PRIVACY CHALLENGES IN CHILDREN'S ONLINE PRESENCE – FROM THE DEVELOPERS' PERSPECTIVE

Csaba Krasznay[1], Judit Rácz-Nagy[2] and László Dóra[3]

DOI: 10.24989/ocg.338.12

Abstract
Parents nowadays are facing with the fact that their children are using apps like TikTok or Instagram, and have the same question as millions of other dads and moms: how can they protect their beloved from the dark side of internet? Most parents are anxious about their kids' online presence, but they don't have the right tools to protect them. Teens feel that they neither can find useful information, nor turn to their parents for advices to protect themselves. There are two options: parental control and educational software. For the first one, there are nearly 140 software for parents. Mostly they offer the same: filtering, banning, spying. These solutions are not just ineffective, because the kids can circumvent the solutions, but usually deepen the issue between the teenagers and their parents. The latter one is too generic, and do not provide hands-on tips. Mongu for Teen is an educational app designed for 9-13-year-old kids and their parents that gives a solution for this problem. In our paper, we highlight the current threats to children's online privacy, the European legislation, that aims to protect them and as a case study, our experiences how a developer should follow this privacy regulation and how effective can be an eduware to improve the privacy awareness of digital families.

1. Introduction

Because of their curiosity, children have been exploring the world from a very young age, not only in the physical world, but also in the virtual world. The now growing Z (born between 1995-2010) and Alpha (2010-) generations [1] have been impacted by several impulses by mass media from infancy through adolescence. Just as every parent teaches his or her child the basic functions and tasks they need to learn – as with precaution when crossing the road – these days, it is essential for parents to provide their children with information when using the Internet.

But this responsibility not solely depends on parents, governments also have serious tasks to express the need of children's safety not only in the physical, but the cyberspace as well. Even the Geneva Declaration of the Rights of the Child of 1924 states in Article 1 that "The child must be given the means requisite for its normal development, both materially and spiritually." and in Article 4 that "The child must be put in a position to earn a livelihood, and must be protected against every form of exploitation." [2] and these principles are serving as a legislative basis for governments for almost a century.

In the digital era, there are countless security problems that juveniles are facing with, but privacy protection is one of the major challenges that needs to be solved by legislators. In the European Union,

[1] National University of Public Service Department of Public Management and Information Technology, H-1083 Budapest, Üllői út 82., krasznay.csaba@uni-nke.hu, www.uni-nke.hu
[2] National University of Public Service Department of Public Management and Information Technology, H-1083 Budapest, Üllői út 82., jucyracznagy@gmail.com, www.uni-nke.hu
[3] Mongu for Teen, H-1037 Budapest, Jutas utca 40/a, dora.laszlo@monguforteen.com, https://monguforteen.com/

the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, better known as General Data Protection Regulation or GDPR regulates this issue. [3] In paragraph (38) of its preamble, it says that "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child." This regulation is both a protective shield for kids and a headache for digital service providers due to the complex technical balance between service quality and compliance requirements on the field of security and privacy.

2. Mongu for Teen Application

In April 2018, two of the authors (László Dóra and Csaba Krasznay), together with a third founder, Veronika Hittner-Horváth, has decided to establish a startup company. Our goal was to educate the growing generation so that they can use digital social services on a secure way and would be able to make responsible decisions in the digital space. All this in such a way that does not impose an additional duty for parents who are not dealing with this issue due to lack of time, intention or experience. We believe that children's desire to explore should not be limited, but a guidance should be given. For this to be accepted, trust must be built, which includes respecting their privacy and producing relevant, accurate, and fun tutorials.

In the application there are two views: one for parents and one for kids. In kids' view, we made them clear what are the threats in social media, what are the potential impacts of their acts, and how they should behave or configure their social application so that they can protect themselves and behave on a responsible way. We apply the technique of gamification in short conversations and show them short videos to let them learn in an exciting way. Once parents connect their accounts with their kid's account, they get relevant information, and tips how to start conversations about social apps used by their children. They can even suspend the usage of the social applications until their kids watch all relevant videos and collect enough points. The application is available from the App Store for iOS devices, Android version will come later.

Parenting experts say the age group which can be influenced the most and who are already using social apps is between 9-13. This is the beginning of the teenage era, which is an important phase of separation from parents and they are our target audience. In that sense, privacy should be mostly protected from the parents from the kids' perspective. For this reason, we consider it important that the parent should not be informed of everything but only the events where he or she needs to intervene (e.g. too much social media consumption). Generally speaking, we're trying to avoid indoctrination or prohibition in our teaching materials. We consider it important for children to understand the consequences of their actions, both for themselves and for others. We assure them that if they wish to avoid certain unwanted events, they will have access to the information they need within the application. Meanwhile, we also consider education as important for parents. In this case, besides the risks, it is also necessary to explain what the application is for and what it is typically used by children.

In the long run, we want to build a complete application that covers all the typical risks a teenager could have with his mobile device: e.g., connecting to an untrusted Wi-Fi network. Further

development of the solution is planned to make the tutorials appear related to a specific event, not just in general. This way, tutorials on free hotspots appear when the child is connected to a free Wi-Fi hotspot. In addition, we are planning to adapt the solutions used in classic parental control features that are required by the parents and follow our philosophy described above.

Today, iOS and Android systems both provide parental controls by default. Because operating system developers are in the best position to customize their platform's services, they are expected to provide the best technical solution. However, in this area, only the easiest-to-operate solutions are built into the platform, and they only provide a good solution for things related to the mobile operating system, not for any community/social/family problems. In addition, platform interoperability is not a goal for any of them, meaning that if the family has both an iPhone and an Android device, these solutions cannot be used in the family with a full feature set.

For these reasons, there are many third-party solutions on the market. Over 100 applications can be found on the internet. Interestingly, however, these solutions basically serve as parental monitoring or they can limit the child. In practice, the education-based approach usually stops at blogging on the websites of some companies, which is hardly reaches the kids. In addition, classical surveillance and/or restraint-based solutions have an increasing impact on parent-child relationships. It is important to mention that in this case the children have an interest to circumvent these systems.

3. Online privacy and security threats

As part of the preparation, we participated several events organized around online children safety. In Hungary, such events are used to held in connection with the International Children's Day in May or occasionally, in elementary and secondary schools. Those events gave us an opportunity to ask the interested parents and their children to fill out a questionnaire and highlight their major problems using digital services. We also ran some direct Facebook campaigns in order to get a feedback on our concept from the parents of our relevant target audience. Although these answers are not representative, we could use the representative research of Psyma Hungary Kft. that was made for the Hungarian National Media and Infocommunications Authority in 2017. [4] Our research can finetune and update the study's results that measured media usage, media consumption and media understanding of 7-16 years old children and their parents.

According to the Psyma research, 48% of the 9-10 years old have their own mobile phone, this number changes to 87% in the age group of 13-14 years old kids. They are 10.17 years old as an average when they get their first own device. 88% of the first devices are smart phones. 69% of the parents in our target audience are using some rules and controls on internet usage. Only 46% of the parents who are using some controls, discuss the acceptable usage and threats before the young one starts using the internet. This is the fourth countermeasure only. Most of them ask what the children is doing, when they see the teenager next to the device. 74% of the adults are aware with the existence of content filtering, but 53% don't use any technical countermeasures as they trust in their children and 45% discuss these issues personally. 84% of the parents of our target audience agrees that his son or daughter uses the digital service on a secure way.

The most common activities on the internet are browsing, listening to music, instant messaging, watching videos, learning and playing. 42% of the 11-12 years old age group and 71% of 13-14 years old age group are registered to a social media service. The first registration is made when they are 11.57 years old as an average. According to this study from 2017, 99% are using Facebook, 63% are

using YouTube, 39% are using Instagram. 75% of the families are registered on the same social media service. 7% of 11-12 years old and 9% of 13-14% suffered from cyberbullying.

The main information sources for the youngsters are the parents (82%), the school (80%) and the friends (51%). The study had 8 basic questions, e.g. what a secure password is. Even the most educated parents and their kids could answer for these relatively easy questions only with a 41% success rate. The average was around 35% in our target audience. In the lower educated families, the children's competence was much higher (47% gained better results than their parents).

Our user research confirms the representative study, but also highlights an interesting anomaly in the perception of parents on children's digital existence and the way how kids are really using their devices. Besides the repetition of Psyma's study, we also asked the participants about their major concerns on the internet and the applications the kids are using. We got totally different answers from the adults and the teenagers. Meanwhile the parents have a fear on harmful content, addiction and over usage, their children don't really care about these risks, but are worried about phishing that is equal to the loss of their user account on social media and cyberbullying, that mostly happens through the social media services they are using.

The other question tried to discover the applications youngsters are using. For the experts, it is not surprising, that Facebook is no longer used by teenagers, as they turned to Instagram and TikTok and will use different, maybe yet unknown services in the near future. For the teenagers, it is not important, what they use, but how they use is it. They want to be connected and live their social life 7/24/365. But the parents can't follow these changes and they still believe that their beloved is playing games and using Facebook. Our experience is that most of the parents have never heard about TikTok which has around half billion users nowadays and is operated from China that raises several cybersecurity and privacy questions.

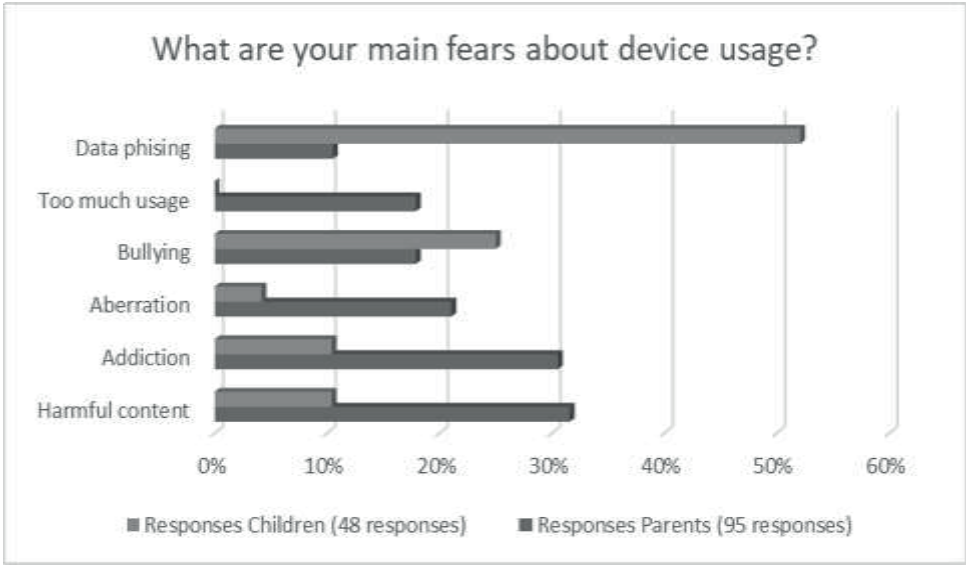

Figure 1: What are the main concerns about device usage?

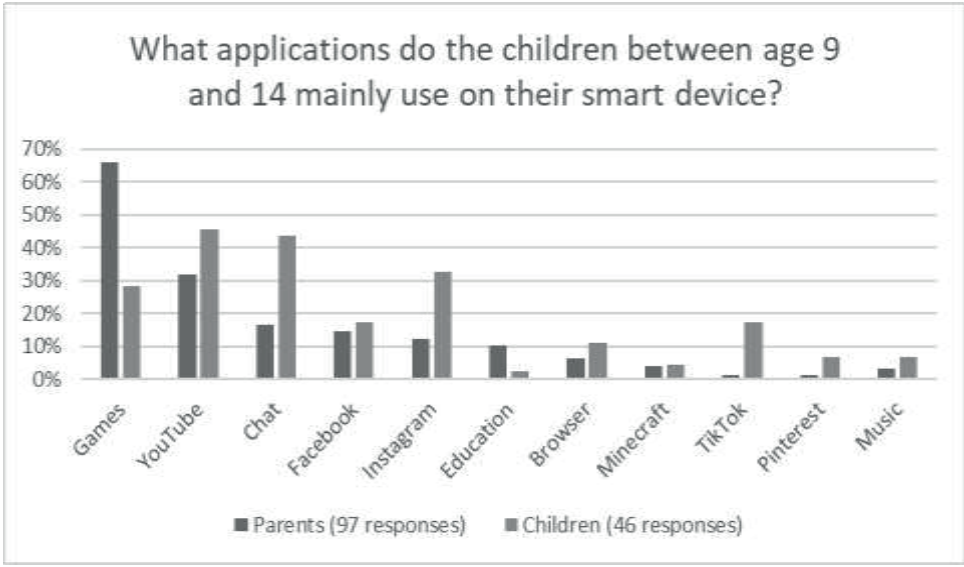

Figure 2: What applications do the children between 9-14 use?

4. Legislative requirements

4.1. European Strategy for a Better Internet for Children

As the application had to be designed in alignment with the European and Hungarian legislation (that is the same from the privacy perspective due to GDPR), first of all, we went through the relevant legal texts. Besides GDPR, there is another important strategy that should be considered. This is the European Strategy for a Better Internet for Children and was declared as a communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions in 2012. [5] Although this strategy is rather old and uses outdated data, the basic statement related to privacy is still valid: "Research shows that there is a serious digital skills deficit amongst Europe's children, despite the popular view that they are "digital natives". For example, 38 % of 9-12-year-olds in Europe who use the internet report that they have a personal profile on a social networking site. However, only 56 % of 11-12-year-olds say they know how to change their privacy settings. Research also found that the range of digital skills and online activities are linked. Therefore, developing safety skills may encourage other skills associated with other online activities."

Our assumption is that Mongu for Teen can support this strategic goal. However, the same document describes what should a digital service provider do for the privacy of children: "Although risks to privacy exist for all users, children are a particularly vulnerable group. Very young children in particular do not know how to change their privacy settings and do not understand the potential consequences of their actions, such as becoming an easy target for grooming or exposing themselves to risks to their online reputation. Therefore, default privacy settings for children should be managed in ways that ensure they are as safe as possible.

Industry is expected to:

- implement transparent default age-appropriate privacy settings, with clear information and warnings to minors of the potential consequences of any changes they make in their default privacy settings and contextual information on the privacy level of every piece of information required or suggested to set up an online profile.

- implement technical means for electronic identification and authentication."

As this strategy is coming from the pre-GDPR era, it also highlights some steps that should be done by the Commission and the member states. We must be stated that most of the requirements below are part of the GDPR now.

"The Commission:

- proposed a new data protection regulation that takes specific account of children's privacy and introduces the "right to be forgotten".
- intends to propose in 2012 a pan-European framework for electronic authentication that will enable the use of personal attributes (age in particular) to ensure compliance with the age provisions of the proposed data protection regulation.
- will support R&D to develop technical means for electronic identification and authentication on relevant services across the EU and their deployment.

Member States should:

- ensure the implementation of EU legislation in this field at national level.
- encourage the adoption of self-regulatory measures by industry and follow their implementation at national level.
- support awareness raising activities at national level."

4.2. General Data Protection Regulation

Children, like adults, have the right to privacy and to the protection of their private and family life. Privacy encompasses the protection of personal data and the confidentiality of the processing of data within online social services. Simplified, data can be collected for a specific purpose under the GDPR, and can be stored for a reasonable time, keeping in mind the time of usage and the principle of data minimization. GDPR gives special protection to children's personal data and imposes greater obligations on data controllers who manage children's data in the course of their activities.

Besides the already quoted paragraph, some other parts also highlight the requirements for application developers. According to (58), "The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualization be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."

Paragraph (65) says that "A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed,

where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defense of legal claims."

According to paragraph 71, decisions based on automated data management, e.g. profiling, including actions taken as a result, should not be applied to children. Paragraph 75 states that risks connected to the rights and freedoms of natural persons may result from the processing of personal data, which may result in physical, material or non-material damage. It also classifies children's data as a high-risk factor.

In Article 8, Conditions applicable to child's consent in relation to information society services, there are additional requirements: "in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."

5. Privacy in Practice

5.1. Legal implementation

GDPR requires to keep and to comply its strict obligations particularly for an application that collects and process children's data. Thus, we faced with a lot of challenges when we wrote the privacy policy that is suitable for both parents and legal experts and can be understood by the youngsters as well. The true defiance is to create a text that is easily understandable, general, protective, brief but at the same time, it contains all the points that the regulation requires.

Writing of the privacy policy had different phases. First of all, it had to be collected and examined the different rules of data protection of the most popular social media sites and applications. Then we could merge these texts in accordance with GDPR rules and from other manuals for example: Children and the GDPR guidance. [6] After the draft has been created, we discussed and further specified it, by focusing on the technical and legal details. We had the possibility to make an interview with dr. Júlia Sziklay, the head of department of the National Authority for Data Protection and Freedom, responsible for the children's privacy. We could ask our questions in connection with the privacy policy. Then we rewrote our policy rather and we sent it to a data protection lawyer for review.

After her advices, we made a more logical and legally specified policy with 11 points with legal definitions too. Although we wrote a well detailed text, we felt that it could be hardly understood because of the legal language, so we decided to make a simple, "child friendly" version of it. The

source that we used was the UN Convention on the Rights of the Child. [7] The most difficult challenge we met is how to explain something complex and difficult subject like data protection for the children? How to comply with GDPR that requires clear, comprehensive formulation, meanwhile some parts of it are confusing even for the experts? Another issue was how to gather the approval of the parents for data collection. In the technical implementation, we provided our policy for reading as the first step during the installation. The policy itself is using a child-friendly composition. As soon as the parent read it, he or she can create a family through the app, confirming the approval of data collection.

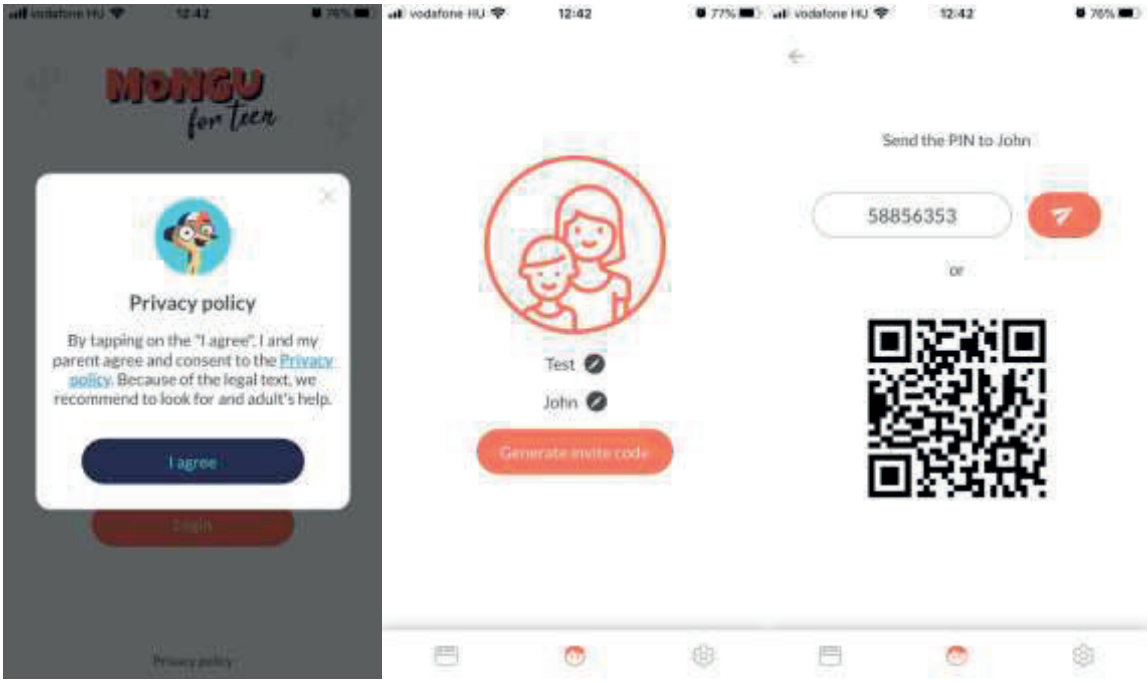

Figure 3: Lettering of figures

5.2. Technical implementation

As highlighted earlier, one of the key aspects of the solution is the user privacy and as a such the data security. We followed the security by design methodology. We put special efforts on the following topics:

1. User management
2. Authorization
3. Secure process for linking family members
4. Secure channels
5. Security handling of log messages
6. Intrusion detection system
7. Minimal data to handle

First of all, we separated the user management data from the application data. Google Firebase were selected as a third-party solution for user management. It is a widely used solution, therefore, the security weaknesses are quickly detected and repaired. Their privacy policy is clear, and it makes sure that the data stored there is not used by Google or any third parties for other purposes than providing authentication services. The framework supports user to login with their Google or Facebook account, or register with their e-mail. On Mongu for Teen side, no other data than a user

specific random identifier is saved in our database. We don't even have access to the users' password, and we don't fetch the e-mail address or anything which can be bound to the user.

The mobile client communicates via API calls with the server. Based on the random identifier, on server side we perform client authorization. It assures that the users can access only data which are specific to them or their families. The authorization is performed on the server side. Even if someone reverse engineers the API, which might be easy for an expert, cannot access any data without valid login credentials. All in all, a child can access data only about himself, and a parent can access data only about him- or herself and the linked children.

Linking family members together is initiated by the parents. They can add kids to the family by defining the family name, kid's name and generate a one-time 8-digit password. This password can be sent to the kid via multiple channels including offline and online methods. Once the kid initiates the joining process, he or she needs to set the one-time password. If it is a valid one, the kid has to confirm that the family name and his or her name is set properly. It is important to make sure that the kid does not join a wrong family.

Beyond what a regular user faces on the security of the Mongu for Teen, there are other considerations which protects the users' data under the hood. First of all, all communication channels are encrypted, and server is authenticated following the best practices, using TLS. We paid special attention to configure to support only secure cipher suites. This assures that no information leaks on the network.

There is a channel which cannot be protected with TLS, but requires special attention, because sensitive information may be transferred. It occurs when a user wants to report an application problem and sends mobile client related logs via e-mail for evaluation performed by the development team. As e-mail channels cannot be trusted, we applied asymmetric cryptography to make sure that all data is encrypted all the way from the user's device to the developer team. Thanks to the asymmetric cryptography only the development team can read the logs. It is important to note that user specific data are not sent without a user action. Logs may contain also network traffic related information. It is used only for debugging. We delete the data according to the data retention policy, and never used for user profiling.

We minimize the amount of data stored. However, still there are valuable information on the server side which must be protected. Therefore, we use the services of a cloud provider which is security focused in order to decrease the chance of data leakage.

6. Conclusions

With the advancement of technology, privacy seems to be lost, as with our consent, we disclose our personal information to the outside world through online digital services. As we have an unimaginable opportunity to be visible for the whole world, we can generally say that we all want to make something lasting in our life, to be visible in the crowd. However, in practice, images, posts, articles, reviews, contacts that appear on the web pages and are associated with our person become data and may be used unlike we intended. This contradiction raises many questions for the end users and legislators as well.

Generations Z and Alpha who have been born into the digital era had no choice. The rapid flow of information affects their psychological behavior, can cause personality disorders, and can even lead to a deterioration in literacy. As parents, who have grown up before the age of Internet and it is

frustrating to think of the societies that will live in the coming decades. In our paper, we highlighted some aspects of the misunderstanding between kids and adults and stressed the importance of trust and communication in a digital family. We also described the actual EU strategies and legislation to protect children in the cyberspace and the difficulties of being compliant as a digital service provider. Lastly, we presented a case study, how an application developer should follow the rules and protect the privacy of the youngest generation.

7. References

[1] NAGY, A. and KÖLCSEY, A., (2017). Generation Alpha: Marketing or Science. Acta Technologica Dubnicae. 7. 10.1515/atd-2017-0007.

[2] League of Nations, "Geneva Declaration of the Rights of the Child of 1924", *Humanium*, [Online], Available: https://www.humanium.org/en/text-2/ [Accessed: January 24, 2020]

[3] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[4] Psyma Hungary, Kft., "Research on media usage, consumption and literacy of 7-16-year-old children and their parents", *National Media and Infocommunications Authority,* 15 August 2018 [Online], Available: http://english.nmhh.hu/document/209495/NMHH_PSYMA_7_16_ages_2017_Executive_summary.pdf [Accessed: January 24, 2020]

[5] European Commission, "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS European Strategy for a Better Internet for Children /* COM/2012/0196 final */", *European Commission,* 2 May 2012 [Online], Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012DC0196 [Accessed: January 24, 2020]

[6] Information Commissioner's Office, "Children and the GDPR guidance", *ICO*, 21 December 2017, 2012 [Online], Available: https://ico.org.uk/media/about-the-ico/consultations/2172913/children-and-the-gdpr-consultation-guidance-20171221.pdf [Accessed: January 24, 2020]

[7] United Nations, "Convention on the Rights of the Child", UNICEF, [Online], Available: https://www.unicef.org/child-rights-convention/convention-text [Accessed: January 24, 2020]

.