [19]. In mobile gaming, anti-social behavior may be directed at other users (e.g., through in-game contact) or it may be directed at within game characters. Conduct risks can also stem from sharing of personal data, since it potentially exposes users to harms associated with the misuse of this data and/or privacy breaches [20].

Commerce risks (also known as commercial risks or cyberscams [10]) refer to risks stemming from the commercial or profit-making aspects of online space, e.g., fraud, accidental spending, perceived pressure to spend, etc. Commerce risks are growing; in 2018, around 17% of 12-15 year-olds in the UK reported that they have accidentally spent money online, up from 9% the previous year [1]. These risks are a late addition to the 4C framework and remain relatively understudied in relation to children and teenagers, in comparison to other types of online risks [10]. According to Ofcom [1], spending pressures in gaming is 'an area of specific and growing concerns among parents of children of all ages'; 39% of parents of children aged 5-15 years old are concerned about pressures to make in-app purchases. These in-app purchases take many forms including access to additional points, tokens or levels, full-app teasers or for game up-grades and add-ons [9], and are integral to revenue generation in free-to-play apps (and games). In-app purchases are regulated, including through opt-in parental controls that moderate spending, such as the "Ask to Buy" system in the app store. In addition to in-app purchasing, advertising is also a way in which users may be exposed to commercial risks within games, resulting in accidental spending, perceived pressure to spend, etc. Perhaps unsurprisingly, advertising is much more salient in free-to-play apps than paid for apps [21] reflecting the integral nature of advertising to current business models.

In the UX and HCI communities there is a small, but growing, body of work exploring 'Dark Design' within technologies [22] [9] [23] [24]. The notion of Dark Design Patterns initially emerged from the UX practitioner community, defined as 'a user

interface carefully crafted to trick users into doing things they might not otherwise do'[25]. A Design Pattern is a proven solution to a general problem which is intended to be reused [26]. Dark Design is driven by economic motivations and emerged from the study of e-commerce web sites where the intention of the designer appeared to be utilizing the design of the web sites to 'trick' shoppers into spending more than they intended or generating other potential income. Twelve original Dark Design patterns were identified [27] which were then explored in a gaming context by Zagal [24] and also studied in more detail by Gray [23]. Fitton [9] brought together existing work on Dark Design and related areas (in-app advertising, in-app purchasing etc.) though a user study involving teenagers to define the ADD (App Dark Design) framework to support the critical consideration of Dark Designs which included six categories containing multiple types of Dark Design: Temporal (Grinding, Play by Appointment, Interstitial Non-app Content), Monetary (Pay for Permanent Enhancements, Pay for Expendable Updates, Pay to Skip/Progress, Pay to Win, Subscriptions, Intermediate Currencies), Social (Impersonation/Friend Spam, Prompts to Share/Review, Social Pyramid Schemes), Disguised Ads (Advergames, Characters Placement), Sneaky Ads (Difficult/Deceptive to Dismiss, Camouflaged Game Items, Notification-based Ads), and Inappropriate (Unsuitable Adverts, Encouraging Anti-Social Behavior, Psychological Manipulation, Persuasive Design, Developmentally Insensitive).

Dark Design is employed heavily in free-to-play mobile apps games for monetization to generate the required revenue for the developers. For those installing a 'free' game on their phone it is unlikely that spending time watching adverts or making in-game purchases in order to play that game would be desirable, and so this provides the motivation for Dark Design. Mechanisms do exist to minimise designers including Dark Design elements in apps. Apple provides guidance to developers submitting their apps for review which states that 'tricking' users is not acceptable [28]. Google Play has a 'Monetization and Ads' policy [29] which contains a 'Deceptive Ads' section; this mentions several basic Dark Design examples which should not be used (Disruptive Ads, Deceptive Ads, Inappropriate Ads) with examples. However, the authors found examples of all three types of these 'Deceptive Ads' in the Android games they evaluated in this work. In 2015 Google Play launched a 'Design for Families' initiative which included a specific 'Family' policy [30] which should be adhered to when developing apps intended for child users. Compliance with the Family policy is specified as requiring age-appropriate advertising, excluding any adult content, adhering to applicable data/privacy laws and more stringent 'Ads and Monetization' guidance [30].

Despite this existing work, Dark Design is often very nuanced and requires a high level of knowledge or experience of design in order for it to be identified and fully understood. There is therefore a need to develop more clear guidance on Dark Design for researchers and practitioners both inside and outside of the field of HCI. Governments are also beginning to take the regulation of apps and games for children more seriously in their policy making. For example, in January 2020 in the UK the Age-Appropriate Design Code [31] was published which primarily controls how data shared by children can be used. This code states 'Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or turn off privacy protections.' which relates directly to the use of Dark Design by app developers. Despite this recent

policy work, Dark Design is not currently part of mainstream approaches to understanding online risks of harm among youth. There is therefore a need to integrate the two together, particularly focusing on Dark Design within Commerce risk.

3 Study: Integrating the 4Cs and Dark Design

In order to integrate the 4Cs and Dark Design the approach taken was to develop a set of questions that could be used to identify specific aspects within mobile gaming apps. Bell, a psychologist and expert in the role of digital media and technology in relation to youth mental health, developed a set of questions to identify evidence of the 4Cs of online risk in gaming apps. Fitton, an expert in youth UX, developed a set of questions to identify evidence of Dark Design (based on the ADD framework mentioned previously). The two authors then pooled their question sets and worked together to refine them, ensuring that the questions were simplified as much as was practical with the intention of allowing them to be applied with low levels of ambiguity by those outside the fields of UX and Psychology. This set of questions forms the RIGA (Risk In Games Assessment) question set which is shown later in the paper in Table 2. RIGA included 15 of the 22 Dark Design types in the ADD framework which made small contributions to Content and Conduct but was most useful in defining the Commerce dimension.

3.1 Evaluation Procedure

RIGA was subsequently used to evaluate 12 popular free-to-play mobile gaming apps that had been previously identified during a UK STEM event as containing 'interruptions and annoyances' (i.e. potential Dark Design elements [11]). The data was gathered prior to the COVID - 19 pandemic from 120 pupils aged between 7-12 years from two junior schools, and from 90 pupils aged 13-14 from two high schools. The question posed in that study was 'What are the worst apps/games for interruptions or annoyances?'. Responses from the two age groups were collated and totaled. Then apps which were not games, and games with extensive gameplay complexity ('Roblox' and 'Fortnite') were removed to leave a final list of 12 games (See Table 1, games ordered by popularity of response, high-low).

In a heuristic-style evaluation, two of the authors of the paper (the evaluators), who were also the designers of RIGA individually played each game for familiarity and then inspected each with reference to the RIGA questions. In both first and second play episodes the evaluators attempted to 1) Complete on-boarding tasks [32], 2) Complete the first level or other equivalent objective, 3) Gather in-game currency and purchase an in-game upgrade. The ordering in which the games were played (then evaluated) was consistent and followed the ordering shown in Table 1. Games were played until the evaluators were satisfied that they had explored as much of the game as was necessary to form judgements or encountered high levels of repetition. Mean total gameplay time per game was approximately 30 minutes across both evaluators. The testing was done independently on two identical Android phones. A screen recorder was used for all gameplay to enable review of what was seen by each evaluator in each game if required.

A spreadsheet was used for coding containing the RIGA questions with drop-down lists for answers and areas for comments. Individual coding data (yes/no answers to each of the RIGA questions for each game) from each evaluator was then compared (risk totals per-game are shown in Table 1 including initial and final agreed totals out of a possible maximum score of 26). Disagreements were resolved through initial discussion of the reasons underpinning the coding, then revisiting and discussing the screen recordings of gameplay if needed. All incidences of coding disagreement were able to be resolved using this method to give the totals show in the far-right column of Table 1.

Table 1. Number of Risks Identified in Mobile Gaming Apps using RIGA.

Game	Coder 1 (Psychologist)	Coder 2 (UX)	Agreed
Geometry Dash	8	8	8
Candy Crush Saga	8	9	9
Helix Jump	7	7	7
Subway Surfers	17	15	17
Cooking Fever	8	8	8
Crossy Road	10	9	10
Knife Hit	14	12	14
Piano Tiles 2™ (Don't Tap...2)	16	17	17
BitLife - Life Simulator	8	8	8
Pick Me Up™	12	11	12
Episode - Choose Your Story	15	15	15
Rider	11	11	11

4 RESULTS

Table 2 shows the results of the evaluation. On the title row for each category we show the number of apps which contained at least one example of that type of risk (e.g. eight contained one or more Contact risk) followed by the results for the specific sub-categories. Nine apps contained some form of **content** risk with the most common content risk was advertising of age-restricted products such as TikTok or Instagram (which are restricted to users aged over 13 years old). Two apps featured unrealistic body imagery (Subway Surfers and Episodes) and two apps featured sexualized content/themes (BitLife and Episodes), with one featuring violent themes, though these were not particularly strong or graphic (Bitlife). Eight apps contained some form of **contact** risk through encouraging users to connect via social media, and of those three incentivized this contact. Two apps (Episodes and Candy Crush Saga) offered bespoke-to-app where users could connect via forums perceptibly over a shared love of the game.

Candy Crush Saga integrated contact between users within the app itself, by allowing users to share in-game 'lives'. Seven apps contained some form of **conduct** risk which often stemmed from the sharing of personal information with the app developers and/or third parties. This conduct risk was incentivized by appearing as a condition of use in three games which is a form of Dark Pattern. For example, Fig. 1 shows screen captures from the data collection agreement when the Helix Jump game is first opened, it appears to the user all three agreements need to be given to 'Start Playing' but only

the third one is actually necessary. Two apps facilitated anti-social behavior but in both instances, this was aimed at characters within the game rather than other users. Just one app incentivized antisocial behavior (Episodes). In this game, avatars could be instructed to behave in socially manipulative ways to gain praise from in-game characters.

All apps contained some form of **commerce** risk linked to in-app purchasing, including the ability to purchase permanent or temporary game enhancements, pay a regular game subscription or to pay to progress within a game. Nine apps had an in-game

Table 2: RIGA (Risk In Games Assessment) Questions and Results of Coding

Risk	***n***	***%***
1. Contact	**8**	***66.67%***
1.1 Does the game facilitate contact between users within the app/bespoke community spaces?	2	16.67%
1.2 Does the game allow facilitate contact between users through social media?	8	66.67%
1.3 Is communication between users incentivized?	3	25.55%
2. Content	**9**	**75.00%**
2.1 Does the game contain unrealistic body imagery?	2	16.67%
2.2 Does the game contain extreme body-shaping behavior?	0	-
2.3 Does the game contain users to nude images/pornography?	0	-
2.4 Does the game contain sexualized content/imagery/themes?	2	16.67%
2.5 Does the game contain violence (visuals and themes)?	1	8.33%
2.6 Does the game contain images of self-harm or suicide?	0	-
2.7 Does the game include advertising of age-restricted products/services?	7	58.33%
3. Conduct	**7**	**58.33%**
3.1 Does the app allow the user to engage in high risk conduct?	6	50.00%
3.1.2 Was this incentivized/nudged?	3	25.00%
3.2 Does the game allow users to engage in anti-social behavior?	2	16.67%
3.2.1 Was this incentivized?	0	-
4. Commerce	**12**	**100.00%**
Commerce: *Compulsive Use*		
4.1.1 Does progression require in-game resources which can be earned through repetitive play?	7	58.33%
4.1.2 Does the game attempt to make its use compulsive or habitual?	8	66.67%
Commerce: *In-App Purchasing*		
4.2.1 Can the user pay to gain permanent enhancements to the gameplay experience?	10	83.33%
4.2.2 Can the user pay to gain temporary enhancements to the gameplay experience?	4	33.33%
4.2.3 Can the user pay to progress?	3	25.00%
4.2.4 Can the user make regular payments to the game?	3	25.00%
4.2.5 Does the user need to purchase immediate currency to buy in-game items?	9	75.00%
Commerce: *Advertising*		
4.3.1 Does the game include advergames?	8	66.67%
4.3.2 Does the game include advertising which is challenging to dismiss?	10	83.33%
4.3.3 Is there advertising related directly to in-game items?	1	8.33%
4.3.4 Does the game include full-screen content not linked to the game?	9	75.00%
4.3.5 Does the game feature adverts that constrain playing times?	6	50.00%

currency to facilitate in-app purchasing. Ten out of the twelve apps contained some form of risk linked to advertising, including adverts that were difficult to dismiss, full screen adverts advergames, adverts that constrained playing times, and adverts disguised as in-game items. Fig. 2 (left) shows an advergame with a clear instruction to interact to play the game, Fig. 2 (right) shows the install page which opened once the user touched the phone screen. Nine apps contained features designed to foster habitual use, including allocating rewards (e.g., in-game currency) for daily log-ins and requiring repetitive play in order to progress.

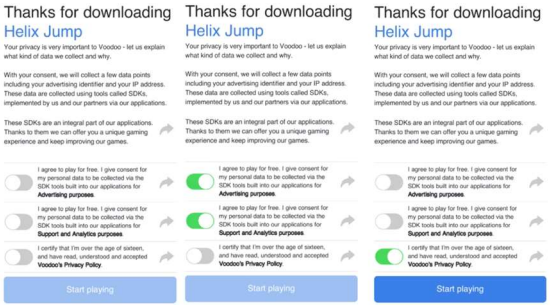

Fig. 1: Helix Jump Privacy Policy

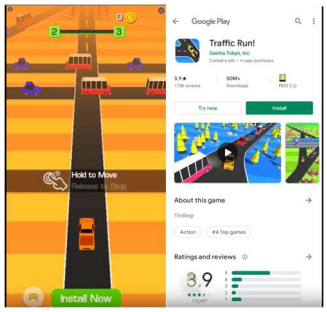

Fig. 2: Deceptive Advergame

5 Conclusion

We have integrated Dark Design research from the UX domain into the broader literature on the 4Cs of online harms from the Psychology domain to create the RIGA question set. The study showed that the RIGA questions proved a useful tool in identifying potential risk of harm in a set of popular Android free-to-play mobile gaming apps used by young people. Despite the existing guidance provided to developers, through using RIGA we found evidence of content, contact and conduct risks, including evidence of Dark Design being used to incentivize this risk. We found - perhaps unsurprisingly given the business models of current free-to-play gaming apps - substantive evidence of commerce risks within the games that we reviewed. It is important to remember that not all risks (or associated harms) are equal and that identification of a risk does not guarantee that an associated harm will occur. However, identification of risks (such as those discussed in this paper) is a crucial first step in understanding and addressing them. While this work is at a relatively early stage it makes a valuable contribution to the growing body of knowledge around Dark Design patterns and shows how understandings of Dark Design can be valuable in other contexts. The RIGA questions are intentionally easy to understand and have potential to be a valuable tool for a range of stakeholders involved in creating, understanding, and safeguarding the use of mobile gaming apps in the context of young people.

References

1. Ofcom: Children and parents: media use and attitudes report, https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2018, last accessed 2020/01/25.
2. Unicef: Global Kids Online Comparative Report, https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html, last accessed 2020/01/25.
3. Mascheroni, G., Ólafsson, K.: The mobile Internet: Access, use, opportunities and divides among European children. New Media Soc. 18, 1657–1679 (2016). https://doi.org/10.1177/1461444814567986.
4. Sudan, M., Olsen, J., Sigsgaard, T., Kheifets, L.: Trends in cell phone use among children in the Danish national birth cohort at ages 7 and 11 years. J. Expo. Sci. Environ. Epidemiol. 26, 606–612 (2016). https://doi.org/10.1038/jes.2016.17.
5. 42Matters: Store Stats for Mobile Apps, https://42matters.com/stats, last accessed 2020/01/25.
6. Google Play: Restricted Content - Developer Policy Center, https://play.google.com/about/restricted-content/, last accessed 2020/01/25.
7. Hu, B., Liu, B., Gong, N.Z., Kong, D., Jin, H.: Protecting your children from inappropriate content in mobile apps: An automatic maturity rating framework. In: International Conference on Information and Knowledge Management, Proceedings. pp. 1111–1120. Association for Computing Machinery, New York, New York, USA (2015). https://doi.org/10.1145/2806416.2806579.
8. Luo, Q., Liu, J., Wang, J., Tan, Y., Cao, Y., Kato, N.: Automatic Content Inspection and Forensics for Children Android Apps. IEEE Internet Things J. 7, 7123–7134 (2020). https://doi.org/10.1109/jiot.2020.2982248.
9. Fitton, D., Read, J.C.: Creating a framework to support the critical consideration of dark design aspects in free-to-play apps. In: Proceedings of the 18th ACM International Conference on Interaction Design and Children, IDC 2019. pp. 407–418. Association for Computing Machinery, Inc (2019). https://doi.org/10.1145/3311927.3323136.
10. El Asam, A., Katz, A.: Vulnerable Young People and Their Experience of Online Risks. Human-Computer Interact. 33, 281–304 (2018). https://doi.org/10.1080/07370024.2018.1437544.
11. Mathur, M.B., VanderWeele, T.J.: Finding Common Ground in Meta-Analysis “Wars” on Violent Video Games. Perspect. Psychol. Sci. 14, 705–708 (2019). https://doi.org/10.1177/1745691619850104.
12. Ferguson, C.J.: Does Media Violence Predict Societal Violence? It Depends on What You Look at and When. J. Commun. 65, E1–E22 (2015). https://doi.org/10.1111/jcom.12129.
13. Vanderweele, T.J., Mathur, M.B., Chen, Y.: Media Portrayals and Public Health Implications for Suicide and Other Behaviors, (2019). https://doi.org/10.1001/jamapsychiatry.2019.0842.
14. Owens, E.W., Behun, R.J., Manning, J.C., Reid, R.C.: The Impact of Internet Pornography on Adolescents: A Review of the Research, (2012). https://doi.org/10.1080/10720162.2012.660431.
15. Perse, E.M., Lambe, J.: Media Effects and Society. Routledge (2016). https://doi.org/10.4324/9780203854693.
16. Holland, G., Tiggemann, M.: A systematic review of the impact of the use of social networking sites on body image and disordered eating outcomes, (2016). https://doi.org/10.1016/j.bodyim.2016.02.008.

17. Slater, A., Halliwell, E., Jarman, H., Gaskin, E.: More than Just Child's Play?: An Experimental Investigation of the Impact of an Appearance-Focused Internet Game on Body Image and Career Aspirations of Young Girls. J. Youth Adolesc. 46, 2047–2059 (2017). https://doi.org/10.1007/s10964-017-0659-7.
18. Livingstone, S., Smith, P.K.: Annual Research Review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age. J. Child Psychol. Psychiatry. 55, 635–654 (2014). https://doi.org/10.1111/jcpp.12197.
19. Goldsmith, A., Wall, D.S.: The seductions of cybercrime: Adolescence and the thrills of digital transgression. Eur. J. Criminol. 147737081988730 (2019). https://doi.org/10.1177/1477370819887305.
20. Montgomery, K.C., Chester, J., Milosevic, T.: Children's privacy in the big data era: Research opportunities. Pediatrics. 140, S117–S121 (2017). https://doi.org/10.1542/peds.2016-1758O.
21. Meyer, M., Adkins, V., Yuan, N., Weeks, H.M., Chang, Y.-J., Radesky, J.: Advertising in Young Children's Apps: A Content Analysis. J. Dev. Behav. Pediatr. 40, (2019).
22. Mathur, A., Acar, G., Friedman, M.J., Lucherini, E., Mayer, J., Chetty, M., Narayanan, A.: Dark patterns at scale: Findings from a crawl of 11K shopping websites, (2019). https://doi.org/10.1145/3359183.
23. Gray, C.M., Kou, Y., Battles, B., Hoggatt, J., Toombs, A.L.: The Dark (Patterns) Side of UX Design. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. pp. 534:1--534:14. ACM, New York, NY, USA (2018). https://doi.org/10.1145/3173574.3174108.
24. Zagal, J.P., Björk, S., Lewis, C.: Dark patterns in the design of games, http://dblp.uni-trier.de/db/conf/fdg/fdg2013.html#ZagalB013, (2013).
25. Brignull, H.: Dark Patterns: inside the interfaces designed to trick you, https://www.theverge.com/2013/8/29/4640308/dark-patterns-insidethe-interfaces-designed-to-trick-you.
26. Alexander, C., Ishikawa, S., Silverstein, M.: A Pattern Language: Towns, Buildings, Construction. Oxford University Press, New York (1977).
27. Brignull, H.: Types of Dark Pattern, https://darkpatterns.org/types-of-dark-pattern, last accessed 2019/03/25.
28. Apple: App Store Review Guidelines, https://developer.apple.com/app-store/review/guidelines/, last accessed 2021/06/11.
29. Google Play: Ads | Monetization and Ads - Developer Policy Center, https://play.google.com/about/monetization-ads/ads/, last accessed 2020/01/25.
30. Google Play: Families - Developer Policy Center, https://play.google.com/about/families/, last accessed 2020/01/25.
31. ICO: Age appropriate design: a code of practice for online services. (2020).
32. Petersen, F.W., Thomsen, L.E., Mirza-Babaei, P., Drachen, A.: Evaluating the onboarding phase of free-to-play mobile games: A mixed-method approach. In: CHI PLAY 2017 - Proceedings of the Annual Symposium on Computer-Human Interaction in Play. pp. 377–388. Association for Computing Machinery, Inc (2017). https://doi.org/10.1145/3116595.3125499.