


A Review on Ethical Issues for Smart Connected Toys in the Context of Big Data

Victor Chang^{1, 2}^a, Zhongying Li¹, Muthu Ramachandran³

¹ International Business School Suzhou, Xi'an Jiaotong-Liverpool University, Suzhou, China

² Research Institute of Big Data Analytics, Xi'an Jiaotong-Liverpool University, Suzhou, China

³ Department of Computing, Creative Technologies and Engineering, Leeds Beckett University, Leeds, UK
Victor.Chang@xjtlu.edu.cn, Zhongying.Li18@student.xjtlu.edu.cn, M.Ramachandran@leedsbeckett.ac.uk

Keywords: Big Data, Internet of Things, Smart Connected Toys, Ethics

Abstract: This report discusses the big data industry and its derived product, the Internet of Things. On this basis, this paper analyzes the ethical challenges encountered by smart connected toys. It also offers some possible recommendations involved with regulation and parental control, and examine what the stakeholders in smart connected toys industry should do under the framework principles of IoT.

1 INTRODUCTION

Benefiting from the rapid growth of big data industry and Internet of Things (IoT), smart connected toys have gained much more popularity than before. From the storytelling-interaction toy like “CogniToys Dino” to the smart connected toys that can communicate with children such as “Hello Barbie” and “Edwin the Duck”, there is a wide variety of smart toys with IoT technologies available these days. The marketers of these smart connected toys promote their products by addressing their functionality of interactive and educational purpose, as well as their content with clarity, education and fun. As a result, this can catch both parents’ and children’s attention and popularity. For the purpose of maintaining these functions, the smart connected toys should constantly use the Internet for data processing and computation, so that it has the response and update for the content. Smart toys are easy to use and can make interactions with adults and children. It can be presented as an encyclopedia for educational purposes. Similarly, it can take videos and pictures, and be served as mini high-end machine with the automated remote sensor unit and simple artificial intelligence unit.


However, it may pose certain threats and vulnerabilities related to ethical issues of the big data

to our children and parents by such almost non-stop connection. For example, pictures and videos of the owners’ homes can be taken and can be hacked and stolen. Additionally, images and video or audio recording of children can also be taken, with the assumption that these can be done without the need to ask permission every time. On one hand, the smart connected toys collect the personal information to provide a customized and interesting experience for children. However, all these can raise ethical questions as follows. Is all the data collected previously informed? Do the children and parents have the right to remove their personal information from the cloud? Furthermore, the threats posed by vulnerabilities may lead to hacking and unauthorized access to the smart connected toys. The sensitive information can be retrieved and even traded in the open market.

2 BIG DATA AND THE ETHICAL ISSUES RELATED

2.1 What Is Big Data?

Since the 21st century, massive data could be created by online services on daily basis. It has become more

^a <https://orcid.org/0000-0002-8012-5852>

challenging to manage them, since the complexity, quantity and the ownership issues can be complicated on search engine services and social media. How do you feel if somebody tells that Baidu handles a daily data with the amount of 2 petabytes of data roughly equivalent to the information of 5000 national libraries, or that every day, on average, around 500 million tweets are created via Twitter? We live in an information age with massive of information developed, exchanged, analyzed and stored on daily basis. However, not all the data can be useful. Therefore, we should critically evaluate what is more important for us, and what we should do about them. This can make us more prepared for the changes that big data society can bring, whether they are positive or negative to our everyday activities.

According to the definition by Gartner, the world's leading research and advisory company, the big data can be extremely large data sets with great variety and may show some kind of patterns, trends, and association after analyzed computationally. "Big data" has become the high-frequency word in today's society. Experts believe that its revolutionary significance is to provide a new tool for people's cognition, judgment and decision-making. It will change the government's operation and supervision mode, boost economic restructuring, and make it easier for people to live with convenience in the information age. A report by technology research firm IDC says forecast revenue for big data and analysis solutions is likely to reach \$27 billion mark by 2022, witnessing a compound annual growth rate of 15.1% during the next 5 years.

2.2 The Impact of Big Data

On the one hand, the big data analytics (BDAs) have emerged due to the increase in the market and business demands. BDAs combine complex mathematics applications like prediction models and statistical algorithms with human and social theories like customer behavior and enterprise optimization. Millions of analysts, researchers, and business users take advantages of big data to make decisions faster and more appropriate. It offers a variety of benefits such as new business opportunity and more effective operations for every walks of life. To be specific, large amount of precious data of the company which has not yet been used can be analyzed in order to gain new insights. Enterprises are urgently exploring executable areas in the data stream. Actually, many projects of big data are born with specific business problems that need to be solved. With the help of

appropriate platforms and software products, companies can quickly increase sales, improve efficiency, optimize their operations, and gain a better customer service. A company can figure out every customer's needs by analyzing the types of products, the price range and the feedback in the past. To further this, a company can forecast what types of services or products and sentiment after purchase, if it makes use of big data analytics. Even more, it can help to create new products as well.

However, such intelligent power is currently confronted with some ethical problems. According to Zwitter (2014), industry is moving towards "changes in how ethics has to be perceived away from individual decisions with specific and knowledgeable outcomes towards actions by many unaware that they may have taken actions with unintended consequences for anyone". Each of these four themes is described next.

Table 1: Ethical issues related to data analytics.

Ethical and related problems	Challenges	Examples
Privacy	Sharing of personal information without permission – de-identifying information	Facebook study in 2012 to test user's emotions without their consent
Security	Protection of data from outside threats	Hospital data ransomed in 2016 due to lax security
Ownership	The rightful ownership of the data used for analytics	Research in illegal behaviors where the courts want the data to build a case against a person
Evidence Based Decision Making	The use of data to make decisions about a population based solely on quantitative information	States make decisions about welfare guidelines using income as the sole factor

Firstly, privacy can be a problem, which means that people's personal information can be recorded under ubiquitous observation. But we should ask whether it has the permission. If not, it can be a kind of privacy spy. Secondly, information security is also a point worth considering. Even if the personal

information is collected with absolute harmless intent, but once it is stored on any servers, data breaches such as hacking can happen. Thirdly, who has the right and legal ownership of the data that could be used for analytics? People generally recognize that they still own their data even if they give the consent to the disclosure statement, but typically they have no right to remove or wipe the data in the following process. Lastly, only using the quantitative information or the numbers to make a decision occasionally leads to an ethical problem. Ignoring personal characteristics and just using the aspect of group might result in a totally different decision (Tene & Polonetsky, 2013).

On the other hand, the rapid development of big data has reset the mode of operation of our society, including the government, business industry, and public service. In the age of big data, the internet has become a digital platform with data resources for people to collect, exchange and analyze. Even mobile phones have the apps and services to trace the whereabouts of the people and the data. For example, if a user leaves a trace, network connected devices like your mobile phone can enable to automatically record no matter what you do and what you say. For an instance, the techradar, a wearable fitness trackers, can monitor how much exercise and food the user has taken effortlessly and with unmatched accuracy. It can also constantly measure the users' core health information, such as burned calories, quality of sleep and step count in order to give users health-related advice in their daily lives. Hence, IoT has become a massive emerging market and more than 25 billion devices with sensors will be expected to come into service by the end of 2020 (Gartner, 2014).

3 INTERNET OF THINGS & SMART CONNECTED TOY

3.1 Internet of Things & IoT Analytics

The earliest mention of the word "Internet of Things" can be dated back to just one year ahead of last millennium and quickly became broadly used due to Kevin Ashton's contribution to the sensing technology. However, the precise definition of IoT was not given at that stage and people uniformly agreed that IoT involves objects and connectivity. Actually, it is Coca Cola machine that became the first practice of the IoT in the early 1980s. Coca Cola company made it connected to the internet to guarantee that there were drinks available to be sold,

and this machine can also check whether the drinks were cold or not. As nearly two decades passed by, IoT technology has enabled billions of people to connect to Internet with computers or mobile devices, reaching the consciousness of the masses.

Nowadays, IoT has a clear definition as a system of two components. One is the devices which allow computation and has the ability to connect to but not interfere each other, and the other is digital machines or "other things" with unique identifiers (UIDs) which can transfer data by internet. Therefore, it is crucial to guarantee the constant data stream and ensure its accuracy without making any errors. Although the IoT does not have a long history, it has also been indispensable in your daily life. Nowadays, almost everyone may carry something with sensing technology without even realizing that we have been closely involved with this network technology. Moreover, for every major city we go, we can be easily and seamlessly connected to the internet everywhere, with thanks to the vast development of internet, wide area access points, and easy-to-register and easy-to-use features that allow users and visitors to stay in touch with the internet and the city easily. Services can be online to make it convenient for the residents. This can also connect to the services such as healthcare, education, transportation and the government, thus forming a kind of smart city plan and development (Chang et al., 2018). Therefore, it is highly probable for IoT to become next technology revolution connecting "everything, everywhere, every time, and everybody (4E)".

On these bases, IoT analytics can be considered as an application combined with data analytics in the context of big data and IoT technology. So the data using in IoT analytics is always seen as the subordinate part of big data in the context of Internet of Things. IoT analytics is more about the process of recognizing and utilizing the value of massive data flow collected by the sensory devices with IoT technology. Currently, IoT analytics is widely applied in the manufacturing industry enabling organizations to gather and analyze the IoT data from their own products and this report takes the smart connected toy as an example to analyze and detect the ethical issues related.

3.2 Smart Connected Toys

3.2.1 What Is A Smart Connected Toy?

The earliest appearance of toys was dolls made of clay, wood, animal bones and ivory traced back to the

ancient Egyptian era more than 5,000 years ago. And a Persian toy with a round wheel was found in the Persian relics about 2,000 years later. Toys have always been an essential part of human’s history and evolved with human beings in the following thousands of years. Normally, a toy can be defined as an object for children to play with and a way to learning by entertaining in human society. Toys have already undergone transformation. Originally they can be made from natural resources like branches and shells, and then be manufactured by machines such as the electronic toys involved with sensors, hardware and IoT technology.

With the development of big data industry and IoT, the toy industry’s revolution is under way and computing technology can be applied to the traditional toys which has been designated as “Toy computing” (Hung 2015). It is a kind of application in IoT analytics that transfer children’s data collected by the physical toys embedded with sensors to the computing services in cloud through networking. These electronic toys with computing services hold the purpose that to offer the environment for children combined with learning, interaction, and entertainment.

The physical part of the toy computing system is almost the same as traditional toys in addition to the embedded sensors and devices that enable to connect to the internet, which should be able to interact with the mobile component like Bluetooth, WLAN, and RFID. In this system, the mobile component plays a role as primary computing procedure including the CPU, memory, sensory input, and output. Figure 1 illustrates the framework of toy computing system.

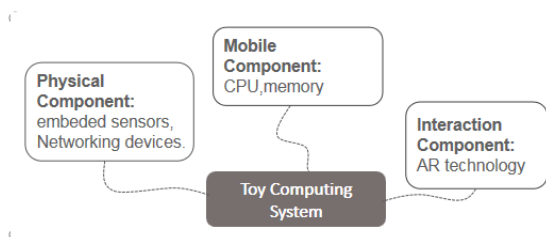


Figure 1: Toy computing system.

On these bases, the smart connected toys can be described as devices formed with a physical toy component embedded with sensory devices. It allows the smart toys to connect to toy computing services in cloud to realize the interactive function via Wi-Fi (Ren et al. 2015). A smart connected toy in this context could be exactly thought of a practical use of the Internet of Things especially applied with

Artificial Intelligence that has the ability to offer Augmented Reality experiences to children.

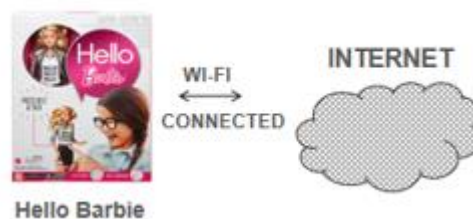


Figure 2: A smart connected toy take “Hello Barbie” as an example.

Based on the previous discussion of big data, IoT, and smart connected toys, this paper aims to make it clear about the relationship among data analytics, IoT analytics, and toy computing, shown by Figure 3 as follows. Data analytics cover all the aspects of data and its analysis, and can be presented by visualization and graphical outputs in different sectors and industry. IoT analytics is under an aspect of data analytics, since it only collects, processes and analyzes data related to IoT. Similarly, smart toy computing is under a specialized area of IoT, as it uses sensor technology to collect data, and sends back to the central units or internet to analyze or search the outputs, and return to the smart toys, which then display outputs to the children.

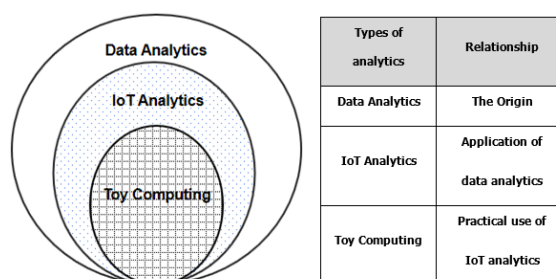


Figure 3: The framework of relationship between data analytics, IoT analytics, and toy computing.

3.2.2 The Data Smart Connected Toys Can Collect

Smart connected toys are equipped with sensitive input/output devices such as speakers, microphones, cameras, and GPS, and these devices may collect many personally identifiable information (PII) as it is shown respectively in Table 2:

Table 2: Collected data by available sensors and devices in smart connected toys.

Devices and sensors	Possible collected data type
Global Position System(GPS)	Location(even with longitude and latitude)
Microphones&speakers	Records for voice of children
Cameras	Pictures of children
Motion Detector	Motions of children
Touch Detector	Fingerprints of children
Thermometer	Body temperature of children
Microcomputer	Addresses, names, ages

Some smart connected toys can blend the function of entertainment and security together like “Cloudpets”. It is a toy similar to a wearable watch, which allows children to have their own virtual pets and exchange voice messages with parents and friends. Parents can get the location with GPS of their children to check safety.

Some smart connected toys are designed for interaction purpose, and such toys must have microphones and speakers for children to communicate with. For example, “Hello Barbie” is a smart interactive doll embedded with voice recognition sensors to listen and reply to the children by sending the voice recordings to cloud computing. Other smart connected toys for interaction purpose like “My Friend Cayla” can even respond to children with gestures. This can be done by understanding children’s movement and their touch with motion detector and touch detector.

Some smart connected toys are designed for educational purpose like “Anki Cozmo”. It is an intelligent programmable toy not only equipped with embedded speaker, camera, and facial recognition to sing, play games and observes its surroundings but also with a microcomputer for children to program via a Python-based SDK. The microcomputer can collect the sensitive personal information (SPI) of children (e.g. home addresses, names, age) before initialize the system of the toy, and transfer to the cloud.

Typically, smart connected toys have connectivity capabilities including Wi-Fi and Bluetooth, so that smart connected toys can reach the local area network for the purpose of IoT data analysis (e.g. natural

language processing, speech recognition) in the cloud. Connectivity devices can also enable the smart connected toys to connect to companion mobile applications after the cloud computing. For instance, the smart connected toy named as “Wiggy Piggy Bankis” make it possible for parents to set tasks, create goals, and send rewards to their children through a companion mobile application related.

3.2.3 The Ethical Problems Related to Smart Connected Toys

Hung and Cheng (2009) define information privacy as an individual’s right to determine how, when, and to what extent information about the self will be released to another person or to an organization. However, most of the children are not consciously aware of the concept of personal privacy. A smart connected toy may follow the child through everyday activities, so the toy can easily build the “emotional connection” with children. As a result, children tend to disclose personal information to smart connected toys as much as possible which means the toys can collect a great deal of data from children even without permission. Besides, almost all the smart connected toys have a privacy policy indicating some privacy aspects related such as what information the toys may collect ,how do they use the children the data and what the toys share with third parties. However, a few vendors of smart connected toys do not state the privacy policy or just indicate in a generic way. What can be worse, is that sometimes even if the parents consent the privacy policy for their children, parents do not truly realize the fact that they did not read or understand the policy entirely.

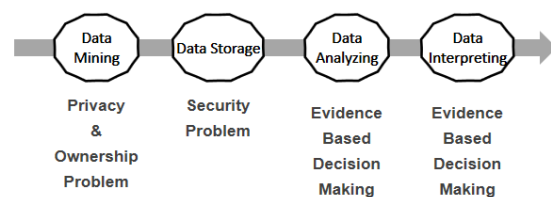


Figure 4: Ethical problems in the process of toy computing.

Additionally, smart toys collect PII data to present a personalized experience for the children. However, PII collection can be a problem if improper security measures are applied to protect either the locally stored data or the data in the cloud. As it illustrated in 3.2.1, the connectivity devices in the smart connected toys including Wi-Fi and Bluetooth can reach the cloud in 2 ways: (1) Smart connected toys to cloud, (2) Smart connected toys to Mobile phone application

(through cloud). Hackers can also attack on the network in these two ways.

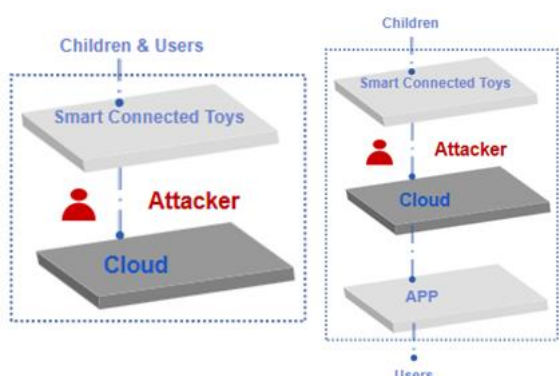


Figure 5: Attack on the network in two ways.

If the hackers successfully attack and take control of the network between smart connected toys and the online computing service, attackers will probably inject audio to induce children to do something harmful which could be much more dangerous (Vlajic et al., 2017).

For example, the attackers can spread content through the audio system, which is adverse for children's growth through the built-in audio in the smart toys. Those negative content includes instructing kids how to open the doors without anyone knowing or lie to your parents. Besides, there are also some mean languages aimed to insult the child and impair their self-esteem and confidence causing psychological hurt to the child. Sometimes attackers can even inflict children by inducing children to opening doors of their homes.

Furthermore, decision making while analyzing and utilizing the data may be a confusing problem. Taking retail industry as example, it is the children who can make up a large proportion of the customer group, so their data such as consumer behavior and other context information may be collected by the marketers to analyze and identify their group characteristics and conduct targeting advertising. However, some application developers take advantage of children's psychographic characteristics of innocence and make some advergames like "Lego Duplo" that features advertising messages, logos and trademarks in a game format. Children without the supervision of parents will probably purchase some virtual products without awareness of its seriousness.

4 METHODS

Firstly, the parents should play a significant role in protecting our children from ethical problems of toy computing. Although children have the right to keep privacy from their parents, parental control still can be considered as an effective and straightforward way for both online and offline. As the recommendation from United Nations International Children's Emergency Fund, parental control should be used for the purpose of identifying all kinds of risks and choosing what is appropriate for their children. On this basis, parental monitoring system can be integrated with toy computing (see Figure 5) and build their own dashboard on mobile phones with related activities for the smart connected toys of their children (Tracy and Westeyn 2012) This dashboard should be where parents can see all the privacy policies of all the smart connected toy they have for check at any time. At the same time, parents can also modify and remove the information collected by the smart connected toy. Furthermore, the dashboard also should have the function of alert mechanism in order to ensure that parents can receive timely notification if there is anything with privacy risk.

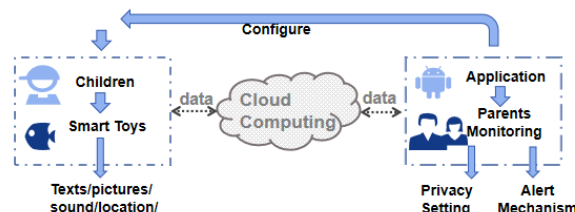


Figure 6: Participation of parental monitoring system.

Secondly, laws and regulations should be made and improved to better guide the development of toy computing. It has constantly been a question worth to be considered with attention about the online security and privacy of children, and it should be taken seriously by toy computing as well. In order to be more effective and straightforward, laws and regulations should consider toy computing, including its physical devices and computing services, to follow the requirements with parental guidance and monitoring. However, there is no law that clearly defines the unique environment of toy computing. For this reason, it is necessary to outline the privacy and security requirements to present a solution for managing the privacy of the toy computing environments. The toy industry has also enacted toy

safety regulations; however, these regulations do not mention privacy.

Nevertheless, there are still relatively few worldwide laws that deal exclusively with online privacy protection for children, for instance, Children’s Online Privacy Protection Act of United States.

Last but not the least, it is essential for smart connected toys to build a comprehensive framework involving all the stakeholders related. In order to reduce the risk of ethical problems, five principles are proposed below (see Table 3).

Table 3: Five principles for the smart connected toys.

Principles	Explanation in details
Authentication	Only children and parents can check the information to avoid malicious attack
Encryption	Hackers can not read data directly only if they know the secret key of decryption
Updates	Regular testing and updates the smart connected toys should be performed to minimize vulnerabilities.
Disclosure	It is essential to clearly disclose privacy-related policies involving the process of collecting and sharing data, and the data collection should be limited within secure protocol.
Control	Consumers should have the ownership to transfer and remove the data collected by the smart connected toys.

These five principles can be effectively and carefully used together in all different usage scenarios, including children involved in taking images and videos, voice records, video conferencing, and also storing data to and retrieving data from the cloud. Therefore, to keep smart connected toys away from ethical problems can be a collective responsibility. Not only the policy makers and consumers themselves, but also the vendors of smart connected toy and distribution channels should obey the above five principles and fulfil their roles in smart connect toys industry. For the vendors and its supply chain, they should design and manufacture

smart toys under these principles, and the distribution channels can use these principles as a filter to determine which brand of smart connected toys to carry and retail.

5 CONCLUSIONS

In summary, it is widely acknowledged that children’s data is extremely sensitive which means that people should especially pay the attention to the personal information of children by parents (Hinske and Langheinrich 2009). Ethical problems pose the threat of physical and psychological harm to child user. So it is essential to proposal a framework, which can achieve these ethical goals to protect the sensitive information of their children by enhancing parental control, improving the regulation and legislation, and arousing all the stakeholders’ awareness of privacy and security. We do believe that the framework can facilitate quick and effective comparison of smart toys ethic practices in future, and be useful to parents, governments, policy makers and toy manufacturers.

REFERENCES

AlHarchy, K., and Shawkat, W. (2013). Implement network security control solutions in BYOD environment. the 2013 IEEE International Conference on Control System, Computing and Engineering (ICCSCE), pp. 7 - 11.

Castle, R., Klein, G. and Murray, D.W., 2008, September. Video-rate localization in multiple maps for wearable augmented reality. In 2008 12th IEEE International Symposium on Wearable Computers (pp. 15-22). IEEE.

Daniel E. O’Leary. (2016) ‘Ethics for Big Data and Analytics’. IEEE Computer Society, 1541-1672/16, pp. 81-84R [Online]. Available from: www.computer.org/intelligent (Accessed: July/August 2016).

Digital Advertising Alliance. (2013). Application of Self-Regulatory Principles to the Mobile Environment. Digital Advertising Alliance. Retrieved from http://mmaglobal.com/files/whitepapers/DAA_Mobile_Guidance.pdf

Gartner. (2014). Gartner says 4.9 billion connected “things” will be in use in 2015. Retrieved from <http://www.gartner.com/newsroom/id/2905717>

Hadžović, S., Šerval, D. and Kovačević, S., 2015, May. Regulatory aspects of child online protection. In 2015 38th International Convention on Information and

- Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 409-412). IEEE.
- Hinske, S., Langheinrich, M.: An infrastructure for interactive and playful learning in augmented toy environments. In: The IEEE International Conference on Pervasive Computing and Communications (PerCom 2009), pp. 1-6 (2009).
- Hung, P. C., Fantinato, M., & Rafferty, L. (2016, June). A Study of Privacy Requirements for smart connected toys. In PACIS (p. 71).
- Hung, P. C., Iqbal, F., Huang, S. C., Melaisi, M., & Pang, K. (2016, July). A glance of child's play privacy in smart connected toys. In International Conference on Cloud Computing and Security (pp. 217-231). Springer, Cham.
- Johnson, M.E., 2001. Learning from toys: lessons in managing supply chain risk from the toy industry. *California Management Review*, 43(3), pp.106-124.
- Jones, M. L., & Meurer, K. (2016, May). Can (and should) Hello Barbie keep a secret?. In *Ethics in Engineering, Science and Technology (ETHICS)*, 2016 IEEE International Symposium on (pp. 1-6). IEEE.
- Kanev, K., 2012, June. Augmented tangible interface components and image based interactions. In *Proceedings of the 13th international conference on computer systems and technologies* (pp. 23-29). ACM.
- Kanev, K., Oido, I., Hung, P.C., Kapralos, B. and Jenkin, M., 2015. Case study: approaching the learning of kanji through augmented toys in Japan. In *Mobile services for toy computing* (pp. 175-192). Springer, Cham.
- Kathryn Montgomery (2015) 'Children's Media Culture in a Big Data World', *Journal of Children and Media*, 9:2, 266-271, DOI: 10.1080/17482798.2015.1021197
- Martin, K. E. (2015). 'Ethical issues in the big data industry.' *MIS Quarterly Executive* 14:2, 2015. . Available at SSRN: <https://ssrn.com/abstract=2598956>
- McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., & Roesner, F. (2017, May). Toys that listen: A study of parents, children, and internet-connected toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 5197-5207). ACM.
- Moustafa Mahmoud. (2018). An experimental evaluation of smart connected toy's security and privacy practice, Thesis (MA), Concordia University.
- Noor, R., Noor Sahila Syed Jamal, S., and Hafizzee Zakaria, K. (2012). Parental mobile control system for children's internet use. 2012 International Conference on Information Society (i-society), pp. 511 - 513.
- O'Leary, D.E., 2013. Exploiting big data from mobile device sensor-based apps: Challenges and benefits. *MIS Quarterly Executive*, 12(4).
- White, G. and Ariyachandra, T. (2016). 'BIG DATA AND ETHICS: EXAMINING THE GREY AREAS OF BIG DATA ANALYTICS.' *Information Systems*, 17.
- Rafferty, L., Fantinato, M. and Hung, P.C., 2015. Privacy requirements in toy computing. In *Mobile Services for Toy Computing* (pp. 141-173). Springer, Cham.
- Saint John Walker (2014) 'Big Data: A Revolution That Will Transform How We Live, Work, and Think', *International Journal of Advertising*, 33:1, 181-183, DOI: 10.2501/IJA-33-1-181-183
- Salomon, D. (2010). Privacy and Trust. In *Elements of Computer Security, Undergraduate Topics in Computer Science* (pp. 273-290). Springer. Retrieved from: http://link.springer.com/chapter/10.1007/978-0-85729-006-9_11
- Shute, V.J., Ventura, M., Bauer, M. and Zapata-Rivera, D., 2009. Melding the power of serious games and embedded assessment to monitor and foster learning. *Serious games: Mechanisms and effects*, 2, pp.295-321.
- Streiff, J., Kenny, O., Das, S., Leeth, A., & Camp, L. J. (2018, April). Who's Watching Your Child? Exploring Home Security Risks with Smart Toy Bears. In *Internet-of-Things Design and Implementation (IoTDI)*, 2018 IEEE/ACM Third International Conference on (pp. 285-286). IEEE.
- Sun, G., Huang, S., Bao, W., Yang, Y. and Wang, Z., 2014, August. A privacy protection policy combined with privacy homomorphism in the internet of things. In *2014 23rd International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-6). IEEE.
- Sung, J.Y., Levisohn, A., Song, J.W., Tomassetti, B. and Mazalek, A., 2007, March. Shadow Box: an interactive learning toy for children. In *2007 First IEEE International Workshop on Digital Game and Intelligent Toy Enhanced Learning (DIGITEL'07)* (pp. 206-208). IEEE.
- Tanaka, F. and Kimura, T., 2009, September. The use of robots in early education: a scenario based on ethical consideration. In *RO-MAN 2009-The 18th IEEE International Symposium on Robot and Human Interactive Communication* (pp. 558-560). IEEE.
- Taylor, E., & Michael, K. (2016). Smart Toys that are the Stuff of Nightmares. *IEEE Technology and Society Magazine*, 35(1)
- Tene, O. and Polonetsky, J., 2012. Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop.*, 11, p.xxvii.

- Thorpe, J.H. and Gray, E.A., 2015. Big data and public health: navigating privacy laws to maximize potential. *Public Health Reports*, 130(2), pp.171-175.
- Tyni, H., Kultima, A. and Mäyrä, F., 2013, October. Dimensions of hybrid in playful products. In *Proceedings of International Conference on Making Sense of Converging Media* (p. 237). ACM., 8-10
- Valente, J., & Cardenas, A. A. (2017). Security & Privacy in smart connected toys. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy* (pp. 19-24). ACM.
- Vlajic, N., El Masri, M., Riva, G. M., Barry, M., & Doran, D. (2018, October). Online Tracking of Kids and Teens by Means of Invisible Images: COPPA vs. GDPR. In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security* (pp. 96-103). ACM.
- Wessel, M., 2016. How big data is changing disruptive innovation. *Harvard Business Review*, 27.
- Westeyn, T.L., Abowd, G.D., Starner, T.E., Johnson, J.M., Presti, P.W. and Weaver, K.A., 2012. Monitoring children's developmental progress using augmented toys and activity recognition. *Personal and Ubiquitous Computing*, 16(2), pp.169-191.
- Yankson, B., Iqbal, F., & Hung, P. C. (2017). Privacy preservation framework for smart connected toys. In *Computing in smart connected toys* (pp. 149-164). Springer, Cham.