(Hrsg.): Privacy and Security at Large Workshop within the GI Informatik 2022,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023 11

Deceptive patterns in consent dialogs on children's websites

Suvi Lehtosalo[1] and Daniel W. Woods[2]

Abstract: Many privacy and data protection laws, such as Article 8 GDPR and the CCPA, establish different requirements when establishing a legal basis for collecting personal data about children. Our study asks whether and how children's websites collect consent. We conduct an automated analysis of 2,066 educational and gaming websites, and a manual analysis of 13 large sites. We measure the prevalence of deceptive patterns identified in prior work, plus a new design consideration, whether the dialog is addressed to the child user's parent or guardian. A small minority of websites address dialogs for children, which suggest the majority of children's websites in our sample may not comply with Article 8 GDPR.

Keywords: Online consent, Data protection, Internet measurement, Child protection

1 Introduction

Under the paradigm of privacy self-management [So12], users are responsible for defining what websites can do with their personal data. Empirical studies demonstrate the challenges in doing so in a meaningful way. One barrier is the decision volume resulting from users browser multiple websites with diverse and complex privacy policies [MC08, BP10, So12]. Even when the user has made a decision, dialogs can be designed to make opting-out difficult [MBS20, No20]. Dialogs frequently contain *deceptive patterns*, which are design choices intended to influence users' decisions; for example, the opt-in option may be highlighted, and the opt-out option hidden behind a 'More Options' button.

Discussions around online consent implicitly assume users are adults with functioning cognitive abilities. Yet, child users have a limited understanding of data collection and privacy risks [Su21]. This view is echoed by debates related to whether child patients can provide medical consent [Sh73].

Such considerations motivated policymakers to create different online consent requirements for children. The General Data Protection Regulation (GDPR) in the EU requires that consent is "given or authorised by the holder of parental responsibility over the child", whereas consent is given by the data subject if they are an adult [MK17]. The difference is even starker under the California Consumer Privacy Act (CCPA), which creates an opt-out

[1] University of Edinburgh, School of Informatics, 10 Crichton St, Edinburgh, EH8 9AB, UK
[2] University of Edinburgh, School of Informatics, 10 Crichton St, Edinburgh, EH8 9AB, UK. Contact email: daniel.woods@ed.ac.uk

consent regime for adults but an opt-in regime for children (Under 16s), which must be obtained from a parent or guardian if the child is under 13 [AE22].

This raises the question of how children's websites collect opt-in consent. Our paper answers:

RQ1 How does the prevalence of dark patterns in consent dialogs vary across adult and children's websites?

RQ2 How does the prevalence of dark patterns in consent dialogs vary across the adult and children's sections of a single website?

RQ3 Who are consent dialogs on children's websites addressed to?

To answer *RQ1*, we sample adult and children's websites from search engines. Dark patterns in this sample are detected by applying a system developed in prior work [KVW23]. To answer *RQ2* and *RQ3*, we craft a sample of popular websites that have a website section specifically for children. We then run both the automated and manual analysis on these websites, comparing the consent dialogs on the adult and children's sections.

Our automated analysis shows that adult and children's websites are similarly likely to display a consent dialog. Further, there is no major difference in the prevalence of dark patterns. Just 7% of dialogs on children's games websites asked for consent from the user's parent or guardian. Our manual analysis of 13 major websites revealed that 5 websites collect consent and personal data in a different way on the children's section of the website, such as displaying a different consent dialog or not setting ID-like cookies on the children's section.

We introduce the necessary background to this study in Section 2. This motivates and guides our methodology, which is described in Section 3. We present our results in Section 4. We reflect on the study in Section 5, and offer a conclusion in Section 6.

2 Background

Legal Online consent has been voluntarily collected since the 1990s when browsers requested user permission before installing cookies [MFF01]. This became a legal requirement in the EU in 2009, as the reformed ePrivacy Directive required websites to obtain consent before "storing or accessing cookies on a device" [Bo13]. The 2016 General Data Protection Regulation further expanded the role of online consent by allowing it to serve as a legal basis for data processing (beyond simply installing cookies). The role of online consent in US privacy law is harder to summarize because the law is fractured across states, agencies and standalone federal laws. To avoid these discrepancies, we primarily focus on studies in the GDPR context.

The GDPR placed particular restrictions on the processing of children's data, recognising that children may be less aware of risks and as such require special protection. Most notably,

children below the age of 16 cannot consent to data processing, though this age threshold can be replaced by a national threshold for children between 13 and 16 [MK17] if the member state decides to do so.

Human Computer Interface Design choices, such as hiding the opt-out behind a 'More Options' button, have been repeatedly shown to influence the users' consent decisions [KPW21]. These designs are known as *deceptive patterns* because they undermine the user's autonomy, and may be non-compliant with European law [SBM20]; as such, it is relevant for us to look at dark patterns as a quantifiable measure of the level of compliance when comparing consent dialogs addressed to children and adults.

Scraping Studies Studies of consent interfaces found on real-world websites were surveyed by Kretschmer et al. [KPW21]. Most studies sample websites from a list of the most popular websites (e.g. Tranco [Po21]) [KPW21]. We are aware of three studies that extract arbitrary dialogs [Ei19, KS21, KVW23]. We use the *DarkDialogs* system, which correctly extracted 99% of dialogs in a hand-labelled sample [KVW23].

Children and Online Tracking Prior work has found that tracking is pervasive on children's websites. A sample of 20 children's websites all contained invisible tracking images [Vl18]. Similarly, children's websites were observed to have the second-highest percentage of websites that perform at least some kind of tracking [Sa19]. Tracking is also prevalent in children's apps [Zh20, Bi18]. Our contribution is the first study focused on consent dialogs on children's websites.

3 Methodology

3.1 Sample of Websites

Automated We need a sample of websites that differ only in whether the users were children or adults. We cannot simply sample from children's websites and compare that to a sample of adult websites. The adult sample would include websites with no children's equivalent, such as financial services or tax advice. This would complicate statistical analysis because consent interfaces vary considerably across website category (see Fig. 4 [HWB21]).

We instead sample from categories for which both adult and children's websites exist, namely games and education websites. We collected these using a search engine, following previous studies of children's websites [Ca03, CZ13, NKA21]. We automatically extracted the results from the search terms: "online games" (GameGen), "online games for kids" (GameKid), "online games for adults" (GameAdult), and equivalently "educational website" (EdGen), "educational website for kids" (EdKid) and "educational website for adults" (EdAdult). This resulted in a sample of 2,066 websites after removing any Google Books results and sites that occurred multiple times under the same search term. Figure 1 shows the number of websites that occur under multiple search terms, which we chose not to remove from the analysis.

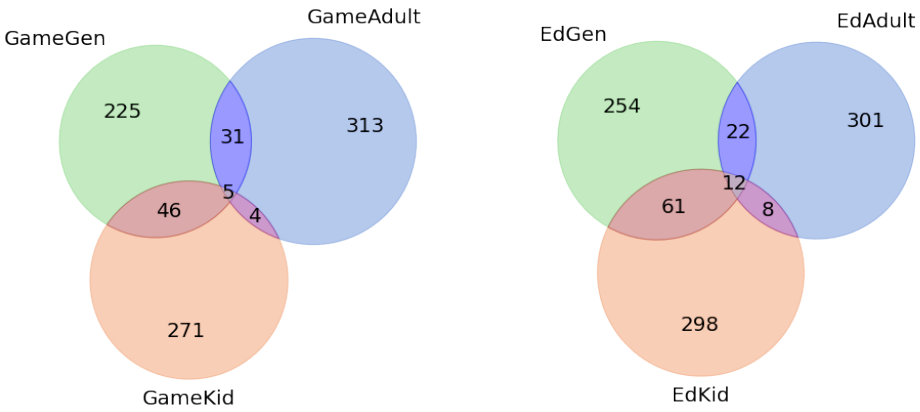


Fig. 1: A minority of websites were sampled under multiple categories.

Manual We collected a sample of 13 websites that had a specific children's section, in addition to the website's generic homepage (see Table 1 for the full sample). The pairs of websites were found based on the author's knowledge, as well as searching "children's websites" and "websites for kids". The websites were accessed on (March 24th 2023) through Google Chrome with the most permissive privacy settings. All previous cookies were deleted before accessing each website.

3.2 Analysis

Automated We used an open-source tool, DarkDialogs, to automatically extract dialogs and detect dark patterns [KVW23]. DarkDialogs detects 10 different dark patterns (*DP1–10*) [KVW23]. We also introduce a new dark pattern that is specific to children's websites:

> *DP11: ConsentFromKids* A cookie dialog on a website aimed for children or for a general audience asks for consent from the user, without specifying that children should have their guardians read and respond to the dialog.

This was implemented by searching for and then manually checking extracted dialogs that contain the words parent/guardian/adult.

We conducted additional evaluation to ensure the system's performance had not degraded over time on websites sampled from Tranco and Google. In terms of dialog extraction, the system correctly extracted a dialog in 93.5% of cases (compared to 98.7% in the original paper [KVW23]). In terms of dark pattern detection, we removed the *ObstructsWindow* dark pattern because of the high false positive rate (40%). After removing this, the system

	Websites		Dialogs		Children's dialogs	
	Total	Loaded	n	% of sites	n	% of dialogs
EdAdult	344	343	215	62.7	1	0.5
EdGen	351	349	232	66.5	0	0
EdKid	381	379	200	52.8	1	0.5
GameAdult	354	353	174	49.3	0	0
GameGen	309	307	199	64.8	8	4.0
GameKid	327	326	180	55.2	12	6.7
Total	2,066	2,057	1,200	58.3	22	1.8

Tab. 1: The majority of education and gaming websites contain consent dialogs. Dialogs that reference the user's parent or guardian are rare, especially among children's educational websites.

had a False Positive rate of 2.45% and a False Negative rate of 7.35%. This highlights how quickly the performance of web measurement systems deteriorate over time.

Manual Each cookie dialog was manually checked for each of the 10 Dark Patterns. We checked whether dialogs on children's websites appeared more child-friendly (using simplified language, a larger font, or bright colours), and whether they asked for consent from a parent. Any other significant difference was also noted. Cookies set after clicking each option were collected via Chrome's Developer tools.

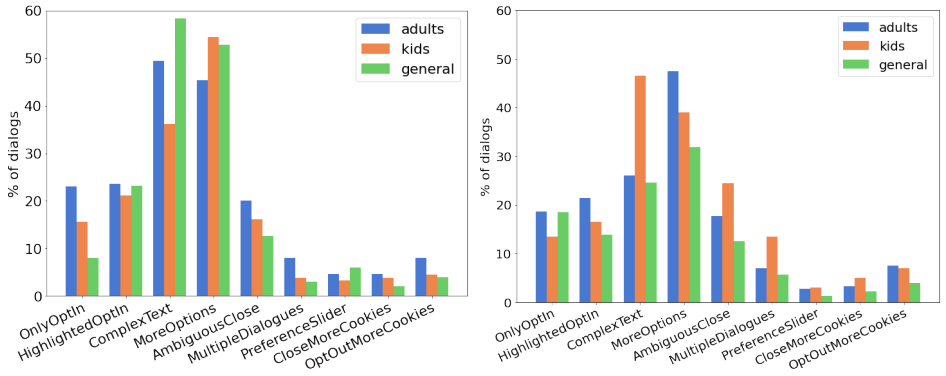
4 Results

4.1 Automated Analysis

We ran the DarkDialogs on 2,066 websites in March 2023. Table 1 shows that 2,057 of these websites successfully loaded. The majority (58%) of websites in our sample had a consent dialog, with the highest prevalence among general gaming and education websites. We use the term *children's dialog*, which corresponds to *DP11*, to denote dialogs specifying that children should ask their guardians to respond to the dialog. Table 1 shows that less than 2% of dialogs are children's dialogs. They are most prevalent on children's gaming websites, although this is still just 7% of websites. Only two educational websites contained a children's dialog.

The tool, DarkDialogs [KVW23], detects additional dark patterns, which are displayed in Figure 2b. We could not identify any generic statements like 'dialogs on children's websites contain fewer dark patterns' because this varied by the type of website. For example, children's gaming websites had a lower prevalence of *ComplexText* than general and adult gaming websites. However, this trend is reversed for education websites.

Dialogs on adult gaming websites display a higher prevalence of each dark pattern than dialogs on children's gaming websites, with the exception of *MoreOptions*. The comparison



(a) Gaming websites.

(b) Educational websites.

Fig. 2: Occurrence of different DPs in the found cookie dialogs.

	Mean	Median	Std deviation	Max	Min
GameGen	14.22	3.0	31.74	179	0
GameAdult	31.35	10.5	48.56	205	0
GameKid	12.26	4.0	23.12	138	0
EdGen	7.49	2.0	18.06	155	0
EdAdult	7.57	4.0	16.94	189	0
EdKid	10.07	5.0	17.42	110	0

Tab. 2: Third-party cookies set after opting in.

to general gaming websites is more variable. We could not identify any comparable trend among education websites.

Differences can be seen in the number of cookies set by websites in each sample. Table 2 shows the statistics of third-party cookies set after the opt-in option was selected. Children's gaming sites set less than half as many third-party cookies as adult's gaming websites. This is reversed for educational websites, in which children's educational websites set more cookies than both general and adult educational websites.

4.2 Manual Analysis

We identified 13 websites with separate children's subsites. Three had no cookie dialog on either website, and a further five had exactly the same cookie dialog on both sites. Notably, Table 3 shows the Ted and Time websites set fewer ID-like cookies (defined as cookies whose value is unique enough to be used as an identifier) on the children's website, possibly because they do not track these users. We were left with five websites that display different cookie dialogs in each section:

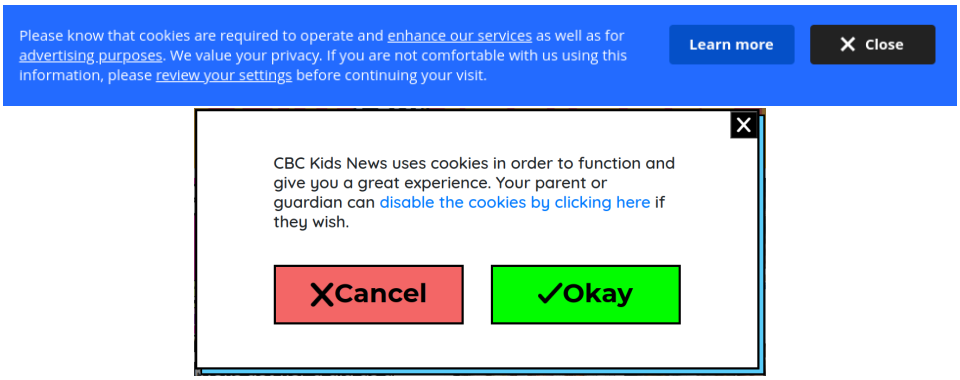


Fig. 3: Contrasting the cookie dialogs on *cbc.ca* and *cbc.ca/kidsnews*, we see that the former is specifically designed for children.

The website *Nationalgeographic.co.uk* has a one-click opt-out, whereas the dialog on the children's page *natgeokids.com/uk* only has a *MoreOptions* button with no 1-click opt-out. The children's page also asks whether the user is a teacher, kid or parent. It then displays the same dialog regardless of which option is chosen, whereas it should prompt the child to ask a parent or guardian to provide consent if 'Kid' is selected. However, Table 3 shows the children's website sets only one ID-like cookie, regardless of the consent decision. It could be that the website does not use this to track users browsing the children's site.

The website *Youtube.com* has a cookie dialog, whereas *Youtubekids.com* does not. Further, the children's site requires users to allow third-party cookies. When it is accessed with third-party cookies blocked, a warning is displayed and the user is not allowed to sign in.

Comparing the dialogs on a Canadian news website (*cbc.ca* to *cbc.ca/kidsnews*), the dialog on the children's website is simplified with a large font and bright colours. It also contains a reference to the child's guardians, but not in the expected way. Rather than request for the child's guardian to *consent* to cookies, they instead say the guardian can "disable the cookies ... if they wish"(shown in Figure 3). The other dialogs contains dark patterns like having no 1-click opt-out.

The children's website *dkfindout.com/uk* has two dialogs: the first one has opt-in and reject options, as well as an ambiguous close button and a "More options"button. After the first dialog has been closed, another one behind it becomes visible. This dialog states that by continuing to browse the site, the user is agreeing to its use of cookies; only a close option and a link to the cookie policy are provided. The recorded number of cookies set (see Table 3) further indicates that the first dialog actually has no impact on the number of cookies set. The general website dk.com/uk only has one cookie dialog, which is similar to the second dialog on the children's website, giving the user no option besides opting in.

Out of the two Guinness world records websites, only the children's section has a cookie

Website	Initial	Opt-in	Opt-out	Close
bbc.co.uk	2	2	2	
bbc.co.uk/cbeebies	3	3	2	
cbc.ca	8			11
cbc.ca/kidsnews	12	12	12	11
cia.gov and cia.gov/spykids	0			
nasa.gov and nasa.gov/kidsclub	0			
dk.com/uk	1	1		
dkfindout.com/uk	2	2	2	
guinnessworldrecords.com	7			
kids.guinnessworldrecords.com	0	0		
nationalgeographic.co.uk	0	10	1	
natgeokids.com/uk	1	1	1	
pbs.org and pbskids.org	2			
tate.org.uk and tate.org.uk/kids	0	11	0	
ted.com	9			9
ed.ted.com	4			5
time.com	7	35	18	
timeforkids.com	3	4	3	
vogue.com	6	37	7	
teenvogue.com	4	46	5	
youtube.com	0	2	1	
youtubekids.com	1			

Tab. 3: The children's website set fewer ID-like cookies for Guinness World Records, National Geographic, Ted, and Time. There is no obvious difference for the other websites.

dialog, which only contains an opt-in button. This is likely because they do not track users browsing the children's site. Table 3 shows that the children's site sets no ID-like cookies.

5 Discussion

We discuss whether these websites are compliant, potential alternative solutions, and the limitations of our study.

Compliance Evaluating website compliance would be simpler if websites could be reliably divided into those websites used by children and those used by adults, and then further divided by jurisdiction. In such a world, children's websites in the EU are non-compliant

with Article 8 of the GDPR if the dialog requests consent from a child user, and not the child's parent or guardian. In reality, most websites are used by both adult and children from a mixture of jurisdictions, which makes it unclear which standard to apply. This motivates two approaches to deciding whether to display an adult or children's dialog.

The most technically difficult approach is to infer the user's age and to present a children's dialog to children. This is analogous to how websites present cookie dialogs based on the user's jurisdiction, such as not showing GDPR-compliant dialogs to users from the US [Ei19, HWB20]. Another approach is to use the observed or intended demographics of users to choose a dialog that applies to all users. This leads to an arbitrary threshold for when a children's dialog should be offered—should a website for which 5% of the users are children? How about 50%?

These differences in potential approaches are why we lack confidence in declaring individual sites as non-compliant. Some websites targeted at adults or with majority adult user bases may have been erroneously included in our search term "online games for kids". It is also possible (although unlikely given the technical challenge) that some websites accurately inferred that all researchers in this study were adults, and hence the website did not display a children's dialog. Nevertheless, it seems reasonable to conclude that the low prevalence of children's dialogs (0.5%/7% respectively of dialogs on children's educational/gaming websites) suggests multiple websites do not comply with Article 8 of the GDPR, given that we accessed these websites from a UK IP address,

Solutions We can either discuss solutions within the current legal paradigm or discuss solutions to the underlying problem. In terms of complying with the current legal regime, we recommend against trying to infer a user's age because doing so likely necessitates collecting additional data about users—this would erode the user's privacy before they are offered a chance to consent. Offering the same dialog to all users avoids this privacy erosion. Websites with a significant share of child users should adapt consent dialogs to address Article 8. Even in such cases, Article 8 also requires the controller to "make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child". It remains unclear what this involves. Given compliance with Article 8 is still ambiguous and that many US states are introducing privacy laws, it may be wiser to simply stop collecting data from users who are most likely children. This is presumably the choice Guinness World Records made given they set no ID like cookies on the children's section of their website.

In terms of the actual problem—that users lack of control over their privacy, and child users have even less awareness of privacy issues [Su21]—it is unclear that consent dialogs help users. The notice and consent approach to privacy law imposes a large decision burden on users [So12]. A parent or guardian interrupting household tasks to respond to a consent dialog on behalf of their child would waste even more time.

One alternative is for users to make a decision that applies to all websites, which would be

automatically communicated by a browser. The Global Privacy Control (GPC) is one such signal [ZA20, HWB21, Zi23], which represents an opt-out of data processing when turned on. Allowing parents and guardians to set the GPC on the device used by their children preserves both parental responsibility and time. However, websites have little incentive to adopt the GPC unless it is effectively enforced; few websites currently respect GPC signals [Zi23]. Further regulation and enforcement is therefore needed before the GPC can be relied on.

Limitations Measuring the Web is hard because the content served changes over time and across vantage points. For example, all of our measurements were made from the UK, which likely impacted which dialog was shown [Ei19]. This issue will become more important when measuring from the US given that privacy laws vary by state. We also discovered that the performance of the automated system that we used degraded since it was designed one year ago [KVW23]. Maintaining open-source web measurement systems remains a challenge for this reason.

It was also challenging to collect a sample of children's websites. Our manual analysis allowed us to find the children's section of large websites, which are undeniably targeted to children. This was more difficult when it came to finding children's websites, given website classifications often contain errors [Va20]. We used Google's search results as a pragmatic solution, which is vulnerable to biases resulting from how Google prioritises websites.

There is no existing research on how children perceive and are affected by dark patterns. This study did not include child participants, so the methods were validated solely from an adult perspective. Future work could include children in the process of assessing dialogs and designing more child-friendly alternatives.

6 Conclusion

Our measurement study asked whether and how children's websites collect consent for data processing from users. Our sample of educational and gaming websites revealed that children's websites were just as likely to collect consent from users. Around 7% of the dialogs on children's gaming websites were addressed to the user's parent or guardian. Children's websites displaying dialogs that are not designed for children may be violating Article 8 of the GDPR, although we are not aware of a legal judgement. Prior work showed non-compliance with other design patterns [No20, MBS20, KPW21].

Bibliography

[AE22] Alomar, N.; Egelman, S.: Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps. Proceedings on Privacy Enhancing Technologies, 4(2022):24, 2022.

[Bi18] Binns, R.; Lyngs, U.; Van Kleek, M.; Zhao, J.; Libert, T.; Shadbolt, N.: Third Party Tracking in the Mobile Ecosystem. In: Proceedings of the 10th ACM Conference on Web Science. WebSci '18, Association for Computing Machinery, New York, NY, USA, p. 23–31, 2018.

[Bo13] Borgesius, F. Z.: Behavioral targeting: A European legal perspective. IEEE Security & Privacy, 11(1):82–85, 2013.

[BP10] Bonneau, J.; Preibusch, S.: The privacy jungle: On the market for data protection in social networks. In: Economics of Info. Sec. and Privacy, pp. 121–167. Springer, 2010.

[Ca03] Cai, X.; Gantz, W.; Schwartz, N.; Wang, X.: Children's website adherence to the FTC's online privacy protection rule. Journal of Applied Communication Research, 31(4):346–362, 2003.

[CZ13] Cai, X.; Zhao, X.: Online advertising on popular children's websites: Structural features and privacy issues. Comp. in Human Behavior, 29(4):1510–1518, 2013.

[Ei19] van Eijk, R.; Asghari, H.; Winter, P.; Narayanan, A.: The impact of user location on cookie notices (inside and outside of the European union). In: Workshop on Technology and Consumer Protection (ConPro'19). 2019.

[HWB20] Hils, M.; Woods, D. W.; Böhme, R.: Measuring the emergence of consent management on the web. In: Proc. of the ACM Internet Measur. Conf. pp. 317–332, 2020.

[HWB21] Hils, M.; Woods, D. W.; Böhme, R.: Privacy preference signals: Past, present and future. Proc. on Privacy Enhancing Technologies, 2021(4):249–269, 2021.

[KPW21] Kretschmer, M.; Pennekamp, J.; Wehrle, K.: Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. ACM Trans. on the Web, 15(4):1–42, 2021.

[KS21] Kampanos, G.; Shahandashti, S. F.: Accept all: The landscape of cookie banners in Greece and the UK. In: IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, pp. 213–227, 2021.

[KVW23] Kirkman, D.; Vaniea, K.; Woods, D. W.: DarkDialogs: Automated detection of 10 dark patterns on cookie dialogs. In: 8th IEEE European Symposium on Security and Privacy. IEEE, 2023.

[MBS20] Matte, C.; Bielova, N.; Santos, C.: Do cookie banners respect my choice?: Measuring legal compliance of banners from iab europe's transparency and consent framework. In: 2020 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 791–809, 2020.

[MC08] McDonald, A.; Cranor, L. F.: The cost of reading privacy policies. Journal of Law and Policy for the Information Society, 4:543, 2008.

[MFF01] Millett, L. I.; Friedman, B.; Felten, E.: Cookies and web browser design: Toward realizing informed consent online. In: In Proceedings of the 2001 CHI Conference on Human Factors in Computing Systems. pp. 46–52, 2001.

[MK17] Macenaite, M.; Kosta, E.: Consent for processing children's personal data in the EU: following in US footsteps? Information & Communications Technology Law, 26(2):146–197, 2017.

[NKA21] Norouzi, Y.; Keshavarz, H.; Athar, Z.: Evaluating children's websites from an information visualization perspective: findings of a comparative mixed-methods study. The Electronic Library, ahead-of-print, 11 2021.

[No20] Nouwens, M.; Liccardi, I.; Veale, M.; Karger, D.; Kagal, L.: Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In: In Proc. of Human Factors in Computing Systems (pp. 1-14). pp. 1–13, 2020.

[Po21] Pochat, V. L.; Van Goethem, T.; Tajalizadehkhoob, S.; Korczyński, M.; Joosen, W.: , Tranco A Research-Oriented Top Sites Ranking Hardened Against Manipulation. https://tranco-list.eu/, 2021. Last accessed 19 October 2021.

[Sa19] Sanchez-Rola, I.; Dell'Amico, M.; Kotzias, P.; Balzarotti, D.; Bilge, L.; Vervier, P.; Santos, I.: Can i opt out yet? GDPR and the global illusion of cookie control. In: Proc. of the ACM Asia Conf. on Comp. and Comm. Sec. pp. 340–351, 2019.

[SBM20] Santos, C.; Bielova, N.; Matte, C.: Are cookie banners indeed compliant with the law? https://arxiv.org/pdf/1912.07144.pdf, 2020. Last accessed 27 August 2023.

[Sh73] Shaw, A.: Dilemmas of "informed consent" in children. The New England Journal of Medicine, 1973.

[So12] Solove, D.: Introduction: Privacy self-management and the consent dilemma. Harv. L. Rev., 126:1880, 2012.

[Su21] Sun, K.; Sugatan, C.; Afnan, T.; Simon, H.; Gelman, S. A.; Radesky, J.; Schaub, F.: "They See You're a Girl If You Pick a Pink Robot with a Skirt": A Qualitative Study of How Children Conceptualize Data Processing and Digital Privacy Risks. In: Proc. of the CHI Conference on Human Factors in Computing Systems. 2021.

[Va20] Vallina, P.; Le Pochat, V.; Feal, Á.; Paraschiv, M.; Gamba, J.; Burke, T.; Hohlfeld, O.; Tapiador, J.; Vallina-Rodriguez, N.: Mis-Shapes, Mistakes, Misfits: An Analysis of Domain Classification Services. In: Proc. of the ACM Internet Measurement Conference. IMC '20, p. 598–618, 2020.

[Vl18] Vlajic, N.; El Masri, M.; Riva, G. M.; Barry, M.; Doran, D.: Online Tracking of Kids and Teens by Means of Invisible Images: COPPA vs. GDPR. In: Proceedings of the 2nd International Workshop on Multimedia Privacy and Security. MPS '18, Association for Computing Machinery, New York, NY, USA, p. 96–103, 2018.

[ZA20] Zimmeck, S.; Alicki, K.: Standardizing and implementing Do Not Sell. In: Proceedings of the 19th Workshop on Privacy in the Electronic Society. pp. 15–20, 2020.

[Zh20] Zhao, F.; Egelman, S.; Weeks, H. M.; Kaciroti, N. A; Miller, A. L.; Radesky, J. S.: Data Collection Practices of Mobile Applications Played by Preschool-Aged Children. JAMA pediatrics, p. e203345, 2020.

[Zi23] Zimmeck, S.; Wang, O.; Alicki, K.; Wang, J.; Eng, S.: Usability and Enforceability of Global Privacy Control. PETS, 2:1–17, 2023.