DATAETHICS

THE CHILD DATA VIOLATORS

The thinkdotank DataEthics.eu has analyzed 14 digital services aimed at or used by children.

Following services are encompassed:

- LEGO
- EduLab
- Momio
- musical.ly
- Facebook
- Instagram
- Steam
- Youtube
- SnapChat
- DR Ramasjang/Ultra
- MyMonii
- Google G Suite Classroom
- Microsoft Education
- Disney

We have looked at what the services are communicating about their practises on their websites. We have had direct contact with a few of them, and we have researched and tried some of them out on our own.

This report should not be seen as a rubber stamp on which services are okay and which are not, but as an attempt to spark true transparency and help children, parents and teachers when they decide what to use and not to use regarding personal data (ab)use.

Pernille Tranberg & Mie Oehlenschlæger, March 2018

Analysis - The Child Data Violators - April 2018

DATAETHICS

Following criteria has been used:

Good data ethics practises:
- No sale or sharing of child data to third parties (e.g. via third party cookies).
- Human moderation of content before it is served to children.
- Parent consent management.
- Non-manipulative behavioral design.

Bad data ethics practises:
- Direct sale or sharing of child data to third parties, e.g. via third party cookies.
- No parent consent management.
- Insufficient or misleading communication.
- Manipulative behavioral design.

In the research it quickly became clear that LEGO and Edulab fully protect childrens' data. Therefore they becan role models for the benchmarking of all the other services, and as they are very similar we describe them together and before everyone else.

Edulab & LEGO (dk)

They don't sell data to or share data with third parties, they have no third-party cookies on websites, that children frequently visit, they don't use Facebook Connect or other SoMe-plugins which also includes data sharing. NO profiling of kids. Both have parents consent management tools and take responsibility for their sub-contractors w data processing agreements. Data is stored in Europe.
LEGO does not use Google Analytics (which is 'free', because you pay with your customer data control). Edulab is practising data minimilazation (e.g. tries to avoid getting social security numbers from the Ministry of Education, as they don't need them, and in a Facebook-retargeting experiment they make sure that no one under 21 years will get their ads. LEGO humanly moderates all content and got this headline in Wired last year: 'How LEGO built a Social Network for Kids That is Not Creepy. LEGO also recommends kids to use pseudonyms. And both of them have guidelines against manipulative design.

Momio (dk)

÷ Everyone can log on and pretend to be a child. No parents consent system - only a call for the kids to read the terms of conditions together with a parent. Very manipulative behavioral design with constant calls for participation in competitions or buying virtual stuff (and probably also illegal use of pre-ticket boxes to receive advertising). Use of cookies, unless you pay to get it ad free and only partly human moderation.
+ New consent rules management due to arrive in May with GDPR. Short and easy but not complete communication. Apart from partly human moderation they have automatic check of violating content.

Musical.ly (chinese)

÷ Their rules dictate that you need to be 13 to use it, but they do nothing to check the age. It is irresponsible, as they must know that many many kids are using the service and thus they treat kids' data as if they were grown-ups. They demand that you use your own name and real data with a real name policy just like Facebook's. They use cookies and everything is tracking by-default, including location. Also manipulative behavioral design with a gift point program and own currency. No moderation at all though it seems that they are starting to change that after this story: Porn is not The Worst Thing on musical.ly.
+ It is possible to get a 'privat' profile where data is processed on your gadget, and they do have good community guidelines.

Facebook & Instagram (us)

÷ Their rules dictate that you need to be 13 to use it, but they do nothing to check the age. It is irresponsible, as they must know that many many kids are using the service and thus they treat kids' data as if they were grown-ups. Use cookies and everything is tracking by-default, including location. Also manipulative behavioral design. Mainly moderation by flagging from users - and their own automatic systems.
+ You can download your data and see, how much you give away. Generally good communication despite a long privacy policy. Impossible to check that they do what they say. They launched a Facebook for Kids in late 2017, which according to many parents are not a good idea, because kids should not be on SoMe.

Steam (us)

÷ Their rules dictate you need to be 13 to use it, but they do nothing to check the age. It is irresponsible, as they must know that many many kids are using the service and thus they treat kids' data as if they were grown-ups. Their games appeal to kids under 13. You are public-by-default and have to actively chose if you want to be 'private'
+ Offers parents control with Steam Family View and appeals to parents to take responsiblity.

YouTube (us) - Google-owned

÷ Their rules dictate that you need to be 13 to use it, but they do nothing to check the age. It is irresponsible, as they must know that many many kids are using the service and thus they treat kids' data as if they were grown-ups and also serve content to the users which is grufully radicalising. Very hard to understand Terms of Conditions wrapped in sweet words that YouTube is doing everything on behalf of the user. Everything is public-by-default and data collections is massive, while manipulative behavioral design is frequent, eg autoplay.
+ After pressure they are moderating a bit more. And they have Youtube for Kids w a good privacy policy.

SnapChat (us)

÷ Their rules dictate that you need to be 13 to use it, but they do nothing to check the age. It is irresponsible, as they must know that many many kids are using the service and thus they treat kids' data as if they were grown-ups. They collect all sorts of data. Everything is tracking by-default- apart from the location-feature SnapMaps which you

have to opt into. Here you see the kids' location in real time in a cute and cool way that must be very hard to say no to as a kid. The map is accessable for everyone though an ordinary browser, where you can see all public snaps. Their design is extraordinarily manipulative with 'streaks' so kids have to babysit each others phones not to be left out of a streak and lose points within 24 hours.
+ They are very open about what they do and write it in an understandable language though their narrative is: We protect you and your privacy' seem to not fit accordingly.

DR Ramasjang & Ultra (dk)

÷ Collect and share data with third parties via cookies on Ramasjang where the target group is 3-6 years and Ultra where the target group is 7-12 years. Ultra has its own Youtube-channel even though you have to be 13 to be on YouTube. Also DR's child MGP program, who targets children under 13, have their own Youtube Channel. At least DR moderates the YouTube-channel according to their own rules.
+ DR has changed for the better re SoMe and data recently. On a subsite at Ramasjang, where there is an Instagram-logo and indirect call for sharing, they say that Instagram is for the parents, but it can be hard to distinguish which pages at Ramasjang are for kids and which are for parents. The websites are without ads, so they constitute good alternatives to the many ad-filled platforms.

MyMonii (dk)

+ No third party cookies, no sale of access to users, not ads and no manipulative behavioral design.

Google Classroom (us)

The core services in G Suite Classroom is Gmail, Kalender, Classroom, contacts, Drive, Docs, Analysis, Groups , Sheets, Slide, Hangouts and Chrome
÷ Their privacy policy is hard to understand. It is not clear what the data, that is collected, is used for and who gets access.
+ Google G Suite contains no ads, and Google says that they are not selling or sharing data with third parties (there are lawsuits in the US claiming the opposite).

Microsoft Education (us)

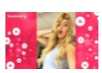
÷ Not possible to find an independent privacy policy for MS Education. Therefore, we assume that the main MS privacy policy is duable. That means MS is using third party cookies and collects data to sell ads.
+ As opposed to Google, MS does not use data from e.g mails, chats, video or text messages or documents to target ads.

Disney (us)

÷ Writes openly that they collect kids' data but it is hard to grasp precisely what they use them for. In the US, Disney is accused of selling kids' data without consent from parents. Disney has different grades of parents consent management, but it is hard to understand what and how you give consent and to what.
+ Disney has good general advise on how to protect one's identity online and advices kids not to give their real name online.






Recommendations

Privacy-by-Default. Services targeted at children or being used by children should always be private-by-default and thereby not public. Basically, it should never be possible to track the user to begin with. In that way it is not up to the children to opt out – almost no one does that – but opt in if they (their parents) are ok with being tracked.

No Profiling. Services aimed at or used by children should never profile their users. That implies: no third party cookies, no Facebook Connect or other SoMe plug ins. It also implies no Google Analytics and, yes, no storing of data that can be identified. Public institutions should be frontrunners and stop all calls for sharing personal data on SoMe that tracks children, and instead develop own platforms to children the way the Danish company LEGO has done it.

No Facebook. Many schools use Facebook as a communications channel between teachers and the children. This should not be the case. Facebook is increasingly unpopular. The Company is accused of illegal data use in Germany, of political manipulation in the wake of the Cambridge Analytica/Facebook scandal, and it is a waste of time building something up on a platform where you don't have the ability to control the use of data and where children are getting off, because their parents and grandparents are there. Public institutions and private companies and organizations should be careful using other SoMe's that have the same business model as Facebook (making money on exploiting personal data).

Digital age of Consent. Children should be able to give consent to their parents if they want to use their pictures from the age of 7 (as in Norway[1]). 13 years is an acceptable age for digital consent; if at the same time the parents are advised not to let their children use social media before the age of 13; and if parents are advised to be actively participating on these platforms together with their children until the age of 15. Services targeted at children under the age of 13 should have consent management software in order to assure that the parents are informed. It is worth noticing that even though many SoMe companies like Snapchat and Steam have an unethical practice where they say that the users should be at least 13, while knowing that they are not, the solution is not to demand a real ID from the children. That would result in children delivering too much real data to these companies.

Digital Identity. Children below the age of 13 are advised to use pseudonyms, when they are online (as both LEGO and German authorities are recommending[2]) if they have to create a profile on a commercial platform. This is both due to physical protection but also to"save" their real name, until they understand how to be a public human being as is the case of SoMe, Also, it is a good idea to install VPN on children'' gadgets.

---

[1] *Guro Skåltveit, Norsk Datatilsyn, interviewet feb 2018*

[2] *Marit Hansen, Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein interviewet feb 2018*

Moderation. All content targeted at children below the age of 13 should be moderated by human beings (eventually in cooperation with machines).

Parents. It is important that parents act as role models and are advised to not share pictures of their children. Children have a right to privacy and they should be able to choose what is public about them.

Other actions that DataEthics recommend being done:

● Describe or translate big tech's Terms of Conditions in an easily understandable way just like the UK Child Commissioner has done regarding SnapChat, Instagram and Youtube.

● Develop a wikipedia-like website with tips, tricks and tools on taking control overr your own data. Inspiration can be found here: dataethics.eu/.

● Establish a digital Ombudsman for Children as they have it in the UK[3] and in Ireand[4] with a specific view on data protection; safe digital environments for children; cyber psychological factors and digital marketing.

● In general: Don't be afraid to make bigger demands about privacy to tech firms and software developers.

[3] *Children Commissioner England interviewet feb 2018*

[4] *Ombudsman for Children's Office i Irland interviewet feb 2018*