Ingrida Milkaite & Eva Lievens

Towards a better protection of children's personal data collected by connected toys and devices

Future-Proofing
our Digital Rights

DFF Digital Freedom Fund

Ingrida Milkaite & Eva Lievens

Towards a better protection of children's personal data collected by connected toys and devices

A snapshot of children's digital lives

Internet connected devices and applications are increasingly present in individuals' lives and homes. These trends inevitably also affect children. From a young age, they use smart devices that are created for them, such as internet connected smart toys, enabling play and learning. They are also affected by devices that are not directly targeted at them but are nevertheless "around" in their daily reality, such as smart home assistants that record and process everything that is said in a home, including children's conversations.

Interactive toys, such as the "Hello Barbie" and "My Friend Cayla" dolls engage in conversation with children, record children's voices, store them through the services of different companies and may also transfer recorded data to advertising, analytics or other companies. Cuddly toys or baby clothing contain medical sensors that monitor children's body temperature, heart rate and

blood oxygen saturation levels which may be consequently sent to a parent or doctor's app. Finally, cute connected robots now share features which include voice recognition, remote video control, gesture-based interactions and facial tracking of children. **Given the fast-paced evolution of technology, unwavering advances in machine learning and big data analytics, and the ongoing digitisation of childhood, it can only be expected that such connected or smart toys and devices will continue to be developed and marketed in the coming years.**

It can only be expected that such connected or smart toys and devices will continue to be developed and marketed in the coming years.

Consequences?

Yet, in an environment where so much information can be collected through interaction with devices, children cease to be mere "players" or "consumers". They become "data subjects" that disclose information or "personal data" about themselves, both consciously and unconsciously. Today, children's personal information is collected and processed in unprecedented quantities, a phenomenon that scholars have denoted the "datafication" and "quantification" of children's everyday lives from a very early age. This phenomenon is facilitated by the increasing adoption of digital devices, the embracing of apps and platforms for a variety of purposes and the vast possibilities to use, analyse and infer information about users, and, as such, becoming a standard practice that is here to stay.

Of course, personal data might be collected and processed to attain valid or beneficial objectives, think about improving a child's health situation. Concerns, however, relate to the collection and combination of children's (sensitive) personal information enabling the creation of child-user profiles. These profiles can then be used for many different purposes, such as, for instance, behavioural advertising which is so sophisticated that it affects people's, and especially children's, choices without them realising it. Moreover, constructing highly detailed personal profiles of children from a very young age onwards

could also lead to potentially discriminatory practices in the future, such as excluding children with certain profiles from particular types of education or refusing to grant specific health insurance policies based on sensitive medical data that a cute cuddly lion once collected and stored.

In the same vein, the use of artificial intelligence technology which processes children's personal information, such as their product preferences, ambitions, likes and dislikes, which is a feature already integrated in the "Hello Barbie" doll, has sparked difficult questions concerning the never-seen-before emotional bonds between children and objects. Finally, the security of such connected toys and the collected data is an increasing concern in many parts of the world. In Germany, for instance, children's smart watches tracking their location (which were hacked in Belgium and the Netherlands) and the "My Friend Cayla" doll were banned because of security risks. The doll was discovered to be hackable, enabling strangers to talk to children through the doll. In the United States, the Federal Bureau of Investigation (FBI) has warned parents about the potential security risks concerning children's interaction with internet connected toys that are equipped with sensors, cameras, microphones, data storage, voice recognition technologies and GPS trackers.

Playing by the rules? Legal requirements for data processing through connected toys and devices in Europe

A recent recommendation by the Council of Europe on Guidelines to respect, protect and fulfil the rights of the child in the digital environment expects Member States, with regard to connected or smart devices, including those incorporated in toys and clothes, to take particular care that data protection principles, rules and rights are respected when such products are directed principally at children or are likely to be regularly used by or in physical proximity to children.

In the European Union (EU), the General Data Protection Regulation, or the GDPR, which became applicable in May 2018, explicitly acknowledges, for the first time in the context of EU data protection law, that children's personal data merits specific protection since children may be less conscious of the risks, consequences and safeguards, and their rights in relation to the processing of personal data.

On the one hand, the GDPR affords certain rights to data subjects, children included, such as the right to be provided with transparent information about

data collection, processing and storage in clear and plain language, the right to object, or to request erasure of their data. On the other hand, the GDPR requires data controllers (any natural or legal person which determines the purposes and means of the processing of personal data (article 4(7) GDPR), to adhere to certain data protection principles. These principles include, for instance, lawfulness, fairness and transparency of processing, data minimisation, purpose limitation, privacy by design and privacy by default, and ensuring the integrity, confidentiality and security of data. In the context of the Internet of Toys (IoT) devices, these requirements mean that the toys shall process children's personal information fairly, only collect the necessary data for the toy, and protect its security. According to the GDPR, "profiling" and other forms of automated decision making that produces legal effects concerning a person or similarly significantly affects a person cannot concern children (see, for example, recital 71 GDPR). In its recent guidelines on profiling, the Article 29 Working Party confirms that there is no absolute prohibition on the profiling of children in the GDPR, but that organisations should, in general, refrain from profiling them for marketing purposes. This should be taken into account by Internet of Toys providers.

In short, just like general toy safety is regulated, as expected by society (for instance the Toy Safety Directive 2009/48/EC which requires particularly high standards concerning the physical, mechanical, chemical, electrical, hygiene and radioactivity risks), there is a lot of potential in the GDPR to ensure that the child's right to data protection is ensured. The proof of the pudding, however, will be in the uptake and enforcement of those rules.

> There is a lot of potential in the GDPR to ensure that the child's right to data protection is ensured.

Ways forward

The new data protection framework in the EU presents opportunities for a consistent application of important data protection principles to ensure children's rights to privacy and data protection. The implementation of these principles may also lead to a much needed "de-responsibilisation" of children and parents. Data processing is often so opaque that it is not realistic to expect

parents, let alone children, to understand the lengthy and complex privacy policies as we know them. **Under the GDPR, it is up to the controllers to ensure that their data processing practices are designed from their inception with the respect for children's right to data protection in mind.** This will require a change in current thinking, a much more future-oriented thinking about values and fundamental principles that should not only be integrated into design processes from the very beginning, but that should also be evaluated and assessed at regular intervals.

> Data processing is often so opaque that it is not realistic to expect parents, let alone children, to understand the lengthy and complex privacy policies as we know them.

National Data Protection Authorities (DPAs) and the European Data Protection Board, established by the GDPR, are the key actors in terms of the actual enforcement of the obligations that the full chain of IoT providers, such as designers and manufacturers of toys, software and app developers and the platforms where the collected data is stored, have with regard to children and their parents. In the coming decade, the extent to which data processing practices through connected toys and devices will actually afford children the specific protection that they merit will not only be determined by those actors in the chain but will crucially depend on guidance and actions by DPAs.

Finally, governmental and non-governmental organisations, as well as schools and child rights advocates should continue to work on awareness-raising with regard to both the benefits and the risks that internet connected toys present, as well as the obligations of data controllers in this context. Participation of children in the connected society as empowered digital citizens starts in early childhood, and all actors that are involved should do the utmost to ensure that this ambitious goal in achieved, here, now and in the future.

About Ingrida Milkaite

Ingrida Milkaite is a doctoral student in the research group Law & Technology at Ghent University in Belgium. She is working on the research project “A children’s rights perspective on privacy and data protection in the digital age: a critical and forward-looking analysis of the General Data Protection Regulation and its implementation with respect to children and youth”. This project monitors the implementation of the GDPR in relation to children(‘s rights) until 2021.Ingrida takes part in the activities of the Human Rights Centre at Ghent University, is a member of the European Communication Research and Education Association (ECREA) and a contributor to the Strasbourg Observers blog.

When algorithms decide your rights

Future-Proofing our Digital Rights

About Eva Lievens

Eva Lievens is an Assistant Professor of Law & Technology at Ghent University and a member of the Human Rights Centre and the Crime, Criminology & Criminal Policy Consortium. A recurrent focus in her research relates to human and children's rights in the digital environment. She is a member of the Flemish Media Regulator's Chamber for impartiality and the protection of minors, the associate editor of the International Encyclopaedia of Laws – Media Law and a contributor to the European Audiovisual Observatory IRIS newsletter for Belgium.

When algorithms decide your rights

Future-Proofing our Digital Rights

About the Digital Freedom Fund

The **Digital Freedom Fund** supports strategic litigation to advance digital rights in Europe. With a view to enabling people to exercise their human rights in digital and networked spaces, **DFF** provides financial support for strategic cases, seeks to catalyse collaboration between digital rights activists, and supports capacity building of digital rights litigators. **DFF** also helps connect litigators with pro bono support for their litigation projects. To read more about DFF's work, visit: **www.digitalfreedomfund.org.**

The **Future-Proofing Our Digital Rights** project was made possible thanks to the support of the Foundation for Democracy and Media and the Renewable Freedom Foundation. **DFF** receives organisational support from Open Society Foundations, Luminate and Adessium Foundation.

Democracy & Media Foundation **Stichting Democratie & Media**

Renewable Freedom Foundation

DFF Digital Freedom Fund

E-mail:
info@digitalfreedomfund.org

Postal address
Digital Freedom Fund
P.O. Box 58052
1040 HB Amsterdam
The Netherlands