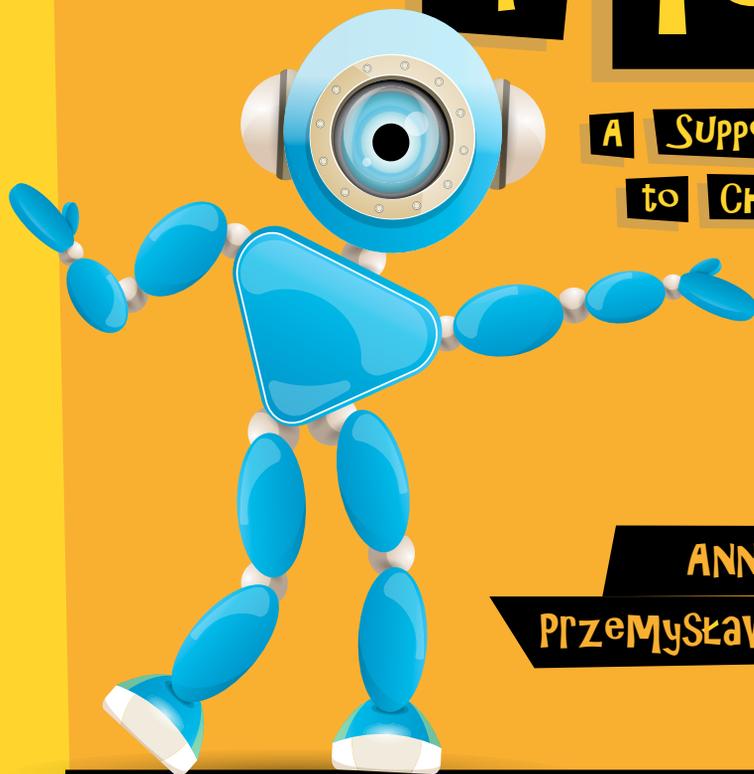




iNtErNet

OF TOYS

**A Support or a Threat
to CHILD'S Development**



ANNA RyWczyńska

Przemysław JAROSZEWSKI

NASK

iNtErNet

oF

TOyS

A Support or a Threat

to CHILD'S DeVeLopMent

NASK

1. 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's

world 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, data protection, as well as taking into account the social context. 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.

Internet of Toys constitutes one of the most dynamically developing sectors of economy. According to the Juniper Research report¹, in 2017 the total number of commercial parcels including smart toys was respectively (in millions):

118.2 America

52.5 Europe

53.3 the rest of the world

In China an increase by 47% is expected annually, on average, until 2022, which will correspond to 18% share in the global smart toy parcel market.

¹ Juniper Research, *Smart Toys: Market Summary* 2017.

The problems related to Internet of things were initially related mostly to security of ICT networks. It was due to the Internet of toys that it they became applicable to children's safety on-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*) towards toy manufacturers and suppliers of technologies implemented in them. The said report also presents an initial typology of interactive toys dividing them into three categories:

- **smart toys**—toys containing elements of 'artificial intelligence', i.e. ability to learn, process information received from a child, etc.—but conducting all local analyses without sending any data to an external service centre;
- **connected toys**—sending data (e.g. photos, audio files) to an external service centre, but not containing elements 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.

In July 2017 the FBI's Internet Crime Complaint Centre issued a warning on its web page. It was aimed to encourage consumers to consider cyber safety before introducing smart, interactive, Internet-connected toys to their homes. In case of smart toys, many questions still should be answered, including: how the safety of data (frequently sensitive data) collected by devices looks like? What happens to them? How are they protected? Who can access them? How can another person take control of them? Taking into account potential threats that may result from the fact that you have a smart toy, it seems important to make a conscious decision when buying it. We hope this guidebook will help you. Its content is the result of a project realised within the framework of the NASK National Research Institute titled 'Internet of Toys—a Support or a Threat to Child's Development.'

The project included:

- a pilot qualitative study in the form of interviews concerning various attitudes and practices typical for people with various levels of capital (economic, cultural), relating to the use of digital devices belonging to the category of the Internet of things (IoT), in particular connected smart toys;
- a pilot quantitative study checking the level of smart toys popularisa-

- tion and the level of knowledge about their safety;
- tests involving selected products from the viewpoint of cyber threats and precautions implemented by the vendor,
 - including information on privacy and safety provided by manufacturers before purchase and in the inside packaging,
 - in technical terms: the types of transmitted data, place where they are stored and processed, their protection (e.g. encryption) and its

correct implementation, as well as the availability and efficacy of protection against undesirable content.

The aim of our guidebook is to familiarise potential purchasers with the problems concerning smart toys. The presented definitions of notions and phenomena, descriptions of functionalities and recommendations should facilitate the use of IoT technologies at home, including interactive connected toys.

2. 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. It is used for shopping, making payments, booking holidays, communication, and keeping in touch with our friends. It is also part of our work, and is used to acquire information and knowledge. 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-line², and almost 80% households have access to broadband Internet³. 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 phones⁴. 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 the entertainment sector, but more and more frequently used in education—or AI (Artificial Intelligence) which is anticipated to revolutionise the industrial world. The IoT solutions are becoming more and more popular. They make it possible to collect, process, and exchange data between items through the computer network.

The digital revolution phenomenon is considered in the social, as well as educational and economic aspects, and the global economic situation is simply conditioned by the information society development. Complex and attentive approach to synergization of technology with other spheres of life, and development of digital competences based on solid educational foundations may bring about equalisation of opportunities and standards of living in the society. It is thus extremely important to implement technologies to children's life in such a manner so as they could use them to satisfy their developmental and social needs—while growing up surrounded by digital devices. The de-

2 Survey: *Nastolatki 3.0*, NASK, December 2016.

3 GUS [National Statistical Office] report: *Information Society in Poland in 2017*.

4 Survey: *Nastolatki 3.0*, *ibid*.

velopment of global network involves not only opportunities, but also challenges concerning safety of its users. The Internet, which gives a vast space for relationships and data exchange, 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 studies⁵ 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.

The guidebook covers 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:

The intersection of the groups involves the area relating to privacy,

1. ASPECTS RELATING TO TECHNOLOGICAL THREATS,

PRIVACY

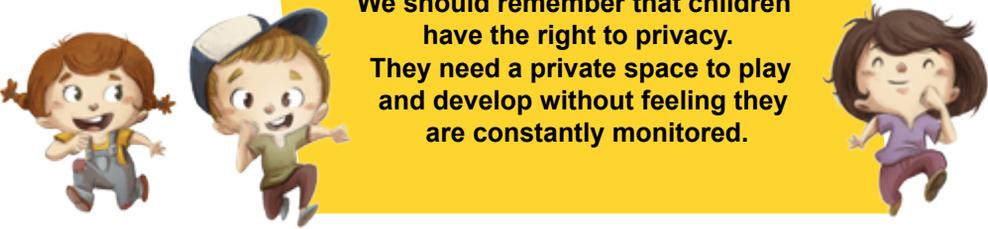
2. ASPECTS RELATING TO SOCIAL THREATS.

⁵ The Use of Mobile Devices by Small Children in Poland, Millward Brown Poland for FDN, 2015.

since it may be the subject of actions undertaken by cyber criminals, who are able to create a false identity by accessing data recorded in children's toys and use it for illegal purposes. 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). The perspective of parents' entering their child's privacy zone was discussed during the Internet Governance Forum in 2016 by a world-famous expert in the subject, John Carr. In his speech he indicated the possible impact of connected toys on relationships inside families through the use of toys as substitutes of real participation in child's life. This problem is also emphasised by Professor Sherry Turkle in her book

*Alone together*⁶.

At the same time, it is worth taking note of an additional aspect of children's privacy, connected with the development of the Internet of things, namely the so-called wearable technologies—that is clothes and accessories with embedded computer and advanced electronic technologies⁷. Many experts believe that⁸ such products, which seemingly are to increase child's safety, may as a consequence restrict children's privacy and personal freedom, at the same time encouraging them to accept supervision. On the one hand, it is natural that parents want to take every opportunity to protect their children, but too much developed surveillance, awareness of permanent monitoring on the part of the parents and teachers may have a significant impact on young people's behaviour and development.



We should remember that children have the right to privacy. They need a private space to play and develop without feeling they are constantly monitored.

6 Turkle Sherry, *Alone Together*, Basic Books 2011.

7 Acquired from: <https://pl.wikipedia.org/wiki/Wearables>. Access from 10.02.2018.

8 Acquired from: <https://www.theguardian.com/sustainable-business/2016/feb/05/big-mother-gps-tracking-technology-threat-privacy-childhood>. Access from 12.02.2018.

A very interesting perspective concerning privacy in children's interaction with smart toys and parents' approach to the opportunity to listen to and monitor children's conversations was described in the pilot studies conducted by experts from Washington University 'Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys'. The study involved eight interviews with parents and children (aged 6–10), during which they were introduced to the workings of Hello Barbie and Cogni-Toy Dino. The parents' observations concerning the purport of recording talks their children have with the toys

were very interesting; they wondered how they could make use of them at all. They thought that they would be able to learn about their children's possible problems, the ones that a child did not want to talk about directly, or to hear the words they did not want them to use. However, on the other hand, they started to imagine their own reaction, how they personally would feel, if they were recorded without their knowledge. The web account for parents which accompanies Hello Barbie even enables them to publish their children's recorded conversations in a social portal. And all this can happen when,

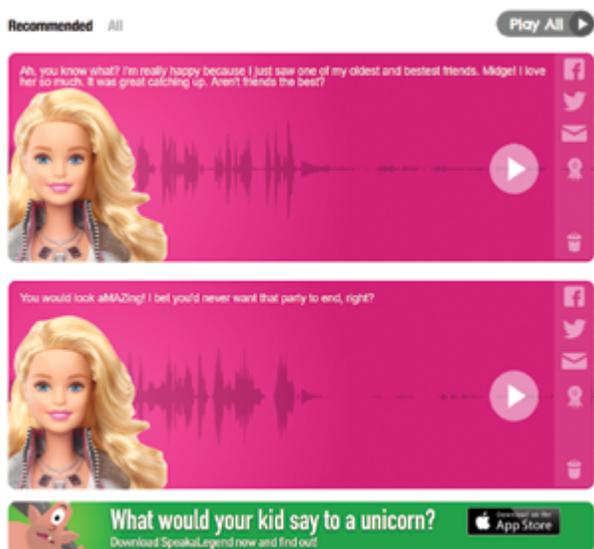


Fig. 1. Parents' panel. On the right there are icons that enable them to publish recordings in the social media

in the majority of cases, the children do not realise at all that their conversations with toy friends are recorded. Most of the children participating in the interviews did not know that their parents could listen to their conversations with Barbie. One child, when found out that the doll recorded the conversations, became even scared. One of the recommendations from the study involved the suggestion that children should be able to listen to their recordings directly from the doll's 'interface'. Everybody agreed that manufacturers and parents had to notify children about all functionalities of the toys.

Social aspects of smart toys are also related to the impact smart toys may potentially have on the ability to build authentic interpersonal relationships by children (the ones based on, *inter alia*, empathy, sensitivity, responsiveness, attentiveness, self-knowledge, reciprocity, interest) and⁹ on children's cognitive development. An extremely interesting perspective for these considerations was presented in the studies¹⁰ based on an experiment involving ninety children aged 9–12 and 15. The study used a Japanese Robovie robot. The majority of children taking part in the experiment recognised the

robot as a social being, who you can make friends with, share secrets with, who has got its own intelligence. 33% of the children would like to give the robot voting rights, and 54% of them thought it was not fair to close the robot in the box if the robot does not like it. Children aged 9–12 showed a much higher tendency to personalise the robot than 15 year olds.

The studies indicated a strong tendency on the part of children to build an emotional relationship with smart devices and trust them. Hence, there is an enormous threat that the child may potentially interact with somebody who is able to take control over the toy, using a remote communication protocol, such as Bluetooth. A stranger might also learn about the secrets that the child shared with a digital friend. On top of that, children may be exposed to hidden commercials implemented in the toy (e.g. Cayla doll mentions popular snacks and sweets in its interactions with children). That is why it is very important that parents are careful when introducing smart toys to their children's world, take care about the proper balance in their social activities and protect their children's privacy.

9 Kahn Peter H. Jr., Shen Solace, *NOC NOC, Who's There? A New Ontological Category (NOC) for Social Robots*, in: Nancy Budwig, Elliot Turiel, and Philip David Zelazo, eds., *New Perspectives on Human Development*, Cambridge University Press, 2017, p. 114.

10 *Ibid.*, p. 106–123

Balance is crucial



Potential consequences for cognitive development¹¹:

- ☞ support in learning:
 - knowledge personalised for the child,
 - incessantly updated by a self-learning teacher
- but
- ☞ risk of an educational bubble:
 - fragmentation of knowledge, being lost in affluence, algorithmic learning,
 - risk of hidden marketing effect on children

Potential consequences for identity development:

- impact on the perception of human–human relationships in the context of man–robot relationship (Shanyang 2006)¹²,
- transcendence: smart toys as a new ontological category (Kahn et al. 2013),
- changes in the perception of privacy,
- smart robots/toys as supervising devices.

Potential consequences for relationship development:

compensation for unsatisfactory relationship in the real world (e.g. Kahn et al. 2013),
 functional diversification of relations,
 teaching the child the master–servant relationship (e.g. Kahn et al. 2013),
 loss of relationship authenticity (Turkle 2007).

¹¹ Influence tables on children’s development presented at the Safer Internet Forum 2017 by dhr. prof. dr. J. (Jochen) Peter from the Amsterdam School of Communication Research/AscorR

¹² Shanyang Zhao, ‘Humanoid social robots as a medium of communication’, *New Media & Society*, 2006 (3), p. 401–419.

3. Internet of Things

The so-called Internet of Things (IoT) is a concept in which devices of everyday 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, washing machines or, finally, toys.

Vehicles also become part of the Internet of Things (often connected with fleet-management systems), as well as traffic lights, buildings and their individual sub-systems, such as alarms or air-conditioning... Each of the groups is completely different. In case of industrial systems, the priority will be uninterrupted operation, since a failure of a power plant block or a sewage treatment plant may cause serious consequences. For the manufacturers of TV-sets or toys the most important element will involve the implementation of new functions which may attract purchasers, and make it possible to build a competitive advantage.

Very diverse are as well the technological solutions used by smart device manufacturers—starting from designs and computing platforms, through operating systems and radio communication protocols, as well as ways to store and transmit data. For instance, for an initial configuration many consumer solutions use Bluetooth Low Energy, Wi-Fi Direct or NFC (and traditional Wi-Fi during normal operation), most often with the use of a smartphone.



Finally, the borderline of the Internet of Things is rather symbolic and fluid. Smartphones may be a good example here. Basically, they should be included into the group of IoT devices (as, nomen est omen, 'smart telephones'). On the other hand, they constitute such mature solutions and are equipped in enormous computing power that we learnt to treat them as a new class of portable computers, where using the GSM network for voice calls is just one of all the available functions.

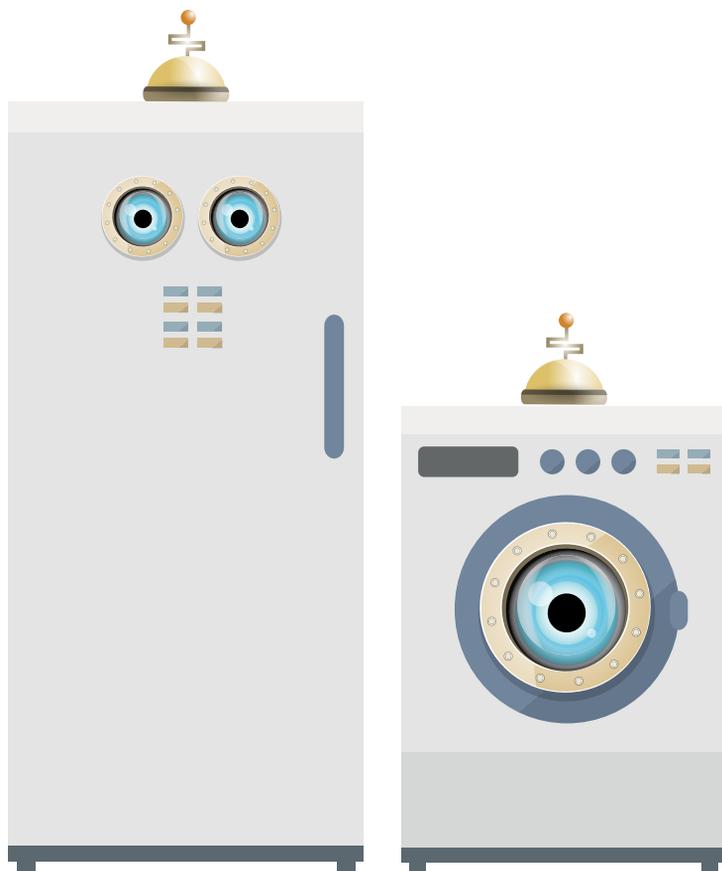
Consequently, treating the Internet of Things as a whole makes limited sense in particular when talking about its technical problems. Nevertheless, below we made an attempt to highlight the most important classes of problems common for smart connected devices.

Limited resources at the production stage: when designing the IoT devices, it is usually necessary to take care about their compact size and energy efficiency. It may lead to a compromise between security (for example, using security strong cryptographic algorithms) and implementation of additional functions. From the manufacturer's perspective, time is also a vital resource. Any delay in marketing a new model of a product may mean losing a market share. They may be thus tempted to limit the tests, including the ones related to IT security.

Components re-use such elements as network cards, BLE cards, video cameras, etc. are usually used in many similar devices manufactured by various vendors. The same applies to programming libraries used in the device's software. In case of some cheap smart devices, products of various brands may differ from one another basically only with casings and visual elements of the user's interface. Hence, finding that a feature is vulnerable in one of the typical elements has effects on many products.

Firmware updates: In order to fix an error in the device's software, a new version must be published by the manufacturer, and then downloaded and installed by the consumer. This update process may be either automatic or manual. In the latter case, users have to periodically check the manufacturer's webpages for firmware updates and install them on their own. In any case, the manufacturer must ensure that consumers can verify the patch comes from a trusted source, and was not modified in any way. Another significant problem involves the fact that the availability of possible software updates after product purchase depends on the time the producer will support the product. In case the producer thinks such support is not profitable, it may turn out that we are left with the product that will not be repaired at all.

It is worth noting that such problems basically refer to all smart devices, regardless of whether they are Internet-connected (i.e. they are elements of IoT) or not.



4. 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 2020¹³, and in the opinion of experts over 70% of households will be equipped with such devices by 2025¹⁴.

This dynamically developing branch of technology becomes more and more popular in Poland. In order to determine a current distribution of

Internet of Things, defined as a next stage of digital revolution, enters every part of everyday life and industry. We speak about IoT, among others, in terms of smart economy, smart city, smart transportation, smart health or smart home.



zdj. Fotolia.com

smart 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.

13 <https://www.gartner.com/newsroom/id/2905717>.

14 <https://www.forbes.com/sites/forbestechcouncil/2017/06/06/best-smart-home-devices-and-how-iot-is-changing-the-way-we-live/#578e929b43bd>.

QUANTITATIVE STUDIES

The study performed with the use of Ariadna panel involving Polish Internet users across the country, composed of N=1051 people. Quotas reflecting population aged 18 and over, grouped by sex, age, and town size. Period of study: 8–11 September 2017. Method: CAWI, and

The study performed with the use of Ariadna panel, involving Polish Internet users across the country, composed of N=1047 people. Quotas reflecting population aged 18 and over, grouped by sex, age, and town size. Period of study: 15–11 September 2017. Method: CAWI.

QUALITATIVE STUDIES

The study performed with the use of an in-depth interview (IDI) between July and September 2017. The interviews were conducted in places of respondents' residence or their temporary stay. It was particularly important in order to conduct observation studies, confront the provided information with the situation accompanying the interview, take into account the information concerning popularisation and use of electronic devices resulting from interior designs, presence of devices within sight during the interview etc.

24 interviews were performed with families selected according to the guidelines of the matrix, assuming diversification according to the place of residence, education level, number of children, and number of parents in the family (both parents/sole father/mother)

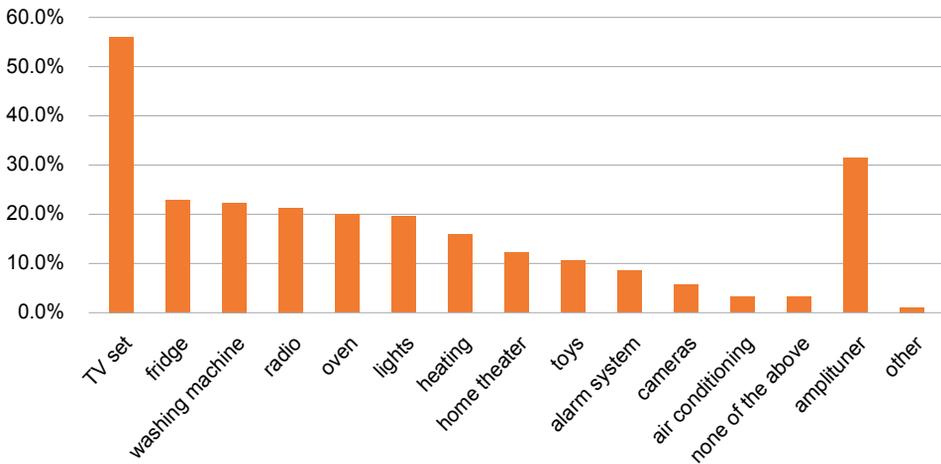
Is my fridge smart?

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 refer-

ring to specific functions of an appliance (e.g. fast cooling of beverages), make their owners believe they are part of Internet of Things.

An example is shown in the below chart presenting answers to the first question asked in the first edition of the studies.

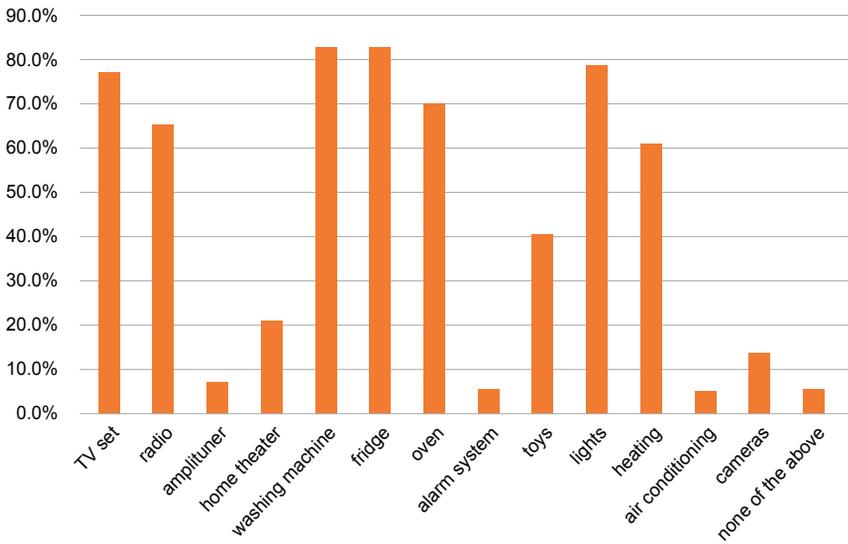
Which of the following devices are in your household and have an Internet connection or can be connected to the Internet, i.e. they are 'smart' devices?



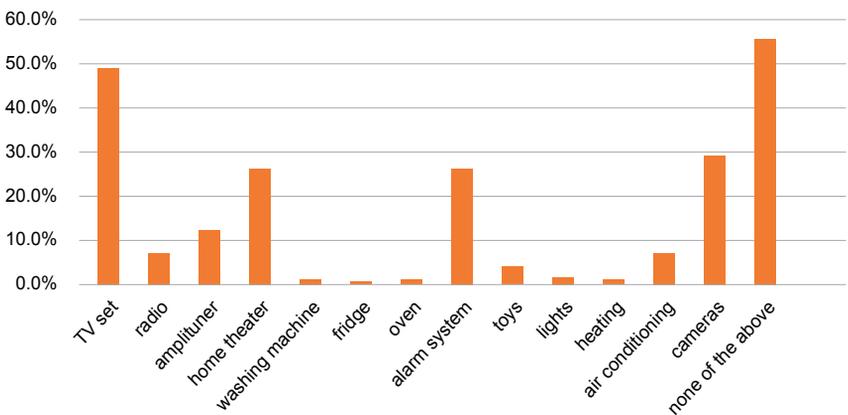
The obtained answers and high possession ratios of smart devices required another study to be performed,

in which the first question was divided into two complementary questions:

Which of the following devices are in your household?



And which of the devices in your household are connected to the Internet?



As it can be observed, after asking directly whether a given device is Internet-connected, the obtained data indicated a much lower distribution of IoT devices in households than resulted from the first panel. When analysing the data, however, one should also take into account the possibility indicated by the qualitative studies—namely, that there is a situation in which respondents have a smart device (it mainly concerns TV-sets), but they do not connect it to the Internet, and use it only as a traditional TV-set. In some cases the respondents had the most modern smart TV on the wall of their flat, but it was not connected to the Internet.

Moreover, 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.

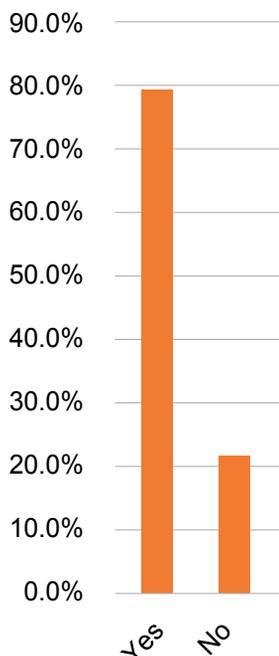
Interviews with the families confirmed the fact that people who have smart devices very often are not aware what it means. There is also no cor-

relation between the fact of having a smart device and having knowledge about other IoT devices.

Who buys and who makes decisions?

Toys are purchased by virtually all social groups, of any age. Almost 80% respondents declared that they purchased toys, out of which 95% people were aged 25–34.

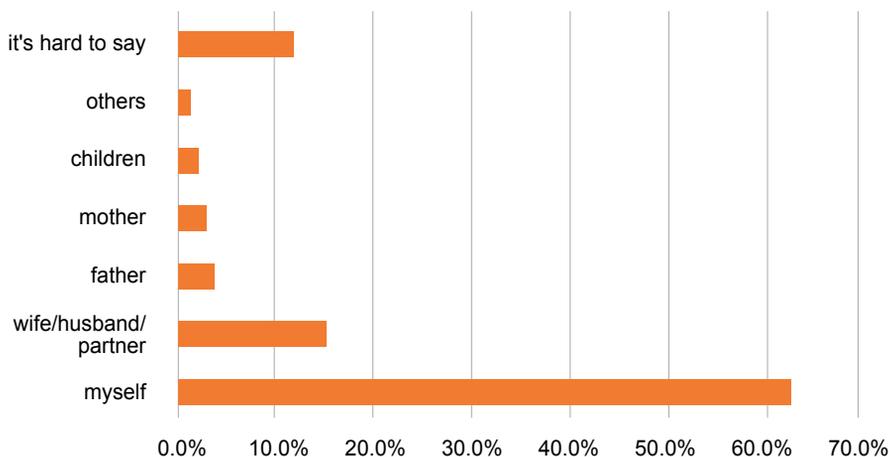
Do you buy toys for your children?

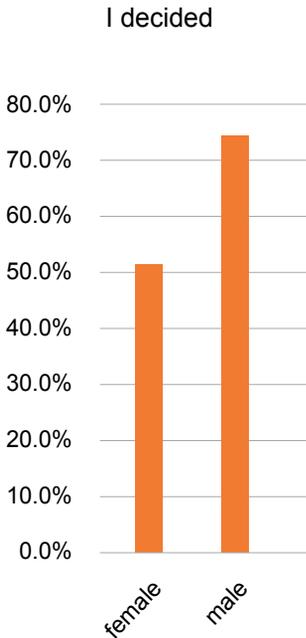


Women buy toys relatively more often (80.3%) than men (76.4%), however, it may change with regard to digital toys in the future since men tend to treat their voice more important in the decision-making process when purchasing electronic devices. The quantitative studies confirm observations from the qualitative studies. In the majority of cases, fathers are quoted as decision-making persons

for digital appliances shopping. Children are their advisers and motivators in the majority of cases. Women are mentioned as decision-makers only during interviews with sole mothers. Additionally, there occur disputable situations: the spouses do not agree on who makes decisions about purchases. Eventually, the argument to resolve the dispute was usually: who pays for the device.

Who in your household has a decisive voice when buying electronic devices?

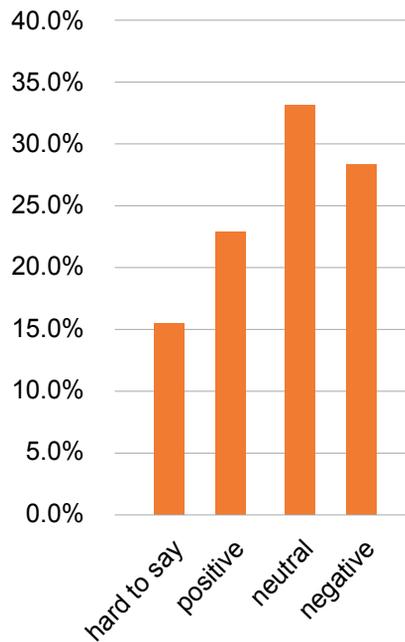




Another aim of the study was to check how the respondents feel about development of the smart toys market. The most positive attitude towards IoT development was shown by citizens of big cities; they gave 10% more of 'positive' answers to the question: How do you perceive the fact that more and more toys can be connected to the Internet? Neutral and positive attitudes are predominant, though almost 30% show great concerns.

How we evaluate IoT technology development in the context of children?

How do you rate the fact that more and more appliances can be connected to the Internet, and can be remotely managed from applications on your smartphone, tablet, or computer?

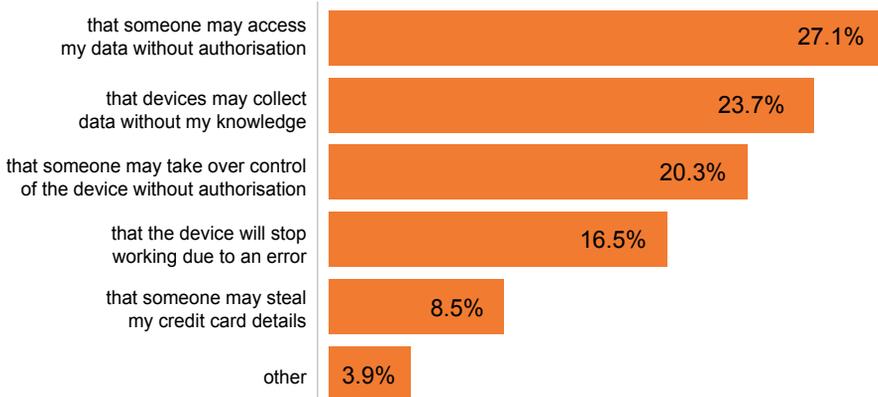


The below chart shows that the greatest concern involves unauthorised access to data. Interestingly, respondents thought that the lowest risk involved direct loss of money, e.g. a bank account compromise or stolen credit card information.

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, a risk of access to personal data; they were afraid that such toys may provide false emotions to their children and that potentially each child may be exposed to dangerous contacts. People showing a positive

attitude towards smart toys hope that they will have a positive influence on children's development, particularly in the educational context, and they believe that it is a natural consequence of digital revolution. Nevertheless, they also have certain concerns, mainly related to overuse of devices by children and the use of Internet as a time killer for young people. The negative evaluation of smart toys involved mainly concerns about surveillance, loss of privacy, and killing children's creativity. Both in the qualitative studies and in the quantitative studies it can be noted that concerns about loss of funds (i.e. potential interception of account data, logins, passwords) are not mentioned as the main risk associated with IoT devices.

What worries you the most about devices connected to the Internet?

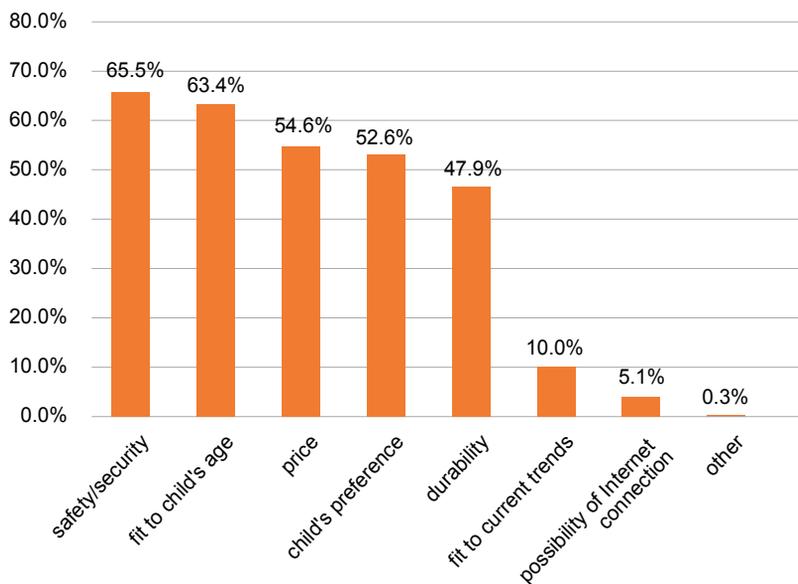


The objective of the study was also to determine the properties which are the most important for parents when choosing a toy. It was a multiple choice question. As presented in the chart, most respondents (65.5%) regarded safety as the most important, along with a large group (63.4%) who thought its adjustment to age is decisive. Price and child's preferences were given the subsequent places. Almost 50% are guided by durability when shopping, thus, it is worth paying attention to this aspect in the context of smart toys since producers

are not always willing to guarantee a longer period of toy operation.

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.

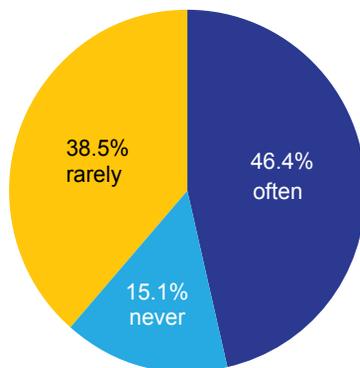
Which features of the toy are most important to you when deciding about purchase?



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%). Frequent talks with children about on-line safety are declared more frequently women (51.3%), than by men (39.1%), however, women are considerably rarely decision-makers and initiators of digital device purchases. During the interviews, parents very often replied that they had not talked with their children about safety in the Internet as they thought children knew more about new technologies and parents did not keep up with it. Parents admitted they could not conduct such talks, and that they should know more about the subject and adjust the scope of the talk to their children's age. At the same time, the majority of respondents thought that parents should be more responsible for their children's education and protection against on-line threats than school. It seems very interesting that the less the respondents knew about technologies and digital activities of children, the higher personal responsibility and role they saw, whereas persons well familiarised with the digital world and personally active Internet users thought that school should lead the way in shaping digital competences, explaining that they could see personally that parents did not keep up

with the technology. It seems like the known proverb: 'All I know is that I know nothing'—the more we get to know the Internet, the more we are aware of the potential challenges accompanying the virtual world.

How often do you talk with your child or children about the Internet safety and the potential online threats?



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. Most respondents unanimously answered that—when buying digital devices, downloading applications, using social media or other on-line services—they read neither their regulations nor the privacy policy. Regulations are read only in cases when people have concerns that

a given on-line service may involve terms and conditions payments, but still it is not a rule. That is why all parents expressed the need to be clearly informed about any functionalities and privacy policies concerning smart toys directly on the packaging or even on the toys themselves. It is worth noting that the data confirm conclusions from the previously quoted studies conducted by the Washington University during which all parents who took part in the interviews had clicked a button to agree to their children's use of the Hello Barbie doll and associated services without any hesitation or familiarising themselves with the privacy policy.

Respondents would like manufacturers to feel responsible for adequate notifications to their potential customers and protection of their data required to operate the devices. Parents also appreciate all sorts of guidebooks which could help them to take care about their children's safety in the context of digital media.

Results of the studies clearly show the need for awareness campaigns explaining the ideas, workings, and challenges of the Internet of Things. Consequently, the aim of this guidebook is primarily to 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

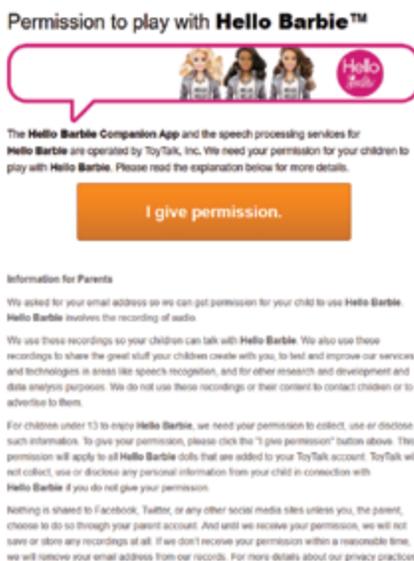


Fig. 2 Parents' consent app for having their child playing with Hello Barbie

of IoT technologies into child's life, starting from conscious purchase, as well as subsequent consistent care about children's safety in the context of protecting their privacy and social development.

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

As we have underlined above, this guidebook is focused mainly 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, we played the role of consumers and bought smart connected toys for testing.

Hello Barbie—a doll advertised as equipped with the function of interactive talk and voice recognition. It is equipped with a microphone. The child's statements are sent to the cloud. The application on the server tries to recognise from a list of several such as 'yes', 'no', conversation topics and provides an 'answer' from a list of several thousands recorded phrases. The doll is recommended for children aged 6–15.



Fig. 3 Hello Barbie doll

Barbie Hello Dreamhouse—a smart doll house. It uses mechanisms similar to those of Hello Barbie in order to use voice commands to activate various functions of the doll house (e.g. playing the music or switching the lights on). The toy is recommended for children aged 3–10.



Fig. 4 Barbie Hello Dreamhouse

Fisher Price Smart Toy Monkey—uses microphone, video camera, and accelerometer for interactive play, responding to key words, activity cards (recognition with the use of video camera) or movement (e.g. tossing up). The toy is recommended for children aged 3–8.



Fig. 5 Fisher Price Smart Toy Monkey

CogniToys Dinosaur—sends user’s voice messages to the server, the application in the cloud is powered by the IBM Watson system which generates answers in the form of natural conversations, quoting encyclopaedic data, telling jokes, singing, etc. Recommended for children over 5.



Fig. 6 Dinosaur CogniToys

Before we discuss possible problems in more detail, let us describe the manner of operation of ‘smart connected’ toys. For all the toys we tested it is possible to distinguish several stages, important from the point of view of understanding the core of their operation:

Registration in the manufacturer’s/ service provider’s server. We are usually asked to create a user’s profile before the toy’s first use. The scope of data provided at this stage varies—at least it is an e-mail address, but we may also be asked to state the child’s name and age. The profile data is stored on the manufacturer’s server.

Toy configuration is usually made with the use of a smartphone. During this process, we will have to provide, at least, a wireless network configuration (name and password) which will be used by the toy to establish a connection in the future. The information will be recorded in the toy’s memory, though it may happen that they will be then sent to the manufacturer (at least one of the toys we tested sent the name of the wireless network it used). In this way, a specific toy is connected with the user’s profile.

During normal use, the toy operates in the following cycle:

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 result. Playing recorded voice response, music, performing an action etc.

We are buying a smart toy

None of the toys we tested was available on the Polish market. We purchased them in an American on-



zofj.Fotolia.com

line shop. What is important, all toys require a smartphone application to be configured. The application may be unavailable for Polish users. Fortunately, the seller clearly informs about the fact on the packaging (see below the last line on the application accompanying Hello Barbie).

- Chat with Barbie for a whole new way to play!
- Hello Barbie doll uses WiFi and speech recognition technology to engage in two-way dialogue
- Use is simple with functionality built into her belt buckle -- press to start the conversation and release to hear Hello Barbie doll respond
- Doll must be placed in charger for initial set-up. Refer to the product description before use.
- This is a US only product. The Hello Barbie companion app can only be found in US app stores.

Fig. 7 Hello Barbie Application

From the description of the toys you learn that they are interactive and smart and that they need to be connected to the Internet (thus they are 'smart connected'). However, it is not easy to understand what their 'smartness' precisely involves, or which data are used by them. Some descriptions refer the user in small print to the privacy policy on the manufacturer's page. So, this is to some extent 'a pig in a poke'.

Custom Conversation, Safe Play

Parents and guardians are in control of their child's data and can manage this data through the ToyTalk account at anytime. For more information visit our official website or call our customer care.

Parents must also set up a ToyTalk account and connect to use the conversational features. Hello Barbie doll can remember up to three different WiFi locations and does not require a smart device after WiFi configuration. Hello Barbie doll is compatible with iPhone 5, iPhone 5c, iPhone 5s, iPhone 6 Plus, iPhone 6, iPad Air, iPad Air 2, iPad 4th generation, iPad mini 2, iPad mini 3; must have iOS 8 or above. Android mobile devices must have Android OS 4.0.3 or above. Use of Hello Barbie involves recording of voice data; see ToyTalk's privacy policy at our official website.

Fig. 8 Privacy issues of the Hello Barbie doll

When we unboxed the toys, we concluded that, after all, we were in a better situation than the consumers who decided to buy the toy after seeing it in the shop. There is hardly any information on the packaging on how the toy operates, not to mention the details about technological solutions used.

What questions should be asked, in our opinion, before we buy such toys?

- **How does the toy exactly operate?**
We may ask the seller for more information, asking for a demonstration. We may also search the Internet for consumer reviews, test results, demonstrative videos, etc. It is worth remembering that descriptions of smart toys and understanding of some phrases (for instance, an 'interactive talk') may be different for people responsible for marketing and for us.
- **What data does the toy collect? Where are they stored? Who has access to them?**
We should find the answers in the privacy policy on the manufacturer's web page. There may be an exact reference link on the box or in the instruction manual (often available to download from the web page) to the document or, at least, the main web page address of the manufacturer. As a last resort, we may look for the technical support section on the web page and ask them for more information.
- **How are the data sent between the toy and the manufacturer's server protected?**
By default we should expect the data to be encrypted. However, this is not always the case. Besides, the encryption itself does not guarantee that the data will not be intercepted. Unfortunately, it is no use looking for exact information in any documentation provid-

ed with the toy. It is worth sending a question to the manufacturer's technical support department, and searching for tests of the toy on in the Internet. Maybe someone has already proved that it is insecure? And maybe just the opposite?

- **How can the software be updated?**

All toys tested by us automatically checked for updates each time they were switched on. However, we did not find any information about that in the instruction manuals. Thus, it is worth asking the technical support team before we buy the toy.

- **How long will the product be supported?**

The producer may stop providing updates any time, which means that any possible errors will not be removed. Worse still, the server itself, which is responsible for the toy 'smartness', may be switched off, which will make the toy almost useless. In the case of one of the toys we bought, such information can be found in its marketing materials. However, it is easy to be overlooked. We even did not find it on the box!

Customize Barbie® Hello Dreamhouse™ with Your Own Sounds!

Using the Barbie® Hello Dreamhouse™ Companion app, it's easy to change the sounds in each play space. Pick a sound for any of 15 locations throughout the house or record your own. To go back to the original sounds, it's as easy as saying "Use the original sounds." The Hello Dreamhouse™ Companion app has three main features. How-to videos guide parents through house assembly; the Wi-Fi Setup takes parents through the process for connecting Hello Dreamhouse™ to a Wi-Fi network for voice activation; and Customize Play allows kids to personalize their experience. The use of Hello Dreamhouse™ involves the recording of voice data. Parents are required to create a ToyTalk account and consent to use of Hello Dreamhouse™ by following the in-app instructions. We reserve the right to terminate the app and speech recognition services after 4/1/2019. This product is English speaking only. Product does not ship to the Province of Quebec.

Fig.9 Information on the toy updates

If we manage to collect all, or—at least—most of the answers, we should consider possible risks, and decide whether we consciously want to purchase the toy.

We have the toy

Some toys process only a very limited set of data. In this case, we may only be afraid that somebody may modify the software in such a way that a video camera, a microphone or a motion sensor may record more than the producer assumed (Is the toy second-hand? Do we trust the seller?). Some other toys send a complete set of records of conversations between the child and the toy to the manufacturer, and—apart from the recordings—also their transcriptions are stored that may be used for machine analyses. In such a scenario, it is extremely important to encrypt the data for transmission, as well as to protect

them against unauthorised access by third parties while stored. In other words, we need to have confidence in the service provider contents and in his technical competences.

It is worth noting that all toys we tested were addressed for English-



zdzj. Fotolia.com

speaking customers. It is very important in particular in the scope of the voice recognition function. In our tests the algorithms did not cope very well with this task (even during 'conversations' with a native speaker). It may pose even a greater problem of children's frustration as their pronunciation is naturally less clear and the language—less correct.

The first task we had to complete before we started using each of the toys was to install and start the dedicated application on a smartphone. It was

necessary to create an account on the manufacturer's web page at the first use. At this stage we had to accept all terms and conditions including the privacy policy. Though we tend to skip such messages with a quick 'Next', in this case we recommend to read the documents carefully. They describe what data are collected, who can process them and for what purpose. In the most extreme cases, the manufacturer declared disclosing of all data (including recordings of the child's conversations with the toy) to third parties, almost without any limitations. You will find a wide analysis of this issue further in this guidebook.

The installed application is used to pre-configure the toy. In particular, to set the access data to a wireless network and to connect the toy with the user's account. Wi-Fi Direct or Bluetooth are most often used to connect the toy. In both cases the connection is established without any authorisation on the part of the toy; it does not require any PIN or password. Consequently, we recommend that the initial connection and setup shall be performed in a place where there is no risk that an unauthorised person will intercept the connection for ill purposes. It should be noted that the use of application is usually only required to configure and reconfigure the toy (e.g. when adding a new Wi-Fi network). Once configured, a toy will operate independently as long as it can

connect to a known Wi-Fi network.

The place where the toy is used is also of importance, exactly due to the Wi-Fi networks that the toy 'remembers' since the toy will connect to any Wi-Fi network which will have identical configuration (name, security protocol, password)—even if it is broadcasted e.g. by a malicious neighbour. Anyone in control of a Wi-Fi device to which the toy gets connected may redirect the communication between the toy and vendor's server, potentially eavesdropping or modifying it. The same risk applies when we consciously use public networks if we do not know who administers such networks, or whether they have been intercepted.

In order to protect the user's privacy and ensure that the data is sent to the proper server, manufacturers may apply cryptography, for instance by using the popular SSL/TLS protocols. During the tests we checked if this is the case. The majority of toys passed the test with no reservations, not only encrypting the transfer, but also verifying whether the other party indeed belongs to the manufacturer and, consequently, refusing to communicate with the substitute server we provided. It was also the case with Hello Barbie doll which was declared in 2013 as susceptible to such a type of attacks. It means that producers have obviously removed the problem and ensured an adequate update of

the software for the doll. Unfortunately, in one of the toys the encryption was poorly implemented and not all the data were protected. In particular, it was possible to install a fabricated update. On the other hand, a properly used and adequately strong encryption prevents us from checking what data are collected by the toy only on the basis of the analysis of traffic between the toy and the server.

All the toys we tested are equipped with the automatic updating mechanism. When connected to the Wi-Fi network, they check the manufacturer's website for the most recent available software updates, download, and install them if required. As we mentioned above, it is extremely important that the cryptographic mechanisms ensure that updates are actually a safe source. An unauthorised change in the toy's software might result in any use of peripheral devices the toy is equipped with (i.e., first of all, a microphone or a video camera) and transfer of data to any server, without any control.

It is worth emphasising that all toys we tested collect data only in response to the user's conscious interaction (typically a push of a button). This is good news since it means that the toys are not 'listening' all the time and they do not send data to the manufacturer if we do not wish so, or if we are not aware.

We also posed a question whether the 'smartness' of the toys may be used against the child, for example, by teaching them an aggressive or vulgar behaviour. In case of the majority of the toys, the answer turned out to be very simple, due to their limited ability to interact and no possibility to generate messages outside the scope of pre-defined scripts (even if the script included over 8000 phrases, as was the case of Hello Barbie). As far as CogniToys Dino is concerned, the potential seemed to be higher because it uses the IBM Watson system and generates responses based on an extended (and probably constantly broadened) knowledge base. However, the producer took care of unsuitable content filters, either by limiting access to undesirable content or responding adequately to any attempts of the testing persons' 'unsuitable behaviour'.

Physical safety of the toy

Another way of 'attacking' a smart toy is through a physical access to its systems and an attempt to recover or modify data and software. The data recorded by the toy include names and passwords to Wi-Fi networks or the user's account data. In turn, apart from the software itself, the elements such as audio messages may be modified that are available when the

toy is not connected to the network (for instance, the messages greeting the child or notifying about errors).

'Smart' toys are nothing more than electronic devices adjusted to communicate with the outer world through embedded sensors (e.g. a microphone or a video camera), as well as with the Internet through standard network interfaces (e.g. Wi-Fi, Blue Tooth).

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.

Hello Barbie

It seemingly does not differ from the other dolls of the producer, however,



Fig.10 Hello Barbie with accessories.

it is equipped with a docking station and a charger (see Fig. 10). When we undress and open the doll, we can see a printed circuit board and identify all

functional elements (see Fig. 11): A wireless network module—Azure-Wave AWCU300E 802.11 b/g/n,

1. Memory storing the software and all data—Gigadevice GD25Q16 16Mbit SPI Flash,
2. An audio module responsible for processing signals from the microphone and sound reproduction—Nuvoton NAU8810 24bit.

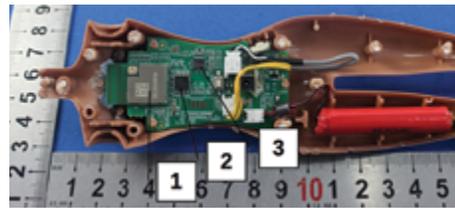


Fig. 11 Opened Hello Barbie doll

Should anyone unauthorised have physical access to the doll, the most exposed element is the memory because all its content can be read. During the analysis it was shown that in order to read the whole memory content, it is enough to solder out the element and read it with the use of a reader. The memory is divided into sections due to its functional areas.

- Section no. 1 includes the so-called Boot loader which enables the toy's software to run.
- Section no. 2 contains configuration of the toll with relevant credentials for a Wi-Fi network. It is worth noting that it was not

possible to read the data, because they were encrypted.

- Section no. 3 contains the software to control the doll.
- Section no. 4 contains software for a Wi-Fi module.
- Section no. 5 contains all audio files used offline.

We do not have an easy access to sensitive data recorded in the doll's memory. Difficult, onerous, and requiring specialised knowledge modification of the software or audio files recorded in the memory is still possible.

Doll users should be forewarned that they should be very careful when buying the toy on the secondary market, and—if they still decided



Fig. 12 Traces left when a Hello Barbie doll has been opened

to purchase it—they should check whether the doll had not been opened before. In the case of Hello Barbie doll, the majority of physical interference attempts should leave some traces. The easiest way to check it is by looking at the cracks where two parts of the doll come into contact with each other. Since the doll is to a certain degree glued inside, the access to its interior part requires some physical strength which normally leaves traces on the edges (see Fig. 12).

Photos of Hello Barbie were taken from: <https://fccid.io/PIYDKF74-15A5W> and <http://someretrecon.com/s/HelloBarbieSecurityAnalysis.pdf>.

Dream House

A smart home made by the same producer as the Hello Barbie doll. After opening we can see two printed circuit boards out of which the green one is worth analysing (see Fig. 13). At the first glance, it looks similarly as the circuit board from the Hello Barbie doll.

We can identify the same functional blocks on the board as in the case of the Hello Barbie doll. Figure 14 shows the individual modules:

1. A wireless network module,
2. Memory storing the software and all data—Winbond W25Q128FV,
3. An audio module responsible for processing signals from



Fig. 13. Central unit of Hello Dreamhouse

microphone and sound reproduction.

The layout of the elements on the board suggests that it is the same system as in the case of Hello Barbie doll, only with more memory. After soldering out the memory chip and reading its content, it turned out that

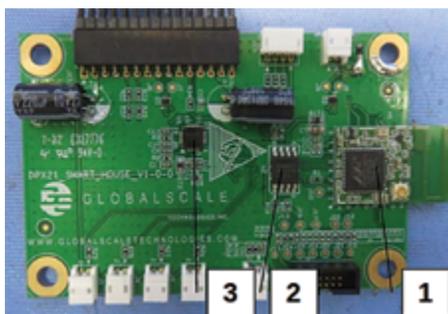


Fig. 14 Communication module of the Dream House

it is exactly the same system as far as the functions used are concerned. A bigger memory was used because of bigger sizes of audio files. In turn, the second board was responsible for the control of the individual elements

of the house, however, it does not communicate with the network.

Unlike the doll, the electronic elements of the house may be accessed easily through unscrewing convenient screws, which do not bear any traces of the manipulation. Consequently, if we decide to purchase such a toy from an unreliable source, it is not possible to verify whether any modifications were made. In such a case, the only solution is to open the toy and check whether the memory chip was soldered out and soldered in again. Usually such manipulations leave traces near the chip foot (see Fig. 15), however, such manipulations may be performed very carefully and do not leave visible



Fig. 15 Sample traces after manipulations with the memory chip

traces of interference.

Pictures of the Dream House were taken from: <https://fccid.io/PIYDPX21-16A5W>.

Fisher Price Smart Toy

It is the most technologically advanced toy covered by the analysis.

From the outside it is a nice teddy panda bear or a monkey (see Fig. 7), whereas inside it holds an electronic system that functionally and technologically resembles a smartphone. In order to connect the toy, it is necessary to split the fur on the back along the section from its tail up to the head base (see Fig. 16) and cut one banding band. Next, we are able to take the casing out from the inside and freely unscrew the cover. The toy is controlled with the use of operating system from the Android family. Placement of a USB port on the circuit board (see Fig. 17) allows us to interact with the device



Fig. 16 Smart Toy—a teddy bear



Fig. 17 Smart Toy after splitting

in the same scope as in the case of a smartphone. We have access to files and processes, we are able to install our own applications, and read all data from the toy. The threat may be depicted the best when preparing an application installed with the Android system and using it to eavesdrop by using the embedded video camera and a microphone.

The smart toy manufactured by Fisher Price allows for a great scope of

manipulation in its software when getting a physical access to it. The only traces that may be visible after such manipulation involve split fur on the back of the toy, which may be carefully sewn up leaving traces that are not visible at first, but only upon closer examination.



Fig. 18 The motherboard of the Smart Toy with the USB port

Pictures of the SmartToy were taken from:
<https://fccid.io/CCT-DNV31-15>.

6. 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, in order to prepare this guidebook, 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 will enter into force in May 2018.

Based on the analyses performed by Everberg Legal Office, we present the most important potential risks connected with the use of smart toys, resulting from the security policies of their producers and their regulations concerning protection of users' privacy.

The scope of data collected by toy / software developer

Smart toys tested for the purpose of this guidebook automatically record and send various personal data of a child that uses the toy. The manufacturers state that the toys may collect, among others, data about the children's interests, things they like or do not like, as well as other data concerning their education. It means that the toy manufacturer stores and processes the data collected during the child's interaction with the toy.

It must be noted that, despite the fact the types of automatically collected data have been determined, this is not a closed list, so the producers cannot limit in any way the scope of data that they can gather and process as a result of children's interactions with their toys. Additionally, the notions describing this open catalogue of collected data are insofar imprecise that **the manufacturer is de facto authorised to collect all and any information acquired during the children's interaction with a given toy.**

Some toys also record audio files acquired when children play with their toys. Such recordings are subsequently processed (analysed, translated, subject to studies) by the manufacturer and his subcontractors. The scope of activities performed with the use of audio recordings acquired in the described way is, basically, unlimited. The manufacturer states that neither audio recordings nor their content will be used to contact children. However, it must be noted that if the producer limited the possibility to use the collected data only within the scope of contacts with children, it must be assumed that they can process these data collected for any other purposes. For example, it may collect and process data acquired through recording of conversations of the household members living with the child who uses the toy.

Parents' access to data collected by the producer

In its policy, the manufacturer of CogniToy Dino stated that the parent had access to the majority of data collected as a result of child's interactions with the toy, but it did not explain what data are not available for the parents and why. According to the regulations binding in Poland (Article 32 of the Law of 29 August 1997 on personal data protection), each person has the right to control

their personal data. Thus, when comparing the privileges of parents who exercise the rights of their children (resulting from the analysed security policy) with the scope of rights resulting from the provisions binding within the territory of Poland—protection of a person the data refer to (and the parent who exercises the rights of their children) is significantly lower on the basis of the policy concerning CogniToy Dino. In this context, there is a **risk of processing of personal data by the toy manufacturer, without the knowledge and consent of the person the data refer to (or a parent of the child the data**



refer to).

Imperfection of the Privacy Shield system

The security policy of the Hello Barbie doll indicates that the manufacturer holds a certificate relating to the 'EU-U.S. Privacy Shield Framework agreement'. The certification program assumes an equal level of personal data protection processed by entities with their registered offices in the US (i.e. the ones entered on the lists of certified entities) and the level of data protection binding in the European Union and Switzerland.

It must be underlined that, in spite of holding relevant certificates, the entities with their registered offices in the US cannot ensure the level of protection required by the European legislation. For example, toy manufacturers may transmit personal data to third countries which do not ensure an adequate level of protection (discussed below in more detail).

Transmitting data to third countries

Pursuant to the provisions on personal data protection binding within the territory of the European Union, transmission of personal data outside the territory of the European Economic Area is permitted only if a given state can ensure an adequate level of personal data protection. Thanks to this

solution, personal data are, as a rule, protected against the consequences of their possible transfer to a state where the regulations in this respect do not assure such level of security as the regime binding in the EEA.

Toy manufacturers often reserve the right to transmit data outside the territory of the US, while not precisely stating which countries they refer to. Consequently, there is a risk on the part of the manufacturer to transmit the collected personal data to a third country where the protection standards are low or they do not exist. It poses a significant risk in terms of preserving the confidentiality of personal data. For example, it must be noted that if such data will be transmitted to the country where it is allowed to trade databases without any restrictions, the persons the data refer to will not have any tools which would make it possible for them to control which entities process their data and why. **Consequently, such persons will be deprived of one of the basic rights granted within the territory of the European Union:** the right to control their personal data processing.

Making data available to prosecution and administrative authorities.

The analysed security policies provide for the possibility to transmit the personal data to law enforcement and administrative authorities in the

US. This possibility is also reserved for the manufacturers practically without any limitations, since one of the conditions of such data provision is the manufacturer's belief about the necessity to transmit the data. Consequently, the manufacturer is authorised to provide the data to state authorities (prosecutor's offices, the police, other services) in any situation.

Such broad rights possessed by the manufacturers essentially mean that state authorities may keep citizens under surveillance on a wide scale, practically without any court supervision in this respect. It stays in a clear contrast to the regime binding, as a principle, in the European Union

where disclosure of personal data to state institutions is restricted to specific situations and subject to court supervision as to, among others, the legitimacy of data disclosure.

As John Carr has emphasised recently¹⁵, perhaps GDPR will be able to ensure sufficient legal basis, which will determine requirements for manufacturers' security policies. It seems that in the near future a system resembling CE marking system should be in place on the smart toy market to allow parents and children rest assured that the things they can purchase or use comply with certain basic standards for the protection of their privacy.



¹⁵ <https://johnc1912.wordpress.com/2017/07/19/more-warnings-about-the-internet-of-toys/>.

Conclusions

Those manufacturers of smart toys whose security policies were subject to analysis do not ensure personal data protection at the level required by regulations binding in the European Union, including Poland.

- The scope of personal data collected and processed by toy manufacturers is not specified, so they may process, basically, all data obtained during interaction with their toys.
- Some toys intercept sounds, and manufacturers may process the recordings without any restrictions, which may deprive or significantly restrict the rights of the party the data refer to (or a parent of the child the data refer to) to control the scope of processed data (one of the basic rights in the data protection regime valid within the EU).
- Manufacturers do not clearly ensure the possibility to access the processed data by the person the data refer to (or a parent of the child the data refer to) to control the scope of processed data (one of the basic rights in the data protection regime valid within the EU).
- The very fact that the manufacturer holds a certificate granted within the 'EU-U.S. Privacy Shield Frameworks' program does not mean that the producer complies with all the requirements concerning personal data processing resulting from the law binding within the territory of the EU.
- A significant threat for the effective protection of personal data processed by toy manufacturers is the possibility to transmit the collected data to the countries with low or even no protection in this respect.
- The possibility to provide personal data to state authorities (e.g. the police, prosecutor's offices, other services) with no court supervision stays in serious contrast to the rules binding within the territory of the Republic of Poland in this respect and may involve unjustified surveillance performed by American administration authorities.

TIPS AND TRICKS**Before buying a toy:**

- Consider whether you took into account all risks relating to the purchase of a given toy and if they are justified by its 'smart' functions? Maybe a traditional toy is a safer choice?
- Do not buy a smart toy under the impulse when visiting a toy shop. You will not find much important information on the box and you will likely not obtain them from the seller.
- Read the opinions about the toy, look for some videos. Try to get convinced if its operation is consistent with your and your kid's expectations.
- Search for information concerning possible problems with the toy's security: news articles, vulnerability reports, etc.
- Be particularly careful towards those toys that have appeared on the market very recently. There is a good chance that the vendor launched them before they were tested properly, and their updated versions will be available soon.
- Do not buy used toys if you do not fully trust the seller, and you do not know their origin. The toy may have been modified, for example in order to send data not only to the manufacturer.
- Adjust the toy to your child's age.

TIPS AND TRICKS

When you have bought a toy:

- When configuring the toy with the use of a smartphone (and also when adding a new Wi-Fi network), make sure you are in a safe place and that nobody is able to connect to the toy apart from you.
- Read carefully the privacy policy before you accept it. Do you know what data will be stored, where and by whom?
- When creating an account, use the password that differs from those you used previously which is adequately strong (consisting of minimum 10 characters and including also the characters from outside the basic alphabet, e.g. numbers, punctuation marks).
- Provide real information about yourself / your children only as necessary to operate the toy properly.
- Remember to connect the toy only with secured Wi-Fi networks. It is not enough that the network is encrypted. Do you really know who manages its access point?
- Regularly check the account where the data from the toy are collected. Remove the unnecessary data on an ongoing basis.
- Do not log in to the account using links received in e-mails or via communicators in order to avoid becoming a victim of data theft. Log in typing the webpage address yourself, or using bookmarks.
- Make sure the toy is switched off when it is not used.
- Take care about the balance between your children playing with peers and the time they spend with digital toys or screen-equipped devices.
- Remember that knowledge implemented in the toys is often selected and limited and the subjects of possible interactions are frequently restricted by the manufacturer.
- Remember that your child may be subject to hidden marketing.

TIPS AND TRICKS

Before you dispose of the toy:

- Remember to remove data from the toy by restoring the device back to factory default status. You should find instructions in the user's manual.
- If you do not plan using a similar toy anymore, consider deleting the account from the manufacturer's service.

Contents:

1. Introduction.....	2
2. Children—first consumers of new technologies.....	5
3. Internet of Things	11
4. Perception and popularity of smart devices in Poland.	
Quantitative and qualitative studies.....	14
Is my fridge smart?.....	16
Who buys and who makes decisions?	18
How we evaluate IoT technology development in the context of children?.....	20
5. Smart toys under scrutiny. Tests and analysis of the issues	25
We are buying a smart toy	28
We have the toy	30
Physical safety of the toy	33
6. In legal experts' eyes.....	39
Tips and Tricks	44
Authors.....	48
Expert co-operation.....	49
International perspective.....	50

Authors:



Anna Rywczyńska

Coordinator of Polish Safer Internet Centre and the Manager of the NASK National Research Institute's Social Projects Team. An expert in the field of children and youth's safe use of online content and new media. Co-founder of the international conference 'Keeping Children and Young People Safe Online'. An author and co-author of publications and educational tools and a member of international working groups, i.a. under ENISA and ECSO.



Przemysław Jaroszewski

He manages the CERT Polska team operating within the structures of NASK National Research Institute. A programmer and a social psychologist. He has more than ten years of experience in the scope of ICT safety. In the course of his career he has been engaged in numerous national and international projects related to the cooperation of hotlines and data exchange. A co-author of training materials and a coach within the programmes for hotlines, i.a. TRANSITS and ENISA CERT Exercises.

Expert co-operation:



Mikołaj Kopec

IT security consultant with many years of experience. Specializes in the security of ICT infrastructure and application. Enthusiast of the embedded systems, OT and IoT, and security aspects related to them. He participated in many projects in the area of the security audit, vulnerability assessment, and penetration tests for companies and institutions from the financial, public and new technologies sectors. He graduated from the Faculty of Cybernetics of the Military University of Technology, with the specialization of ICT Networks.

Implementation of quantitative research —Ariadna National Research Panel



Conducting a legal analysis Law Firm Everberg



E V E R B E R G

ONE STEP AHEAD

International perspective:



Chris Pinchen, 'The Privacy Agency'

Parents should be aware that most IoT toys are made by toy manufacturers, not tech companies. This can mean that the whole IoT part takes second place, and the toy companies are not experts, nor often experienced, in digital security. Parents should also consider whether the technology used in the toys will be maintained, and if they will be expected to pay for upgrades to keep the device functioning. If a toy has software or hardware that is no longer supported, will the toy still be usable? Remember the toy company is interested in selling toys and may be outsourcing the technology, databases and data gathering to third parties—do those third parties have experience or a good reputation in their field. What obligations are they under with respect to privacy and data protection? Is it possible to even get this information? And also, what about legal jurisdictions—where is the data saved, under which territories and applicable laws?



Barbara Buchegger, Pedagogical Manager of Safer-internet.at

Connected toys enter our children's rooms and life from an early age on. From dolls, robots, cars, to smartwatches or glasses: often it is difficult to detect what data is collected, how secure the connection is and how to deal with these new digital assistants. Thus, parents need more guidance and information on the risks and opportunities of these toys in their kids life: This relates to surveillance and privacy on the one side, but also to risks such as children relying too much on parents or other adults since 'they anyway always know what I am doing'. Still, connected and smart toys offer as well the opportunity to learn things in a until now unknown and unimagined way.

Authors: Anna Rywczyńska, Przemysław Jaroszewski
Proofreading: Katarzyna Wilczek
Cover design & layout: Aneta Witecka

Copyright NASK National Research Institute
Illustrations: Fotolia.com

NASK—National Research Institute
Kolska 12.
01-045 Warszawa
www.nask.pl

First Edition
Warsaw 2018
ISBN 978-83-65448-06-4

NASK

NASK is a National Research Institute supervised by the Ministry of Digital Affairs. NASK conducts research focused mainly on efficiency, reliability and security of IT networks and other complex network systems. The majority of NASK's activities is related to ensuring Internet security.

Responding to incidents affecting network security in Poland and coordination of activities in this area is handled by the NC Cyber department, within which operates CERT Polska. NASK also maintains the domain.pl registry.

Educational activity and popularization of the information society idea plays an important role. At NASK Academy, social projects and unique trainings for companies and institutions with particular emphasis on the subject of ICT security are offered. For years NASK has also been engaged in conducting the European Commission's Safer Internet Programme promoting safe use of new technologies and Internet resources among children and young people.

NASK also conducts systematic social research in the area of Internet security and digital education, including a nationwide survey among young network users titled 'Teenagers 3.0'. The research projects are consulted by the Scientific Committee of Experts for the Development of Information and Communication Technology in Education, which hosts renowned scientists and specialists in the field of education and the use of new technologies in teaching.

NASK runs the IT Szkola e-learning portal (www.it-szkola.edu.pl) addressed to upper secondary school students and teachers. Content offered by IT Szkola is designed to develop digital competences. The portal offers online lectures and certified courses.

Within the framework of the institute there is the Dyzurnet.pl team, the only contact point in Poland that responds to anonymous reports received from Internet users about potentially illegal material, such as pornographic content involving a minor.

NASK acts as the operator of the Polish Nationwide Educational Network—a program that aims at providing access to fast and secure Internet to all schools in Poland.

NASK National Research Institute
Kolska 12, 01-045 Warszawa
phone +48 22 380 82 00, fax +48 22 380 82 01, nask@nask.pl
www.nask.pl

