©Wydawnictwo UR 2019
ISSN 2080-9069
ISSN 2450-9221 online

„Edukacja – Technika – Informatyka" nr 1/27/2019
www.eti.rzeszow.pl
DOI: 10.15584/eti.2019.1.21

**ANNA RYWCZYŃSKA**[1], **PRZEMYSŁAW JAROSZEWSKI**[2]

# Influence of the Use of Digital Technologies on the Physical Activity of Children Aged 7–17 Years in the Opinion of Parents

[1] M.Sc., NASK – National Research Institute; SWPS University of Social Science and Humanities, Polska
[2] M.Sc., NASK – National Research Institute, Polska

**Abstract**

Toys with integrated technology are not a new thing. We are familiar with talking dolls or remote control cars. However, the interactive toys connected to the internet, which has appeared in recent years, and which are the natural consequence of the development of the internet of things, may bring a revolution to the world of children. Following article is the result of the research project „Internet of Toys a support or a threat to child's development?" aimed at verifying the readiness to introduce digital toys as well astesting what is the level of security associated with the smart connected toys usage. A mixed methods research: pilot qualitative study in the form of interviews concerning various attitudes and practices relating to the use of digital devices, in particular connected smart toys, together with a quantitative study, gave an overview on the smart toys popularisation and the level of knowledge about their safety. Moreover, tests over selected products from the viewpoint of cyber threats and precautions implemented bythe vendor made it possible to come up with safety recommendations for future or present smart connected toys users. Communicative companions may bring not only fun and education, but also a dose of threats. What happens to the data collected by the toys, how easy it is to reach unauthorised access to the device and who potentially may come into these data possession? Last but not least this article tries to answer the questions on what consequences might bring to children social development, permanent parental supervision,restrictions of children's privacyand the possibility that digital toys might become a replacement of a real participation in the child's life.

**Keywords:** Internet of Toys, Internet of Things, smart connected toys, privacy, vulnerabilities, children safety online, security, research, family, education, awareness raising

## Introduction

Toys integrating technologies are not new. Embedding advanced technological functions, including microprocessors which ensure interactivity during play, already has a long tradition. Talking dolls or remote-controlled racing cars are widely known. Such toys (as, for instance, AIBO dog-robot or Tamagotchi) were created as early as at the end of the 20th century. However, smart connected toys appearing in recent years, as a natural continuation of the Internet of things (IoT), may revolutionise the children'sworld of toys. Communicative

companions–while ensuring an attractive way of spending their time, supporting education, and teaching technologies–also introduce considerable challenges, mainly in the context of privacy and data protection. Since toys based on the Internet infrastructure and mobile technologies are potentially susceptible to all problems, involving cybercrime, they create new challenges relating to children's cognitive development.

The problems concerning the Internet ofthings were initially related mostly tosecurity of ICT networks. It was dueto the Internet of toys that it becameapplicable to children's safetyon-line. In December 2016 FOSI (Family Online Safety Institute) published the document titled Kids and the Connected Home: Privacy in the Age of Connected Dolls, Talking Dinosaurs, and Battling Robots in which the landscape of the smart toy world is analysed from the viewpoint of safety and the grounds to apply the rights provided for in COPPA (Children's Online Privacy Protection Act, 2000) towards toy manufacturers and suppliers of technologies implemented in them. The said report also presents aninitial typology of interactive toysdividing them into three categories:

- **smart toys**–toys containing elementsof 'artificial intelligence', i.e.ability to learn, process informationreceived from a child, etc.–but conductingall local analyses withoutsending any data to an externalservice centre;

- **connected toys**–sending data(e.g. photos, audio files) to an externalservice centre, but not containingelements of 'artificial intelligence';

- **connected smart toys**–combining the features of both abovementioned groups; using resources of external service centre (where the data collected by a device are sent) to communicate with the user.

Taking into account potentialthreats that may result from the factthat you have a smart toy, it seemed very important to make a conscious decisionwhen buying it. That was a purpose of the project conducted within the framework of the NASK – National Research Institute that aimed at providing potential customers with tips and recommendations on smart connected toys by preparing a guidebook based on research and product testing.

**Internet of Things**

The so-called Internet of Things (IoT) is a concept in which devices of every-day use are connected with one another, usually in a wireless way. This allows them to exchange data and often provides remote control mechanisms in a full or restricted scope. Such definition is obviously very general and consequently somewhat problematic in use. First of all, the spectrum of 'things' included in the Internet of Things is very wide. On the one hand, we have devices used in industrial systems: robots, smart gauges or switches. On the other hand, there are gadgets for individual consumers: watches, TV-sets, washingmachines or, finally, toys.

**Children—first consumers of new technologies**

Digital technology nowadays constitutes an inseparable part of everyday life and accompanies almost all activities we undertake, either in our professional or private life. Children grow up in the environment of digital technology virtually from their birth and the average age they start to use the Internet on their own is 9–10 years of age. Over 93% of Polish teenagers stay practically non-stop on-line (Survey: Nastolatki 3.0, 2016), and almost 80% households have access to broadband Internet (GUS, 2017). Over the last few years a dynamic growth in using mobile technologies by children and teenagers has been observed. Tablets and smartphones increasingly often replace desktop computers. More than 30% stay on-line almost all the time through their mobile phones (Nastolatki 3.0, 2016). Social media are developing, strongly embedded in the mobile Internet sphere, as well as robotics, VR/AR (Virtual Reality/Augmented Reality) – the most quickly developing in theentertainment sector, but more and more frequently used in education – or AI (Artificial Intelligence) which is anticipated to revolutionise the industrial world.

The Internet, which gives a vast space for relationships and data ex-change, may also expose users to such threats as: loss of privacy, exposure to dangerous contacts, harmful content, including those calling for risky behaviour and those disseminating false information (the so-called fake news). Internet-related risks include also issues concerning dysfunctional use of the network, among others, leading to Internet-addiction.

Even properly selected information from the Internet may negatively impact child's development, if it is introduced to their world too early or too intensely. Children whose cognitive experiences are limited only to screen-equipped devices that begin to replace their regular plays and different interactions with others and perception of the real world with all senses, are even exposed to disorders in the development of neuron structures in the brain. Nevertheless, results of studies (The Use of Mobile Devices by Small Children in Poland, 2015) are alarming: over 40% of 1-year and 2-year olds in Poland use tablets or smartphones, and among these every third child uses mobile devices every day or almost every day and much longer than recommended. In the context of recommendations issued by the World Health Organisation, stating that children below two years of age should not have any access to devices equipped with screens, it is clearly observed that digital world enters children's lives in a revolutionary manner, and frequently this process lacks conscious management on the part of their parents.

In that article we try to cover a new phenomenon in the context of children's safety in the Internet–the interactive connected toys and 'machine learning'. The issues may be divided into two main groups:

- aspects relating to technological threats,
- aspects relating to social threats.

The intersection of the groups involves the area relating to privacy, since it may be the subject of actions undertaken by cyber criminals. On the other hand, the toys themselves are recording various interactions, including conversations between the child and the toy, and make them available to parents (or other users of the application) without knowledge or consent of the users (i.e. the children). Hello Barbie, one of most developed smart connected toys, even enables them to publish their children's recorded conversations in a social portal. And all this can happen when, in the majority of cases, the children do not realise at all that their conversations with toy friends are recorded.

**Perception and popularity of smart devices in Poland. Quantitative and qualitative studies**

Almost 25 billion IoT devices are expected to be in use globally by 2020, and in the opinion of experts over 70% of households will be equipped with such devices by 2025 (forbestechcouncil, 2017). In order to determine a current distribution ofsmart devices in Polish households, with a particular attention to the popularisation and knowledge about the Internet of Toys, quantitative and qualitative studies were conducted in mid-2017 which gave a broader overview of the perception and spread of IoT technologies.

The quantitative studies were conducted twice. The first study showed the respondents had difficulties to define items belonging to the Internet of Things. It seems that marketing campaigns and rhetoric describing the devices as 'smart', when in fact referring to specific functions of an appliance (e.g. fast cooling of beverages), make their owners believe they are part of Internet of Things.

The study showed that the most common holders of smart TV (the most common smart appliance in Polish households) are persons belonging to the age group 45–55, living in small and medium-sized towns. People living in medium-sized towns (20–99 thousand inhabitants), aged 25–44, are also the most common holders of smart alarm systems. Smart toys are rather rare at present and their holders are most frequently people with higher education level, aged 35–45, and living in big cities. Interviews with the families confirmed the fact that people who have smart devices very often are not aware what it means. There is also nocorrelation between the fact of having a smart device and having knowledge about other IoT devices.

Another aim of the study was to check how the respondents feel about development of the smart toys market. Neutral and positive attitudes are predominant, though almost 30% show great concerns.Interestingly, respondents thought that the lowest risk involved direct loss of money, e.g. a bank account compromise or stolen credit card information. The qualitative studies also indicated a rather neutral attitude towards the development of Internet technologies in the

context of toys, whereas almost all of the answers were marked with certain doubts. The parents most often paid attention to the issues involving the protection of children's privacy, they were afraid that such toys may provide false emotions to their children and that potentially each child may be exposed to dangerous contacts. The negative evaluation of smart toys involved also concerns about killing children's creativity.

Most respondents (65.5%) regarded safety as the most important, but the question is to what extent attention paid to safety refers to physical aspects of toys (the risk of swallowing by small children, no adequate attestations), and to what extent it will also include the problems relating to Internet security. It should be noted that the interviews were conducted in Polish, where 'security' and 'safety' are described by the same word. It is therefore hard to determine which of the two the respondents had in mind.Based on answers to the question concerning the frequency of talks conducted with children about Internet security, it may be stated that this subject is still not mentioned in many households (15.1%), or it is very rare 38.5%). Parents admitted they could not conduct such talks, and that they should know more about the subject and have the ability to adjust the scope of the talk to their children's age.

An alarming fact consistently showing in responses is that the parents pay little or no attention to terms and policies regarding products and online services they buy.

**Smart toys under scrutiny. Tests and analysis of the issues**

This article is focused on smart toys connected to the Internet. The connection usually means a certain type of interaction with the services available on the server belonging to either the manufacturer or to a cooperating third company. In case of each toy, the details concerning the interaction may look completely differently. Usually, however, the majority of raw data collected from the environment are sent to be processed on the server. Thanks to the fact that the analysis is made outside the toy, the toy itself does not need a high computing power. Nevertheless, as it can be easily figured out, such a model may pose a potential threat to our privacy. In order to check how secure such toys are in practice, authors played the role of consumers and bought smart connected toys (Hello Barbie, Barbie Hello Dreamhouse, Fisher Price Smart Toy Monkey, CogniToys Dino) for testing.The full report on tests and outcomes is available in the guidebook "Internet of Toys – a support or a threat to child's development".

Normal working cycle of a smart connected toy consists of:

- Collecting data from the user. The toy records the sound, image or accelerometer readings and sends them to the server (sometimes partially processed).

- Data processing on the server. Depending on the particular toy, for instance, a graphic symbol analysis or full voice recognition may be performed. The software on the server generates a response (e.g. a voice message, a command for the toy to perform a certain action that the script version of the story told) and sends it to the toy. So, this is what the 'smartness' of the toy is embedded in.
- Presentation of results. Playing recorded voice response, music, performing an action etc.

During tests, we set up a small laboratory. The virtual machine that acted as a router had also DHCP server installed and running, as well as a DNS server, an HTTPS proxy (generating SSL certificates on the fly), and a packet sniffer. The wireless router was configured to act as a network switch, providing no services on its own.For the purpose of the study we have identified as well several surfaces of attack, i.e. scenarios or use cases where one or more vulnerabilities may allow to steal data, alter firmware or otherwise technically abuse the toy, however, the list was not meant to be exhaustive.

- Communication between the toy and its companion application
- Update mechanisms
- Interception and modification of data exchanged between the toy and the server

Smart connected toys send lots of data to a cloud server operated by the manufacturer (or a contracted third party). If this data can be intercepted or manipulated, the consequences may include theft of data, eavesdropping on conversations between a child and the toy, altering toy's responses as well as tampering with firmware updates. The technique used for such purposes is called a "man-in-the-middle" attack (MITM) and involves traffic manipulation such as ARP poisoning in local networks or DNS hijacking over the Internet.

Most toys were using TLS for encryption. During one of the tests, all such traffic was routed to the local proxy which would reply with a fake certificate in an attempt to decrypt communication. As expected, toys failed to connect to our fake cloud server.

One of the tested toys: CogniToys Dino does not encrypt full communication between the toy and the cloud. Instead, it uses SIP to set up a voice call, and encrypts the voice messages with AES. This approach causes several problems. First of all, the auto update process is performed in plain text, allowing for easy acquisition of firmware as demonstrated below, as well as for injecting of own files. Further on, Valente and Cardenas (2017) have discovered at least three weaknesses of the VoIP encryption in CogniToys Dino, leading to possibility to replay communication using another Dino device or even to eavesdrop live communication.

- Protection of user data on the server

Some toys, like Hello Barbie, send a lot of private data to the server (especially full voice recordings of conversations) and store it there. While this fact itself can be disturbing, it is crucial that the storage is adequately protected.

**Physical safety of the toy**

One of many aspects concerning the broadly understood safety of 'smart toys' is the possibility to get a physical access to elements responsible for communication or data storage. This is especially applicable when such a toy originates from the secondary market. On the other hand, when the toy has been lost or stolen, the new owner might retrieve sensitive data from the device. There is also a possibility that somebody may insert additional functions to the toy, enabling-for instance-to eavesdrop children during their play or household members who are within the scope of the embedded video camera or microphone. The laboratory tests showed the risk of buying used toys if one do not fully trust the seller. The toy may have been modified, for example in order to send data not only to the manufacturer. Moreover it seems very important to remove data from the toy by restoring the device back to factory default status before selling the item.

**In legal experts' eyes**

A vast number of smart toys currently available on the market are manufactured by entities with their registered offices in the US, based on American legal regulations concerning privacy and personal data protection. The toys purchased for test purposes were also bought in the US. For that reason, they do not fully correspond to the regulations valid in the European Union, including Poland. The level of personal data protection and their privacy within the territory of the US is, basically, lower than in the European Union, either taking into account the current legal status, and the EU-wide reform of the personal data protection system which entered into force in May 2018. Before the purchase the aware and detailed analysis of the privacy policies provided by the toy's producers should be conducted.

Results of the research and tests clearly show the need for awareness campaigns explaining the ideas, workings, and challenges of the Internet of Things. It seems crucial to primarily describe the technological issues of smart devices, to present risks specific to smart connected toys, and to offer parents and carers tangible advice concerning conscious introduction of IoT technologies into child's life.

## Literature

Children's Online Privacy Protection Act (COPPA). Retrieved from: http://www.coppa.org (1.04.2000).

Family Online Safety Institute, "Kids and the Connected Home: Privacy in the Age of Connected Dolls, Talking Dinosaurs, and Battling Robots" (2016). Retrieved from: https://www.fosi.org/policy-research/kids-connected-home-privacy-age-connected-dolls-talking-dinosaurs-and-battling-robots/ (9.09.2017).

FBI's Internet Crime Complaint Centre. Retrieved from: https://www.ic3.gov/media/2017/170717.aspx (9.02.2018).
GUS (2017). *Information Society in Poland in 2017*. Retrieved from:
https://www.forbes.com/sites/forbestechcouncil/2017/06/06/best-smart-home-devices-and-how-iot-is-changing-the-way-we-live/#578e929b43bd (3.10.2017).
https://www.theguardian.com/sustainable-business/2016/feb/05/big-mother-gps-tracking-technology--threat-privacy-childhood (12.02.2018).
*Juniper Research (2017).* Smart Toys: Market Summary.
Kahn, P.H. Jr., Shen, S. (2017). NOC NOC, Who's There? A New Ontological Category (NOC) for Social Robots. In: N. Budwig, E. Turiel, P.D. Zelazo (eds.), *New Perspectives on Human Development* (p. 13-142). Cambridge University Press.
Shanyang Z. (2006). Humanoid Social Robots as a Medium of Communication. *New Media & Society, 3*, 401–419.
Survey: Nastolatki 3.0, NASK (2016).
The Use of Mobile Devices by Small Children in Poland (2015). Millward Brown Poland for FDN.
Turkle Sherry, Alone Together, Basic Books (2011).