Internet of Toys - Vernetzte Spielwelten

Engl. transl.: Internet of Toys - Interconnected playing environments

# Keywords

* pedagogy
* psychology
* law, technical development

# Details

## Year

2018

## Issued

2018

## Language

German

## Authors

Österreichisches Institut für angewandte Telekommunikation

## Type

Report and working paper

## Publisher

Österreichisches Institut für angewandte Telekommunikation öiat

## Topics

* Internet usage, practices and engagement
* Content-related issues
* Risks and harms
* Online safety and policy regulation
* Other

## Sample

3 days of case study in toy stores (Toys’r’us, Müller, Saturn, Mediamarkt, Conrad, and Libro)
Literature review
Legal analysis
9 expert interviews (law and consumer protection, European data protection, internet of toys, and ethics, developmental psychology and digital gaming, pedagogy and digital gaming, social robotics and ethics, internet of toys development and ethics, developmental psychology and children, pedagogy and internet of toys, data protection, data security and digital gaming)

## Implications For Parents About

Parenting guidance / support

## Implications For Policy Makers About

Creating a safe environment for children online

## Implications For Stakeholders About

## Other Stakeholder Implication

Shop assistants

# Abstract

This study explored the phenomenon of the "Internet of Toys". The aim was to shed light on the possible effects of networked toys on children from an educational and psychological point of view, as well as to provide a case study-oriented analysis of the legal framework and challenges, with a focus on Austria. The project also provides an outlook on future development paths for the classification of risks.
The aim of the processing of the results is to strengthen the competent and safe use of networked toys, as well as to promote the development of safe and sensible toys. The following materials were prepared for this purpose:
- A folder for parents
- A fact sheet for sellers
- A fact sheet for developers
(Translated by the coder)

# Outcome

"The pervasiveness of digitalisation has reached children’s bedrooms: more and more, toys are equipped with microphones and connected to apps. They answer to questions and may be programmed by children. Although the development of smart and connected toys is at its beginnings only, it needs to be taken very seriously in consideration of the possible implications it may have on privacy, the commercialisation of childhood, and the profiling of children. Also, the question of the opportunities of these new forms of play needs to be addressed. This research project has inquired into the phenomenon of internet of toys in Austria (December 2017 – January 2018) – it was funded by the netidee. The focus was to inquire the legal framework in place as well as to explore the pedagogical and psychological dimensions of this change of play patterns. The objective was to develop, based on a thorough analysis of the phenomenon, advice material for parents, developers and vendors. This study is exploratory in nature – based on a typology of smart and connected toys, five case studies were more thoroughly analysed: (1) A doll, which may be personalised online (Lotta, VTech): Parents make indications of i.e. the daily routines of their child. The doll uses the information of the online profile which is not stored. No further data is recorded, the name of the child is only to be recorded on the doll itself. (2) A teddy bear, which may be personalised in an app (Freddy, Vivid): The app allows to set up a data profile of the child with free-text information such as name, birthday, name of friends and family, hobbies, routines, etc. The teddy bear is connected via Bluetooth (without password) with the app and uses the information in a one-directional way (no speech recognition). (3) A dinosaur with speech recognition and artificial intelligence (Cognitoys): The dinosaur is based on the artificial intelligence of IBM Watson and equipped with speech recognition. There is an app as well as a parent dashboard online as control panel for the adults. The toy cannot be purchased in Austria. (4) A car with an app to record videos and pictures (SpyVi, Jamara): The car is connected to an app which builds up a network on its own. The network is password-protected, but the password is the same for all devices sold and may not be changed. The toy records videos and pictures; the device is the remote control. (5) A robot with speech recognition and an app (i-Que, Vivid): The robot has been numerously criticized by consumer agencies for its lack of data security. The toy is connected via Bluetooth with the app, there is no password. The analysis of the case studies shows that the protection of the data and the privacy of children is not yet sufficiently met by developers. Currently, toys are being sold, which do not conform to data protection law and basic data security principles.
Results
If a child plays with a toy which processes data, Austrian data protection law will apply. This also implies that during holidays in non-EU countries other laws may apply. Data protection concerns personal data, which allow to identify a child. In the context of the internet of toys, this does not merely include the name of child or its address but may be also information on daily routines, pictures, videos or audio recordings. The processing of personal data in the internet of toys is legal only if it is necessary to the core function of toy. It is unclear whether parents may legally give their accordance to further processing of data. Thus, it may be said: Any publication, further recording and processing of play data is presumably forbidden under Austrian law. The study shows that the development of smart and connected toys is at its beginnings – though, it needs to be taken seriously as previous data leaks and currently sold products prove. To explore the implications nine expert interviews and literature was analysed. The results shed light on the concerns of psychologists and pedagogics with respect to a robotization of childhood, but also on the criteria of toys which make sense for children.
Ultimately, the following seems essential:
• There is the need to raise awareness of parents for the issue It is very difficult to assess whether a toy sold is secure – parents need support to be equipped with the knowledge to recognize smart and connected toys which will not harm their child. Therefore, the study has developed a folder as well as an online panoply of advice. Also, this relates to retailers which may support parents in an informed choice with a fact-sheet. In the long term it will be essential to develop parenting strategies on how to deal with these toys as new digital media. Questions should be for instance where and when a toy with speech recognition is used. Also, it is necessary to accompany children when they play with devices answering to their questions – as speech assistants these toys do not function without raising questions.
• There is the need for developers to ensure secure toys
Despite the media coverage criticizing the lack of data security in the “internet of toys”, the study shows how toys fail basic security standards with respect to data processing. Children should not be used to test speech recognition and networked objects, there is the need to further strengthen the importance to pay special attention to protecting children and their play." (Österreichisches Institut für angewandte Telekommunikation öiat, 2018, 10-12)