International Working Group
on Data Protection in
Telecommunications

Protecting the Privacy of Children in Online Services[1]

Working Paper

Adopted at the 65th meeting, 9-10 April 2019, in Bled, Slovenia

Introduction

1. Children are a vulnerable category of online services users. Their naiveté, and lack of capacity for making an informed decision, increase the risk of a false feeling of control, or other unintended consequences of their online behavior. In some cases, the collection and use of data pertaining to children, may constitute privacy and data protection violations, and in some cases it may lead to other unlawful consequences, ranging from mere nuisances to more serious consequences such as cyberbullying, sexual and other exploitation.

2. Children spend a significant amount of time using online services such as websites, apps, gaming services, voice over IP services and Instant Messaging Services through a variety of devices, such as smart phones, tablets, PCs and smart TVs, as well as other IOT devices such as virtual assistants. The services are used by children for a variety of purposes, including entertainment, interacting with friends, family and third parties, consuming music and videos, and looking for information for a variety of purposes including school tasks.

3. All these services collect and process personal data, starting with contact information, location data, still or video images, usage data and data about interactions with the services, etc.

4. Online services should be adequately protected, and designed in a way that respects individuals' privacy rights. This could include, but not be limited to, mechanisms that will enhance transparency and ensure the validity of consent given for the collection and processing of data related to children.

Scope

5. The paper applies to online services that are intended for children.

[1] The Office of the Privacy Commissioner of Canada abstains from the adoption of this Working Paper.

6. Its purpose is to highlight the main privacy risks and challenges associated with the use of online services by children, and provide recommendations for policy makers, online services developers and providers, and regulators.

Definitions

7. For the purpose of this paper:

   A **child** is a person 18 years and under. For the purpose of informed consent, there can be lower age limits provided for by applicable law.

   A **parent/guardian** is the lawful mother or father, or any other holder of parental responsibility who for the purposes of providing consent acts as the child's legal representative.

   An **online service** is a service that is provided by electronic means, without the parties being simultaneously present, on individual request. These services may include websites, apps, gaming services, voice over IP services, Instant Messaging Services, VOD services and more.

8. The provisions of this paper should be read and interpreted in light of the United Nations' Convention on the Rights of the Child according to which:

   a. In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration (Article 3a); and

   b. No child shall subjected to arbitrary or unlawful interference with his or her privacy (Article 16).

Risks and aggravating factors

9. Children are still developing the skills that they need to act an informed digital citizen, and therefor are not fully aware of the risks and harms that might result from their data being collected and processed.

10. Privacy policies are complicated to understand, even for adults.

11. Children don't always have the knowledge that is required to manage privacy settings and protect their data.

12. Children do not understand that the disclosure of personal data, including contact information, may result in the transfer of their data to third parties, or the integration of the data with other available data sources, without their knowledge. There are many risks that the data will be misused for a variety of purposes including the creation of behavioral profiles, identity theft, cyberbullying and even sexual abuse.

13. In many cases, apps and websites share data with third parties without the knowledge of the users. The complexity of such systems and the underlying technology (cookies, fingerprints, iframes, SDKs, etc.) is difficult for adults to understand, let alone children.

    Possibilities for intervention, especially in the form of technical tools, are difficult for children to understand.

14. The disclosure of personal data during the use of online services has long-term consequences, sometimes irreversible, for the child's future. In other cases, the child's actions may also have an irreversible effect on other parties (e.g., posting a picture or comment about a third party).

15. Due to the factors mentioned so far, it is often not feasible to obtain informed consent from children regarding the collection and processing of their data in online services even where it is legally permissible.

16. Although parental consent is an effective tool to enhance privacy protection and to ensure informed consent for the collection and processing of data, it requires, in some cases, authentication mechanisms in order to determine users' age and authenticate the consent of the parent/guardian. Implementing such mechanisms raises the risk of collecting excessive data which in turn would also be a violation of privacy.

Recommendations

For policy makers

In order to strengthen privacy protection of children in online services, and address the above mentioned risks, policy makers should promote regulations, concerning the following:

17. Data of children should be collected and processed by online services only after receiving the freely given, explicit and informed consent of their parents/guardians, unless:

    a. The child has reached an age at which applicable law provides for the ability to consent, and the child her- or himself has freely given explicit and informed consent;

    b. There is another legal basis for the collection and processing of the data, for which consent (of the data subject or their parent/guardian) would not normally be required;

    c. The best interest of the child will be served by not involving their parent/guardian (e.g., child protection hotline).

18. Data of children must be deleted upon their request or that of their parent/guardian in order to reduce negative implications for the child's future. In the absence of a reasonable justification (e.g., an obligation under the law to hold the data), controllers should not refuse the request of a child or parent/guardian to delete data of the child.

19. Data controllers should only retain children's' data for as long as is necessary to provide the service. Adults, whose data was collected and processed when they were children, should also have the right to have that data deleted upon request.

For controllers

Parental Consent

20. Subjecting collection and processing of children's personal data to parental consent is an effective tool to overcome the lack of ability to receive informed consent from children and therefore where consent is the legal ground for the processing, data controllers should process personal data of children only after receiving the consent of their parents except in the cases described in No. 17.

21. When the online service is offered to the general public and not just for children, but is commonly used by children, the controller should make reasonable efforts to verify if the user is a child and to verify that the consent is given by the parent/guardian.

22. Verification processes might result in collecting additional personal data about children and their parents/guardians, and therefore controllers and industry at large are encouraged to develop reliable mechanisms that would verify the age of the user and the authenticity of the parental/guardian consent in a proportional manner. One state-of-the-art approach for this is the application of data minimizing technologies like zero-knowledge proofs for testing whether the user has reached a certain age.

23. Once the controller has knowledge that the data subject has reached the age for which parental consent is no longer required, the controller should not rely on the consent of the parent/guardian for continued storage and use of previously collected data, but should obtain the consent of the data subject himself. Controllers should not collect age data exclusively for the purpose of fulfilling this requirement.

Transparency in online services for children

24. Controllers should make it clear to children and their parents/guardians that providing data is subject to parental/guardian consent (unless there is a legal obligation or other applicable legal basis that would allow the collection without parental/guardian consent).

25. Controllers should inform the children (if and to the extent to which data is collected directly from them) and their parents (except in the case described in No. 17.c) in particular about the collection, use and processing of data, the purpose for which the data was collected and their user rights (e.g., access, deletion) before collecting the data.

26. Controllers should disclose in detail the types and level of sensitivity of data collected, the possible risks of data being transferred to unknown third parties and contact details of the controller.

27. Controllers should inform the children and their parents/guardians about their privacy policy, and the way in which the parents/guardians may give their consent for the collection and processing of the child's data.

28. The above information will be delivered to users in an accessible and comprehensive manner using appropriate and child friendly means (graphics, videos, dashboards, etc.).

Privacy by Design and by Default and additional privacy enhancing mechanisms to be integrated in online services for children

29. Services for children should include Privacy by Design and Privacy by Default mechanisms and additional privacy enhancing mechanisms. Wherever they foresee interaction with the user, these mechanisms should be designed in an age appropriate manner.

30. Controllers should implement technical and organizational measures to ensure that, by default, only personal data which is necessary for each specific purpose of the processing is collected, processed and stored. This obligation applies to the amount of data collected, the extent of the processing and the period of the storage.

31. The younger the users for which the service is intended, the more stringent the privacy by design mechanisms that should be implemented.

32. The type of data collected and its sensitivity should also be taken into consideration when developing privacy by design mechanisms.

33. In order to implement Privacy by Design and by Default mechanisms, it is highly recommended to perform a Data Protection or Privacy Impact Assessment to identify and mitigate privacy risks for children, including the age verification process if implemented.[2]

34. Changing privacy settings and defaults in a way that may result in decreasing privacy should only be possible after obtaining parental/guardian consent.

35. The service provider should explain to children and parents/guardians the importance of strict privacy defaults and warn about the consequences of changing the settings, in a clear, age-appropriate language, including visuals where relevant. This warning should appear when the user asks to change strict settings to more lenient ones (e.g., settings that entails potential risks for identifying the child, creating profiles, installing cookies, etc.).

36. Additional privacy enhancing mechanisms may include pre-defined sentences to be used in the service, "closed garden" mechanisms that prevent sharing the data with other networks without prejudice to the fulfilment of data portability requests, etc.

[2] There may be a legal requirement to perform a DPIA in certain jurisdictions in those circumstances

Data quality

37. Children mature and develop over the course of years, and therefore, often data about them becomes outdated and irrelevant to the purpose for which the data was originally collected and processed.

38. It is highly recommended to implement mechanisms that will enable the correction, updating and deletion of irrelevant, incorrect or excessive data. Mechanisms offered to children for this purpose should be age-appropriate.

Access rights and data portability

39. Mechanisms for access rights and data portability should be designed in a manner that fulfils the child's best interest taking into account:

    a. The duties of the parent/guardian for the child's well-being;

    a. The child’s rights of autonomy and privacy;

    b. The age of the child or the age for which the service is intended; and

    c. The type of online service.

For regulators

40. Regulators should raise public awareness of the risks for children in online services.

41. Regulators should consider exercising their powers to audit or investigate online services for children or which are commonly used by children. Where they obtain information about practices that create risks for children, they should use this information in order to address those risks in guidelines and best practices.

42. At the international level, regulators around the world should share the above mentioned information about risks and best practices, and should consider engaging in joint enforcement actions when needed.