International Working
Group on Data Protection in
Telecommunications

Privacy Risks with Smart Devices for Children

Working paper

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

Introduction

1. Smart devices for children encompass smart toys, smart watches, baby monitors and other devices specifically targeted to children. These devices use the internet for the purposes of determining real-time location, tracking of and direct communication with young children. They may store names, photos and continuous and historic geolocation data, and may monitor health data as well.

2. In 2016 and 2017 Norwegian Consumer Council (NCC) began analysis of consumer and privacy issues in three internet-connected toys[1] (My Friend Cayla and Hello Barbie, and the robot i-Que) and four smart watches[2] (Gator 2, Tinitell, Viksfjord, and Xplora). The reports spurred a lot of media attention as they pointed out a disturbing lack of regard for consumer rights, security and privacy.

3. Further investigations by consumer associations in the UK, Belgium, Germany and Spain found worrying security flaws in common smart toys on the market[3].Growing concerns have led to initial responses from lawmakers[4], consumer associations[5, 6], privacy and electronic communication supervisory[7] and even bans on the sale of certain smartwatches for children with an "eavesdropping" function.

---

* The Office of the Privacy Commissioner of Canada abstains from the adoption of this Working Paper.

1 NCC report: #Toyfail: An analysis of consumer and privacy issues in three internet-connected toys (https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf). NCC report also includes technical analysis made by a consultancy firm: Investigation of privacy and security issues with smart toys, https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technicalanalysis-of-the-dolls-bouvet.pdf.

2 NCC report: #WatchOut: Analysis of smartwatches for children (https://fil.forbrukerradet.no/wpcontent/uploads/2017/10/watchout-rapport-october-2017.pdf). NCC report also includes technical analysis made by an IT consultancy firm.

3 ANEC & BEUC: Cybersecurity for Connected Products Position Paper (https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf).

4 The EU Commissioner for Justice, Consumers and Gender Equality, Vera Jourova, expressed her worries about the impact of connected dolls on children's privacy and safety (https://www.bbc.com/news/world-europe-39002142). In its Public Service Announcement of 17/10/2017, the FBI warned of possible cyber exploitation of IoT devices including watches and toys (https://www.ic3.gov/media/2017/171017-1.aspx).

5 European consumer associations (BEUC and ANEC), for example, called on lawmakers to ensure that mandatory requirements for technical safeguards are introduced according to the principles of security by default and by design (https://www.beuc.eu/publications/beuc-x-2017113_serious_security_and_data_protection_flaws_in_smartwatches_for_children.pdf).

6 Options consommateurs, a consumer association based in Canada, as well as Concordia University, also conducted independent research on this issue, funded by the Office of the Privacy Commissioner of Canada. Links to the reports can be found at can be found at https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completedcontributions-program-projects/2017-2018/p_201718_01/ (Options consommateur) and https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-andknowledge-translation/completed-contributions-program-projects/2017-2018/p_201718_07/ (Concordia).

4. According to market reports children's smartwatches will account for 30% of smartwatch shipments in 2021[9], while privacy concerns were most worrying according to user surveys[10].

5. While smart dolls and robots for children are primarily interactive toys that respond to children's voices and converse with them, smart watches for children are essentially wearable mobile phones that allow parents/guardians to use an app on their smartphones to monitor, keep in touch with and track the location of their children. Depending on the make, smart watches are able to make/receive calls, have contact lists, offer GPS tracking in app, geofencing, emergency button and voicemail.

6. Smart devices for children are part of the growing trend of attaching sensors to a broad variety of devices and connecting them to the internet, commonly referred to as the Internet of things[11] (IoT).

Scope of the working paper

7. This working paper focuses on privacy issues specific to smart devices for children and accompanies the work carried out by the Working Group in the area of parental consent and protecting the privacy of children in online services[12].

8. Whilst raising specific privacy issues of their own, on-line services for children, game consoles and similar devices are not in the scope of this paper.

Privacy risks

Overview

In the following, the paper points out data protection and privacy risks that have already been realized based on the reports mentioned above.

9. As a general finding of the above-mentioned reports on consumer and privacy rights, the terms of use and privacy policies mostly lack the expected level of

---

7 https://www.cnil.fr/en/connected-toys-cnil-publicly-serves-formal-notice-cease-serious-breachprivacy-because-lack-security

8 Bundesnetzagentur takes action against children's watches with "eavesdropping" function (https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17112017_Verbraucherschutz.html)

9 http://mobilemarketingmagazine.com/310m-global-wearable-sales-2017-gartner

10 University of Washington: Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys (http://techpolicylab.org/wp-content/uploads/2016/01/Toys-That-Listen_CHI-2017.pdf).

11 The working Group has previously written on privacy risks associated with wearable devices (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2015/28042015_en_2.pdf), updating firmware in embedded systems in the Internet of Things (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2017/2017IWGDPT_Working_Paper_Firmware_Updates-en.pdf).

12 Working Paper: Protecting the Privacy of Children in Online Services.

transparency towards the individuals – they are using vague language, are unclear about the scope, purposes, retention times and secondary uses of the collected data and reserve the right to change the terms at any time. This substantially undermines user control and erodes respect for basic principles of privacy and data protection, such as lawfulness of processing, as further elaborated below.

10. Several security flaws in smart devices for children and/or accompanying apps have been identified that allow attackers to gain access to sensitive information such as video recordings, geolocation and photos whilst on the other hand providing unreliable safety functions (emergency button and geofencing).

11. It is not only children and parents/guardians whose privacy rights are at risk. Reports have shown that parents/guardians have been using smart watches to eavesdrop on teachers during lessons[13]. Similarly, some producers reserve the right to use contact data from the toys and/or associated apps, thus processing personal data of unsuspected third parties.

Lack of transparency

12. The principle of transparency requires that any information and communication relating to the processing of personal data be easily accessible and easy to understand, and that clear and plain language be used. Instead, individuals are often not made aware of, or are even misled by, the design of the user interface, which can lead to acceptance of privacy unfriendly settings.[14]
13. Terms and conditions and privacy policies for smart devices for children are often not easily available through the app stores and on official websites of the product and/or company.

14. The information provided often does not address the needs of parents/guardians, and of children, in separate and appropriate language for each. For example, although the terms should be directed at parents/guardians, some examples make it unclear whether they are actually aimed towards children.

15. The terms of use are often not written in clear and easy to understand language and are not in a user-friendly layout. Terms of use and privacy policies for smart toys are often not product specific and have been found to contain between 6000 and 8000 words, which is the equivalent of about 15-20 pages.

16. Several terms of use include vague wording (e.g., “we may”), which offers little transparency to the parents about what the smart device for children and functionalities of it actually do.

13 https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN//17112017_Verbraucherschutz.html

14 For instance, «default settings and dark patterns, techniques and features of interface design meant to manipulate and nudge users towards privacy intrusive options», «Deceived by design, How tech companies use dark patterns to discourage us from exercising our rights to privacy», Report by Forbrukerrådet (Norwegian Consumer Council), 27.6.2018, https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

17. The terms of use are mostly unclear about the scope of personal data that is processed and merely reference applicable data protection legislation.

18. The terms of use are generally vague about data retention and reserve the right to terminate the service at any time without sufficient reason. They state that they may keep personal data for “legitimate business or legal purposes” without further elaboration.

19. All these factors contribute to the fact that the terms of use and privacy policies are not giving sufficient information to understand the service.

20. Furthermore, changes to the terms of use are not communicated to the parents/guardians, who would have to resort to regularly checking the producer’s website to be properly informed about the changes in functionality of the smart device for children, the processing of personal data and their rights.

Unlawful processing

21. The transparency deficiencies lead to further legal concern, in particular to lack of informed consent as clear information is a prerequisite for valid consent.

22. Often, as in the case of smart watches, the information cannot be presented on the device itself. Also, consent is often not obtained during the registration process for the accompanying app. In consequence, there is no valid informed consent at all.

23. Consent for processing of data is often bundled with the acceptance of terms and conditions. This means that the user cannot distinguish between the processing for the performance of the contract, and that based on consent. In this case, there exists no freely given consent for the processing of data beyond the performance of the contract, and that processing is unlawful.[15]

Unauthorized secondary use

24. Terms of use and privacy policies are generally very vague about the sharing of data with third parties and state that they can share data with “vendors, consultants, and other service providers”, without specifying exactly with which third parties the data is being shared or giving examples of what this entails. Even when specifically mentioned, these third parties maintain their own privacy policies, which makes it very difficult for the parent to ascertain what their children’s data, including their voice, photos, IP addresses and locations, are actually being used for.

25. As an example, voice data that is collected, and which may contain sensitive personal data, is often used for analytical and research purposes. It may even be used to improve services unrelated to the relevant device, such as to enhance and improve the speech recognition and other components of other services and products offered by producers of smart devices for children.

15 Cf. Working paper on Protecting the Privacy of Children in Online Services.

26. The companies behind the smart devices for children refer to wide licenses to use and distribute childrens' voice data, while failing to properly identify or restrict the purposes for which such information may be used.

27. Some of the devices transfer personal information to a commercial third party, who reserves the right to use this information for practically any purpose, unrelated to the functionality of devices themselves.

Data Minimization/Excessive collection

28. When children's´ voices and interactions with the devices are stored over long periods and made accessible for secondary use, data is typically processed excessively.

29. Technical data access permissions (e.g., in apps that accompany the smart watches) are often not limited to strictly function-related purposes of the smart devices.

30. In some cases, producers or licensors claim they need to collect their users' contact names for speech recognition purposes. This is of special concern since the contacts whose names are collected are unsuspecting parties, who have no way of knowing or consenting to their information being collected or used.

Data retention

31. Collected data will often be kept on the providers' and other third parties' servers for a long time, sometimes without any limitation at all.
32. If users delete data stored in their devices, they might not be aware that copies of these data persist at other storage locations, and continue to be processed.

Inadequate security

33. Reports on smart devices for children have identified a series of security flaws that could lead to personal data of children and parents/guardians being compromised, and the confidentiality of private conversations among children and parents/guardians being breached. It was discovered that some the smart devices for children have practically no embedded security. The most common security flaws are the following:
    a. Lack of authentication mechanisms being used while pairing with Bluetooth enabled, which could lead to a third person being able to connect to the device as long as they are turned on and not already actively paired with another device, thus using the smart device for children as a Bluetoothheadset. Anyone could potentially compromise the smart device for children in order to both converse with and covertly listen to the children or other people in the presence of the device.
    b. In the case of smart watches some of the devices have flaws which could allow a potential attacker to take control of the apps, gaining access to children's real-time and historical location and personal details, as well as even enabling them to contact the children directly.

c. Some features, such as the emergency button (alerting the parents/guardians if the child is in distress) or the geofencing function (informing the parents/guardians whenever the child enters or leaves a pre-designated area), have been identified as unreliable thus providing a false sense of security.
d. Other security flaws that have been identified in security testing include location spoofing, misuse of voice call functionality and covert account takeover.
e. There are often no, or insufficient, provisions made to update the software of a smart device when security flaws are discovered.

Recommendations

General

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.[16] Data processing with smart toys particularly affects children and adolescents, a group of data subjects regarded with particular need for protection in many data protection laws. This should be reflected not only in increased transparency requirements and the implementation of appropriate ways for children and parents/guardians to manage privacy settings and exercise their data protection rights but also in strong restrictions for secondary uses of data. This applies in particular to data that is inextricably linked with data subjects, such as voice data, and which can be used for personality analysis and the prediction of future behaviour, health states, etc.

Manufacturers/producers:

34. Clear, accessible and readable terms of use should notify parents/guardians of exactly which personal data will be processed, by whom (including third parties), for what purposes, about retention times, control options and user rights. Particular attention should be paid to the processing of sensitive data such as voice recordings.

35. Even if parents/guardians are those making the decision, children should be made aware of risks for educational reasons. Therefore, there should be information in age-appropriate language about the data processing involved.

36. Establish a clear distinction between the processing of personal data necessary to perform the contract with the individual, and the processing of personal data that must be based on consent.

37. Consent must be obtained to process personal information for purposes that go beyond what is necessary for the performance of the contract. Granular consent

16 United Nations: Convention on the Rights of the Child (https://www.ohchr.org/en/professionalinterest/pages/crc.aspx).

should be sought for other than basic processing of personal data with the possibility of specific and separate opt-in for different purposes of processing.

38. Parents/guardians should be notified in advance about changes in terms of use and privacy policies so they can make informed choices about the use of smart devices for children.

39. Manufacturers of smart devices for children should follow the privacy by design and security by design approach, which entails that privacy and security-related risk assessments are undertaken during the entire design-process.[17] Privacy and security measures and safeguards should be embedded into product design while services offered should respect in particular the principles of data minimization and purpose limitation. Smart devices for children should not collect more data than necessary for the functionality of the service and this data should not be used for purposes that are not intrinsically required for these functions.

40. Information security standards should be respected, incorporating encrypted connections and stored data, manual activation of microphone, visual indicators when the device is recording voice, control accounts/dashboards for parents/guardians, filters, secure Bluetooth and wi-fi pairing and connections.

41. Notice about video capturing and voice recording should not only be described in the terms and conditions but also on the packaging of smart devices for children. For such notice, standardized icons should be developed.

42. Smart devices for children and accompanying apps should benefit from security and firmware patches.[18]

43. Terms of use should clearly indicate data retention periods considering the data minimization principle.

44. User rights should be respected, and methods should be provided to exercise them easily. “Parent/guardian dashboards” for smart devices for children are an example of good practice enabling parents to control, review, share, and delete

    any recordings or other personal data collected through the use of the smart device for children.

Other data controllers and processors

45. If a third party application or system is used for interaction with the toy, all previous requirements regarding personal data processing must be applied. In particular, the information provided to the users should clearly identify all third parties involved in the data processing with their geographic location, and the points of contact for exercising the users’ rights.

---

17 Gürses, Troncoso and Diaz: Engineering privacy by design reloaded (http://carmelatroncoso.com/papers/Gurses-APC15.pdf).

18 Cf. Working Paper: Updating firmware of embedded systems in the Internet of Things.

Standardization bodies

46. Standardization bodies should consider the need for certification mechanisms and standards which enable manufactures to meet the data protection requirements.

Users (parents/guardians and children)

47. Parents/guardians should be aware that smart devices for children offer unprecedented functionalities and should refrain from buying products that do not offer clear and easy to understand terms of use, privacy policies and control dashboards.

48. Children should be given guidance on the appropriate use of the smart device.

49. Parents/guardians should consider the appropriate age for giving such a smart device to their children, keep the device turned-off while not in use, use common security measures such as strong passwords and safely delete any personal data when giving the device away[19] [20].

50. Parents should refrain from buying products that offer potentially privacy impacting functionalities (e. g., internet connectivity, voice recording or geolocation), unless those are necessary for the intended use.

Schools and teachers

51. As smart devices for children are often also used in schools, teachers should inform themselves about the relevant privacy risks of smart devices and provide appropriate guidance to children.

52. Schools should have policies in place to vet smart devices used in the classroom in order to understand the relevant privacy and security risks and should provide appropriate guidance to parents/guardians and students. In areas where the use of the smart device might infringe on the rights of other children, or school employees, the schools should require that the devices be turned off, or not brought to those areas at all.

Data protection authorities and regulators

53. Data protection and privacy authorities should closely follow the developments and regulation in the field of smart devices for children and, in line with their competencies, demand clear and specific terms of use from respective data controllers.

---

19 See for example: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/ 7523979

20 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/11/blog-the-12-ways-that-christmas-shoppers-can-keep-children-and-data-safe-when-buying-smart-toys-and-devices/

54. Where appropriate technical standards exist, regulators that have the legal powers should make the application of these standards mandatory.

55. Data protection and privacy authorities should enforce requirements regarding notification, data subject's rights, the principles of proportionality and security of personal data from manufacturers or other third parties (app makers, analysis and marketing companies, etc).

56. Using their awareness raising competencies data protection and privacy authorities should promote best practices in the field of smart device for children, particularly in the field of transparency, consent and empowerment of the parents.

57. Data protection and privacy authorities should consider conducting tests and benchmarks of mainstream and/or innovative smart devices for children in association with consumer protection authorities and associations.