IRIE
International Review of Information Ethics Vol. 27 (12/2018)

Vol. 27 (11/2018)

Ethical Issues of Networked Toys

edited by Juliet Lodge and Daniel Nagel

Editors of this issue:

Prof em. Dr. Dr. Juliet Lodge
University of Leeds; Member, Privacy Expert Group, Biometrics Institute (London);
Senior analyst, Saher Ltd.

Dr. Daniel Nagel
SGT Rechtsanwälte, Stuttgart, Germany

Editors of IRIE

  ISSN 1614-1687

Vol. 27 (11/2018)

Content:

  ISSN 1614-1687

Editorial: On IRIE Vol. 27

Technology is ubiquitous: boundaries between the world we live in and the internet become more and more blurred thanks to networked objects. The borders that once separated the sanctity and privacy of our home from our online lives have been dissolved through the advent of the Internet-of-Things (IoT), encompassing even those realms traditionally reserved as secure places for development: childhood and children's toys. Traditional early childhood development, once founded on the safety of interactions within a closed circle of peers and family, has now been augmented with digital realities and externally networked connections. Questions must be posed as to how the introduction of digitally networked toys affects childhood, both negatively and positively, and most certainly in ways not yet fully understood. How might 'robo-toys' affect the experience of childhood and influence early childhood development, and how will they shape new online and off-line expectations?

Early research and application in this area requires a thorough ethical review – a scholarly task that we want to initiate with the following issue – where we will explore the challenges, benefits and pitfalls of networked toys.

For over a decade, the International Review of Information Ethics has led the charge in exploring new frontiers of ethics and technology, such as networked toys. Having covered topics ranging from robotics to religion, IRIE has ventured some of the most thought-provoking conversations of the digital age. These types of conversations are just getting started. The editors are proud to announce that after 15 years of publication under the leadership of IRIE Founders, Editor-in-Chief, Professor Rafael Capurro, alongside Dr. Felix Weil, whose operative management of IRIE has been key to its success, alongside Professor Thomas Hausmanninger, IRIE will re-launch in 2019, hosted by the Kule Institute for Advanced Study (KIAS) at the University of Alberta, Canada. The journal will undergo a new design and will adopt a renewed commitment to its editorial advisory board.

The transfer of the journal will accompany the relaunch of the International Center for Information Ethics, also to be hosted at the University of Alberta under a new administration and website. The editors at IRIE consider it a privilege to have worked closely with Professor Rafael Capurro for the last two decades and wish him the very best for his well-deserved retirement. IRIE looks forward to several forthcoming editions, including a special edition honoring the life and work of Norbert Wiener, an edition on Information Ethics (IE) where a critical examination of the field of IE will address the origins and evolutions of the field, and an edition on Ethics in Artificial Intelligence.

Sincerely yours,

the editors of IRIE

ISSN 1614-1687

Juliet Lodge, Daniel Nagel:

Introductory Remarks to the Ethical Issues of Networked Toys

Sunni the plush gummy bear is silently sitting on the bookshelf in the dorm room of three-year-old Hannah. Sunni has a green dress, a fluffy body, big eyes with beautiful eyelashes and a built-in camera with Wi-Fi connection. Hannah is sound asleep while the cameras humming motor keeps adjusting to monitor Hannah's breathing rhythm and to count phases of potential apnea. At the same time, a high-resolution picture of Hannah is transmitted to both her parent's screen in the living room and a remotely accessible server in case that Hannah's parents go out for dinner. The latter is only accessible through a secured password, or so the parents hope.

A settlement between the FTC and VTECH, a manufacturer of connected toys, earlier this year showed that any connection is only as good as its weakest link, which in this case was the poor safeguarding of the collected sensitive data by VTECH.[1] VTECH operates Kid Connect, a messaging tool for minors, where parents can control the settings and thus the contacts their children have. In order to provide this service VTECH collects a surprisingly conclusive amount of data from both parents and their children. VTECH claimed to only store the respective data encrypted. They, however, failed to prevent hackers from gaining access to the data including pictures of children, data about their age and their home addresses. VTECH and FTC settled on a fine of 650,000.00 $ as well as on yearly audits of the realization of a comprehensive data protection program. Other reports unfortunately do not sound more reassuring and include inter alia a loss of voice recordings taken by toys,[2] Bluetooth back-doors for interactive dolls,[3] as well as snooping via smartwatches.[4]

While some states and toymakers have reacted,[5] the best first step to approach this is to take a step back and have a closer look at the underlying issues.

Networked toys - Artificial guardians for little princesses or demonic plastic princes?

Networked toys dominate the shelves in toy stores at a time when neither their real benefits nor their potentially latent dangers have been fully explored. Do hyper-connected toys transform the relationship between adults, the child and its environment? Do they shape their minds and predispose them to seek convenience and speedy responses rather than rely on their own autonomous capacities for critical thought?

Questions such as who really is in control arise, both of the toys - parents, third parties or even the toddlers themselves - and of data (including biometrics) that might be collected for unclear purposes and opaque

[1] https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated

[2] Lorenzo Franceschi-Bicchierai, Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings, https://motherboard.vice.com/en_us/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings

[3] Bundesnetzagentur zieht Kinderpuppe „Cayla" aus dem Verkehr, Press Release of 17 February 2017 https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Presse/Pressemitteilungen/2017/27012017_cayla.pdf?__blob=publicationFile&v=2

[4] Bundesnetzagentur geht gegen Kinderuhren mit Abhörfunktion vor, Press Release of 17 November 2017, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Presse/Pressemitteilungen/2017/17112017_Verbraucherschutz.pdf?__blob=publicationFile&v=2

[5] Cf. E.g. Germany banning smartwatches for children (see Fn 4) or Mattel stopping the production of a toy AI device, Haley Tsukayama, Mattel Has Canceled Plans for a Kid-Focused AI Device That Drew Privacy Concerns, Wash. Post (Oct. 4, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/04/mattel-has-an-ai-device-to-soothe-babies-experts-are-begging-them-not-to-sell-it.

ISSN 1614-1687

destinations. For what specific or linkable purpose and above all where and to whom is data transmitted? What ethical considerations should be addressed?

Is there an actual benefit for the children themselves? Do hyper connected devices and robo-toys teach them how to handle technology or does it erode their capacity for autonomous reflection as speed and convenience are prioritised in their on-line and off-line worlds? Do such toys presage fundamental transformation of childhood and the imagined and physical worlds?

Ulrich Gasper takes the lead in adressing these important questions in this issue by shedding light on the impact of networked toys in the playground, while Rocco Panetta and Federico Satore depict the legal backdrop which serves as a basis for any evaluation of such toys. Finally, Isabelle Moeller answers critical questions on the qualification and use of biometrics and artificial intelligence in respect to children.

Ulrich Gasper:

Children at Play: Thoughts about the impact of networked toys in the game of life and the role of law

Abstract:

Information communication technology is spreading fast and wide. Driven by convenience, it enables people to undertake personal tasks and make decisions more easily and efficiently. Convenience enjoys an air of liberation as well as self-expression affecting all areas of life. The industry for children's toys is a major economic market becoming ever more tech-related and drawn into the battle for convenience. Like any other tech-related industry, this battle is about industry dominance and, currently, that involves networked toys. Networked toys aim to enhance convenience for children and parents alike. Increasingly difficult to resist, these convenient networked devices are also a societal game changer. Neatly nestled in a lacuna juris and surrounded by a lack of clinical evidence, networked toys raise complex ethical issues concerning human development. This article lays bare the regulatory nexus for networked toys and invites ethical thinking to fill the gap to ensure sufficient protection for all human developmental stages. Networked toys not only affect but also might interfere with child development. Therefore, the article initially summarises the four key psychological stages through which the neurological development of the human brain processes. Each of these stages involves vital windows for human development in cognitive, emotional and social dimensions. Missing any of these developmental windows changes an individual human for life. The article then takes a look at the two main legal frameworks protecting the stages of human development which are applicable to networked toys: First, the examination of the human rights framework with its major segments emanating from the fundamental rights to privacy for family and home, to a child's education as well as to personal data reveals the use of current networked toys as a shielded part of parenting which tends to be at odds with privacy and data protection requirements. Second, the product liability framework for toy manufacturers requires evidence-based causality for putting a child's safety at risk. Unfortunately, these legal frameworks fail to offer sufficient protection of the human developmental stages. There is a lacuna juris. Although networked toys involve the risk of negatively impacting human development in every dimension, clinical psychological studies are impossible to acquire as court evidence for product liability because they take too long to provide reliable data while exposing several generations of children to the examined risk in the process. Meanwhile the temptation of convenience continues to drive the industry and consumers of networked toys and devices, which are already impacting children of all age groups. Accepting this phenomenon as an element of cognitive dissonance in society and in science falls far short of an appropriate ethical balance. The need for creating such an ethical balance concerning networked toys is all the more imperative because even if the networked toy industry managed to eliminate all psychological risks for human development and every legal conflict with privacy and security, significant ethical and societal risks of networked toys remain due to inevitable technological bias. Against these mounting changes, it is suggested that only an ethical approach of interdisciplinary research and learning seems most promising to develop an appropriate equilibrium between the complex challenges posed by networked toys and the societal values at stake.

Agenda:

ISSN 1614-1687

Author:

- **Ulrich Gasper LL.M.**
- Attorney at law at Selting Rechtsanwälte, Selting Rechtsanwälte, Schildergasse 32-34, 50667 Köln
  ·+ 49 -221 –126990, gasper@selting.com, ··www.selting.com)
- managing editor of two IT-law journals published by Verlag Dr. Otto Schmidt KG, Gustav-Heinemann-Ufer 58, 50968 Köln:
  "Computer Law Review International" (CRi, cr-international.com) and
  "Computer und Recht" (CR, cr-online.de)
- Relevant publication:
  - Arnold Roosendahl, Mari Kert, Alison Lyle, Ulrich Gasper. Data Protection Law Compliance for Cybercrime and Cyberterrorism Research. In: Babak Akhgar, Ben Brewster (Eds.), Combatting Cybercrime and Cyberterrorism. Springer, 2016. p. 81.

Children at Play

Thoughts about the impact of networked toys in the game of life and the role of law.

Networked devices including networked toys involve complex ethical issues for parents and children. The neurological development of a human brain (I.1.a)) processes through four different psychological stages each of which involves vital windows for development in the cognitive, the emotional and the social dimension (I.1.b). The development in these three dimensions is crucial for the individual and for society and, therefore, protected by fundamental rights and guarantees (I.2.a). Networked toys seem to be at odds with privacy and data protection requirements (I.2.b)). They also involve the risk of negatively impacting the cognitive, emotional and social dimension of human development (II.1.). This probably relates to cognitive dissonance in society and in science (II.2.). Even if the psychological risks for human development and the legal conflict with privacy and security were ironed out, significant ethical and societal risks of (ideal) networked devices/toys remain (II.3.). The set-up of the legal framework necessarily involves a vulnerability to all ethical and societal risks posed by networked toys, so that an ethical approach of interdisciplinary research and learning seems most appropriate to develop an acceptable equilibrium between the complex challenges of networked devices/toys and the societal values at stake (III.).

I. Children and Networked Toys

According to the German classic Friedrich Schiller "man is only fully a human being when he plays".[1] Through play humans can rise above natural urges and ethical restrictions and enjoy, however briefly, freedom and completeness.[2] While Schiller developed his concept of the play-drive in contemplation of the noble play of the beautiful arts, the play considered in this article is confined to children and networked toys. Using a networked device may bring out the child in anyone at some point. Using their innovative and smart functions more often than not feels like playing with a new toy. After all, this is part of their appeal. An entire cyberspace world is at one's fingertip. Networked devices are fun, cool and smart for all. Nevertheless, human societies have grown to distinguish between adults and children. This has to do with the human brain being born remarkably unfinished. Instead of arriving with everything wired up ("hardwired") the human brain allows itself to be shaped by the details of life experience causing long periods of helplessness as the young brain slowly moulds into its environment ("livewired").[3]

1. Stages of Human Development

From a legal perspective, reaching the age of eighteen turns a human into an adult who is a fully responsible member of society and does not require parental permission for concluding legally binding contracts any more.

[1] Schiller, *On the Aesthetic Education of Man in a Series of Letters*, (letter 15), p. 107, took the reciprocal view that a human only plays whenever he is in the full meaning of the word human, and that he only is human when he plays: "der Mensch spielt nur, wo er in voller Bedeutung des Wortes Mensch ist, und er ist nur da ganz Mensch, wo er spielt." (V, 618) cited according to Hoffmeister, Wörterbuch der philosphischen Begriffe", 2. Edition, 1955, p. 573.

[2] Safranski, „Schiller oder Die Erfindung des Deutschen Idealismus", 2004, p. 413 - 415.

[3] Eagleman, The Brain,2015, p. 6.

a) Neurological Approach

From a neurological perspective, the human brain's transformations of childhood and adolescence continue until the age of twenty-five by when the tectonic shifts in human identity and personality have ended and the brain appears to be fully developed.[4] The most significant changes in the human brain occur during childhood and adolescence. Perhaps surprisingly, the number of brain cells is the same in children and adults and the flexibility appears in how those cells are connected:[5]

- At birth, a brain's neurons are disparate and unconnected. In the first two years, the neurons begin connecting up rapidly as they take in sensory information and as many as two million new synapses are formed every second.
- By the age of two, the human brain has built twice as many synapses as an adult brain. At this peak number of synapses, the human brain adopts a strategy of neural "pruning".
- During childhood, the human brain pairs back about fifty percent of its synapses keeping and strengthening only those synapses which successfully participate in a circuit because they are used for interacting with the actual environment of the human.[6] This developmental strategy of matching a human brain to its environment is smart but runs the risk of losing vital connections if the environment is deprived of emotional care and cognitive stimulation.[7]
- At the beginning of adolescence, just before the onset of puberty, the prefrontal cortex of the human brain sprouts new cells and new synapses initiating a second phase of neural "pruning" which lasts about a decade.[8]
- During the teenage years the volume of the prefrontal cortex comprising the areas required for higher reasoning and the control of urges, reduces by about one percent per year.[9]

While in adulthood after the age of twenty-five, experience continues to shape the physical structure of the human brain by exploiting its plasticity,[10] the neurological perspective reveals that the brain develops the identity and personality of a human by a process of constant neural "pruning" back of connecting synapses during childhood and teenage years. Like paths in a forest, connections are lost if they are not used.

b) Psychological Approach

The neurological perception appears to adequately match one of the most influential theories of cognitive development proposed by Jean Piaget. Focussing on how human thought processes develop and influence the way we understand and interact with the world, Piaget suggested the following four stages of cognitive development:[11]

[4] Eagleman, The Brain, 2015, p. 18.

[5] Eagleman, The Brain, 2015, p. 7.

[6] Eagleman, The Brain, 2015, p. 9.

[7] Eagleman, The Brain, 2015, p. 10 and 13.

[8] Eagleman, The Brain, 2015, p. 15.

[9] Eagleman, The Brain, 2015, p. 15.

[10] Eagleman, The Brain, 2015, p. 18-20.

[11] The following description of Piaget's four stages of cognitive development draws on Cherry, "Piaget's Theory: The 4 Stages of Cognitive Development", 14 May 2017 available at: https://www.verywell.com/piagets-stages-of-cognitive-development-2795457.

- Sensorimotor Stage: Between birth and age 2, infants know the world through their movements and sensations. During the final part of this stage infants learn that things continue to exist even though they cannot be seen ("object permanence") and that they are separate beings from the people around them.
- Preoperational Stage: Between ages 2 and 7, children learn to use words and pictures to represent objects. During this stage, children tend to be egocentric and struggle to see things from the perspective of others while they still think about things in very concrete terms.
- Concrete Operational Stage: Between ages 7 and 11, children begin thinking logically about concrete events, but struggle with understanding abstract or hypothetical concepts. Children become less egocentric and begin to think about how other people might think and feel while more and more realising that their own thoughts are unique to them.
- Formal Operational Stage: Between age 12 and adulthood, teenagers develop the ability to think about abstract concepts. Skills such as logical thought, deductive reasoning, and systematic planning also emerge during this stage.

Piaget's cognitive developmental theory suggests that there is a *qualitative* change in how children think as they gradually progress through these four stages. The cognitive development is heavily influenced by children's play experiences, but is not the only dimension in which children develop. Besides the physical dimension, there are also the emotional and the social dimension which are also shaped by their play:

- Cognitive development includes creativity, discovery, language skills, verbal judgment and reasoning, symbolic thought, problem-solving skills, and the ability to focus and control behaviour.
- Emotional development includes feelings of happiness, feelings of power over the environment, emotional awareness, sensitivity to others, emotional strength and stability, spontaneity, humour, and feelings about self.
- Social development occurs largely during children's play interactions, as children learn to play in larger and larger groups, and as they begin to learn about appropriate behaviours within certain contexts.

All four dimensions (physical, cognitive, emotional, social) are affected when a child plays in its given environment.

c) Windows of Time

Both the neurological and the psychological approach suggest that there are particular time windows in the formative years of a human within which very specific cognitive developments have to take place and skills need to be learned. Once those windows for cognitive development have closed, the growing human being is affected by these cognitive capabilities for life. The development of the brain is smart and reflects human evolution which continues to adapt to its environment. Networked devices have been part of this environment for more than a decade. At first, networked devices like smartphones or tablets became toys for children with apps and games running on the device. Then or simultaneously, networked devices were instrumentalised as parental assistants. Networked toys specifically targeted to children seem to be a rather recent phenomenon.

2. Networked Toys: Between Fundamental Rights and Duties

Networked toys for children share key functionalities of networked devices like smartphones or tablets. They all can connect to the internet via a hotspot or mobile phone network and mostly also offer a bluetooth connection as well. As toys for the non-adult, they are marketed as an expression of parental care for the child. From a legal perspective, parental care for a child may be viewed as a balance between fundamental human rights of the parents and of the child. This balance is supplemented in most societies by the state providing education and subsidiary care for the child.

a) Relevant Fundamental Rights

At global level, the Universal Declaration of Human Rights (UDHR)[12] enshrines in Art. 16 paragraph 2 UDHR the family as the natural and fundamental group unit of society. Though everyone (including children) has the right to education[13], parents enjoy according to Art. 26 paragraph 3 UDHR a prior right to choose the kind of education that shall be given to their children. The right to privacy in Art. 12 UDHR protects anyone's privacy, family home and correspondence from arbitrary interference.

The international community has committed to ensuring the rights of a child through the adoption of the Convention on the Rights of the Child[14] (CRC) in 1989. According to Art. 18 paragraph 1 sentence 2 CRC, parents have the primary responsibility for the upbringing and development of the child. According to Art. 31 paragraph 1 CRC, the state has to recognise the right of the child to engage in play and recreational activities appropriate to the age. The right to privacy for a child in Art. 16 paragraph 1 CRC is identical to the right to privacy in Art. 12 UDHR. Further, while respecting the responsibilities, rights and duties of parents, the state is required to provide appropriate directions and guidance in the child's exercise of the rights recognised in the CRC. So far and perhaps surprisingly, out of the 140 signatory states only the United States of America has yet to ratify the Convention on the Rights of the Child after having signed it in 1995.[15]

At regional level, the Member States of the Council of Europe base their guarantee of human rights not only on the UDHR, but also on the European Convention for the Protection of Human Rights and Fundamental Freedoms[16], better known as the European Convention on Human Rights (ECHR). The ECHR guarantees the right to respect private and family life (privacy) in Art. 8 ECHR. The right to education is enshrined in Art. 2 of Protocol No. 1 to the EHCR and demands that the Member States respect the right of parents to ensure the child's education and teaching.

Also at regional level, the Member States of the European Union have to respect human rights and the rule of law not only because of their obligations under the ECHR and the UDHR, but also because of the Charter of Fundamental Rights of the European Union (EU-Charter). The EU-Charter guarantees the right to respect for private and family life, home and communications in Art. 7 EU-Charter and the right to protection of personal data in Art. 8 EU-Charter. As of May 2018, the General Data Protection Regulation (GDPR) introduces for the first time special data protection regulations for children.[17] Children have the right to such protection and care as is necessary for their well-being, according to Art. 24 paragraph 1 EU-Charter, and the family enjoys legal, economic and social protection, Art. 33 paragraph 1 EU-Charter.

Against the background of these international human rights obligations, it is hardly surprising that states place the care for what is in the best interest of the child first and foremost on the parents at national level as well.

[12] United Nations, General Assembly, Universal Declaration of Human Rights (UDHR) Resolution 217 A, A/RES/3/217 A, 10 December 1948.

[13] Art. 26 paragraph 1 sentence 1 UDHR.

[14] United Nations, General Assembly, Resolution 44/25, „Convention on the Rights of the Child", adopted on 20 November 1989, entry into force on 2 September 1990.

[15] The USA merely signed the Convention on the Rights of the Child in 1995. See United Nation's High Commissioner for Human Rights web site at https://treaties.un.org/pages/viewdetails.aspx?src=ind&mtdsg_no=iv-11&chapter=4&clang=_en.

[16] Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols Nos. 11 and 14 and supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13), 4 December 1950.

[17] On the special regulations for the protection of children within the GDPR: Kress/Nagel, CRi 2017, p. 6-9.

The arrangement of parental care usually enjoys constitutional status[18] and one of its key protection mechanisms is the guarantee of privacy for family and home.[19]

b) Relevant Networked Toys

Any networked device inevitably produces, collects and transfers data. Using the accrued data is the whole point of networked devices including networked toys. From a legal perspective, there are three key questions regarding this use of the data: (i) How are the data collected? (ii) How are the data transferred? (iii) Who may access to the data? These three questions allow to identify three types of networked toys relevant as far as the fundamental guarantee of privacy for family and home is concerned:

aa) Banned Toys

The tension between privacy and how data are collected has led the German legislator to prohibit any misuse of transmitting equipment. Section 90 paragraph 1 sentence 1 German Telecommunications Act prohibits owning, manufacturing, marketing, importing or otherwise introducing any transmitting equipment which is particularly suitable for intercepting the non-publicly spoken words (or for taking pictures) of another person without being detected because it is mistaken as something else or disguised under an object of daily use. This provision is not specifically designed to protect children, but in 2017 two different networked toys were prohibited based on this provision:

In February 2017, the Federal Network Agency (Bundesnetzagentur) banned the networked fashion doll "Cayla" manufactured and sold by Genesis Toys from the German market.[20] "Cayla" answers fact-based questions, plays games, reads stories, and even solves math problems. Genesis Toys uses third-party voice-recognition software by a U.S.- based company, and the doll requires an iOS/Android application to use the software. The doll's mobile application researches and supplies "Cayla" with factual answers to questions, but it also prompts children to set their physical location, parents' names and school name.[21] The parental consent for collecting children's personal information was obtained when the user downloaded the mobile application and agreed to the terms of service. However, also a child could click agree in the mobile application and also solve the simple-addition question for verification of a human user. In June 2017, this has lead the U.S. Federal Trade Commission (FTC) to add networked toys, children's products collecting personal information and voice-activated devices to the products and services covered by the Children's Online Privacy Protection Act (COPPA) and to require a knowledge-based authentication for consent that only a parent could answer.[22]

[18] See e.g. (cited according to www.constituteproject.org): Art. 6 paragraph 2 of the German Constitution: Art. 63 of the Croatian Constitution; Art. 32 paragraph 4 Czech Charter of Fundamental Rights and Basic Freedoms; Art. XVI paragraph 2 Hungarian Constitution; Art. 48 paragraph 1 Polish Constitution; Art. 38 paragraph 2 Russian Constitution.

[19] In the USA the Children's Online Privacy Protection Act (COPPA) makes it illegal to gather data on children under 13 without parental permission, 15 U.S. Code §6502(a)(1).

[20] Bundesnetzagentur, "Bundesnetzagentur zieht Kinderpuppe „Cayla" aus dem Verkehr", press release, 17 February 2017.

[21] Buffington/Dharmadasa, "Keeping Up with Cayla: Concerns over Interactive Toys Spur an FTC Update of COPPA Guidelines", 24 July 2017, available at: https://www.socialgameslaw.com/2017/07/coppa-ftc-interactive-toys-cayla.html#page=1.

[22] Cohen/Magee, "FTC updates COPPA compliance plan for business", FTC Business Blog, 21 June 2017 available at: https://www.ftc.gov/news-events/blogs/business-blog/2017/06/ftc-updates-coppa-compliance-plan-business; Buffington/Dharmadasa, "Keeping Up with Cayla: Concerns over Interactive Toys Spur an FTC Update of COPPA Guidelines", 24 July 2017, available at: https://www.socialgameslaw.com/2017/07/coppa-ftc-interactive-toys-cayla.html#page=1.

In November 2017, the Federal Networked Agency banned smartwatches for children which also function as secret audio observation device.[23] These banned smartwatches for children contain a SIM-card and function as mobile phone which connects to the parents' phone through a companion app not only allowing for realtime location tracking and direct communication with the child, but also enabling a parent to audio monitor the child's surroundings.[24] One such smartwatch is the Viksfjord watch distributed in Norway which was tested by the security company Mnemonic for the Norwegian Consumer Council.[25] The Viksfjord watch uses the companion app SeTracker which includes functions like geofencing and "monitoring". The "monitor" function allows the app user to send an SMS to the watch which makes the watch place a covert call to the parent phone resulting in a one-way conversation where the parent can listen in on the child (and their surroundings) without the child being aware of this happening.[26]

bb) Networked Toys Without Security or Privacy

The security of a networked device including networked toys concerns the questions of how the data are transferred and who may access the data.

Apart from the Viksfjord watch, the Norwegian Consumer Council had three other smartwatches for children tested on their security and privacy standards because the main purpose of these smartwatches is to give parents peace of mind while their children play freely outside. The smartwatches and their companion app turned out to have critical flaws:

- Without the parents' knowledge, a potential attacker could take control of the companion apps and thereby not only gain access to the child's real-time and historical location and personal details but also enable them to contact the child directly.[27]
- Two safety-enhancing features intended to alert the parents were unreliable in practice luring the parents into a false sense of child safety: the "SOS button" for if the child is in distress and the "geofencing" function for whenever the child enters or leaves a designated area.[28]
- Only one smartwatch service asked for consent to the data collection. While this might still be evaluated as lawful according to Art. 6 paragraph 1 lit. (b) GDPR because the data processing is necessary for the performance of the contract, it is unlawful in non-EU jurisdictions requiring consumer consent.
- None of the smartwatches allows deletion of location history or a user account from its services at any point.[29] In the EU, this is in breach of Art. 17 paragraph 1 (a) GDPR which grants the consumer a right to erasure of personal data which are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- Further, Art. 5 paragraph 1 (c) GDPR prohibits any data processing which is incompatible with the explicit purposes for which the data was collected. However, while one companion app mentions that

[23] Bundesnetzagentur, „Bundesnetzagentur geht gegen Kinderuhren mit Abhörfunktion vor", press release, 17 November 2017.
[24] Forbrukerrådet, „#watchout – Analysis of smartwatches for children", October 2017, p. 3.
[25] Mnemonic, Security Assessment Report, „GPS Watches for Children", The Norwegian Consumer Council, 18 October 2017.
[26] Forbrukerrådet, „#watchout – Analysis of smartwatches for children", October 2017, p. 11.
[27] Forbrukerrådet, „#watchout – Analysis of smartwatches for children", October 2017, p. 3.
[28] Forbrukerrådet, „#watchout – Analysis of smartwatches for children", October 2017, p. 4.
[29] Forbrukerrådet, „#watchout – Analysis of smartwatches for children", October 2017, p. 19.

the children's personal data will be used for marketing purposes, the other three smartwatch services leave parents unclear how this information may or may not be used.[30]

- Finally, one of the smartwatch services transmits the unencrypted children's location data to China.[31] The transfer of personal data to a third country outside the EU requires an adequacy decision by the European Commission pursuant to Art. 45 GDPR basically stating that the third country ensures an adequate level of data protection. In the absence of such adequacy decision, appropriate safeguards, enforceable data subject rights and effective legal remedies for data subjects have to be provided, Art. 46 GDPR. Because the processing activity concerns not only a service rendered within the EU but also a monitoring of behaviour within the EU, the data processing in China has to comply with the GDPR, Art. 3 paragraph 2 (a) and (b) GDPR.

The vulnerability of a potential attacker taking control of the networked toy so that direct communication with the child is possible without the parents' knowledge, has been found in several other networked toys by consumer protection organisations. The degree of technical know-how for a potential attacker has been found to be zero in four and almost zero in three networked toys because the Bluetooth connection[32] had not been secured at all:[33]

- I-Oue Intelligent Robot is a colourful robot with a voice of its own which, among sound effects, talks back to the child aged 5+[34]. Anyone having downloaded the app to their smartphone or tablet and within Bluetooth range could start chatting by typing into a text field what will then be spoken to the child by the robot's voice which provides no clues as to who is speaking.[35]
- Furby Connect is a networked toy designed as cuddly furry "e-pet ball" talking back to the child aged 6+[36] and does not use any security features when pairing with a device via Bluetooth.[37]
- Toy-fi Teddy is a cuddly teddy with button on its chest or in one of its paws for the child aged 3+[38] to send and receive recorded messages and the Bluetooth connection lacks any authentication protection.[39]
- Wowwee Chip is a barkingrobot dog for children aged 8+ which listens to commands, follows its ball or the child and its Bluetooth connection has no security features.[40]

[30] Forbrukerrådet, „#watchout – Analysis of smartwatches for children", October 2017, p. 17-18.

[31] Forbrukerrådet, „#watchout – Analysis of smartwatches for children", October 2017, p. 4.

[32] Usually, Bluetooth has a range of about 10 metres, but there are methods for extending this range significantly.

[33] Which?, „Safety alert: how easy it is for almost anyone to hack your child's connected toy", 14 November 2017, available at: https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/;Stiftung Warentest, "Kinderleicht zu kapern", test 9/2017, 34f.

[34] Manufacturer recommended age.

[35] Which?, „Safety alert: how easy it is for almost anyone to hack your child's connected toy", 14 November 2017, available at: https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/; Stiftung Warentest, "Kinderleicht zu kapern", test 9/2017, 34, 35.

[36] Manufacturer recommended age.

[37] Which?, „Safety alert: how easy it is for almost anyone to hack your child's connected toy", 14 November 2017, available at: https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/.

[38] Manufacturer recommended age.

[39] Which?, „Safety alert: how easy it is for almost anyone to hack your child's connected toy", 14 November 2017, available at: https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/; Stiftung Warentest, "Kinderleicht zu kapern", test 9/2017, 34, 35.

[40] Stiftung Warentest, "Kinderleicht zu kapern", test 9/2017, 34, 35.

Networked Toys with Weak Security and Privacy

The degree of technical know-how for a potential attacker has been found to be minimal in three networked toys because their Bluetooth and WLAN[41] connection has only insufficient security features:[42]

- Cloud Pets is a stuffed networked toy for children between 3 and 7[43] which comes in bunny, cat, or dog varieties and enables parents to send messages to a child which are then played back on a built-in speaker. Bluetooth and WLAN connection are only secured with a password but no additional coding.[44] There is only little knowledge required for someone to hack the CloudPets and have their own messages played.
- Fisher-Price Smart Toy Bear or Monkey is a cuddly bear or monkey talking back to the child aged 3 to 8[45] and its Bluetooth and WLAN connection suffers the same vulnerability as the one of CloudPets.[46]
- Mattel Hello Barbie is for children aged 3+[47] which talks back to the child and its WLAN connection also suffers the same vulnerability as the one of CloudPets.[48]

For children below the age of 3 Mattel had planned a networked device especially designed for children called Aristotle which would switch on a night light to soothe a crying baby. For that age group, Aristotle was more for the parents combining home virtual assistant technology and a small camera as audio and visual baby monitor.[49] However, Aristotle was equipped with artificial intelligence enabling it to adjust its support activities even to the point where it could help a pre-teenager with homework.[50] At the beginning of October 2017, Mattel announced that it had cancelled its plans to sell this child-focussed smart hub because it did not "fully align with Mattel's new technology strategy" after the US-based Campaign for a Commerical-Free Childhood had labelled Aristotle as snooping intruder and two members of the US Senate voiced their concerns about the data being gathered, stored and shared by the device.[51]

[41] Wireless Local Area Network (WLAN).

[42] Which?, „Safety alert: how easy it is for almost anyone to hack your child's connected toy", 14 November 2017, available at: https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/;Stiftung Warentest, "Kinderleicht zu kapern", test 9/2017, 34f.

[43] Manufacturer recommended age.

[44] Stiftung Warentest, "Kinderleicht zu kapern", test 9/2017, 34, 36.

[45] Manufacturer recommended age.

[46] Which?, „Safety alert: how easy it is for almost anyone to hack your child's connected toy", 14 November 2017, available at: https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/; Stiftung Warentest, "Kinderleicht zu kapern", test 9/2017, 34, 36.

[47] Manufacturer recommended age.

[48] Stiftung Warentest, "Kinderleicht zu kapern", test 9/2017, 34, 37.

[49] Lee, „Mattel thinks again about AI babysitter", BBC, 5 October 2017, available at: http://www.bbc.com/news/technology-41520732.

[50] Tsukayama, „Mattel has cancelled plans for a kid-focused AI device that drew privacy concerns", Washington Post, 4 October 2017, available at: https://www.washingtonpost.com/news/the-switch/wp/2017/10/04/mattel-has-an-ai-device-to-soothe-babies-experts-are-begging-them-not-to-sell-it/?utm_term=.d63f3e8642ff.

[51] Lee, „Mattel thinks again about AI babysitter", BBC, 5 October 2017, available at: http://www.bbc.com/news/technology-41520732; Tsukayama, „Mattel has canceled plans for a kid-focused AI device that drew privacy concerns", Washington Post, 4 October 2017, available at: https://www.washingtonpost.com/news/the-switch/wp/2017/10/04/mattel-has-an-ai-device-to-soothe-babies-experts-are-begging-them-not-to-sell-it/?utm_term=.d63f3e8642ff.

While Mattel ultimately cancelled Aristotle, Amazon unveiled the first child-focussed apps for its networked virtual assistant device Echo in summer 2017 including a version of SpongeBob[52] and Sesame Street[53]. Earlier in March 2017, Google rolled out its Family Link app aimed at parents and enabling them to control their children's usage of (Android) networked devices by (i) managing the apps available to their child, (ii) regulating the child's screen time, and (iii) remotely locking the child's device for bedtime and other priorities.[54] In the first week of December 2017, Facebook launched its Messenger Kids app aimed at users under the age of thirteen and allowing them to send texts, videos and photos on which they can also draw or ad stickers to.[55] Because any voice request to Amazon's Echo and any communication with Facebook's Messenger Kids app inevitably leads to collecting a child's data, Amazon and Facebook require parents to verify their identities before their children can use the apps to meet the requirement of parental consent necessary under the US Children's Online Privacy Protection Act (COPPA).[56] This neatly leads to the observation that such parental consent is also required whenever children[57] use their parents' networked virtual assistant device be it Alexa (Amazon), Bixby (Samsung), Cortana (Microsoft), Google Assistant or Siri (Apple).[58]

3. Stakeholders and Applicable Legal Frameworks

The neurological and the psychological approach revealed key constants in the development of a human being from childhood to adulthood. Most importantly, there are time windows in the formative years when specific skills are either acquired or not. The growing human beings are children and teenagers, while fully grown human beings may be parents. Both, the child and the parents enjoy fundamental rights and freedoms concerning the child's development which have to be balanced against each other by each national state.

While the child has the right to education[59], the parents have a prior right to choose the appropriate education for their children[60] and the education shall be directed to the full development of the human personality[61] (Art. 26 UDHR). Further, the balance of fundamental rights gains complexity when the manufacturers of networked devices including networked toys are taken into account as third relevant stakeholder. These manufacturers enjoy the fundamental right to realise their economic right (Art. 22 UDHR) and the market share for networked toys is expected to triple by 2020.[62] The fourth stakeholder is the national state which is in many EU and other

[52] Nickelodeon's SpongeBob Challenge.

[53] Sesame Workshops' Sesame Street.

[54] Since September 2017, Google's Family Link app is available throughout the US without an invitation, with three basic groups of controls ready for use, see: Lawler, "Google opens up 'Family Link' parental controls for Android", engadget 29 September 2017, available at: https://www.engadget.com/2017/09/29/google-family-link-controls-android/.

[55] Tsukayama, "Facebook's new messaging app deepens debate over kids' social-media use", The Washington Post, 4 December 2017, available at: https://www.washingtonpost.com/news/the-switch/wp/2017/12/04/facebook-now-has-a-messenger-app-just-for-kids/?utm_term=.76bb16fe8bff.

[56] Darrow, "Amazon Wants More Kid-Friendly Alexa Apps", Fortune, 31 August 2017, available at: http://fortune.com/2017/08/31/amazon-alexa-kid-friendly-apps/; Tsukayama, "Facebook's new messaging app deepens debate over kids' social-media use", The Washington Post, 4 December 2017, available at: https://www.washingtonpost.com/news/the-switch/wp/2017/12/04/facebook-now-has-a-messenger-app-just-for-kids/?utm_term=.76bb16fe8bff.

[57] Children aged below 13 in the US (15 U.S. Code §6502(a)(1)) and aged below 16 in the EU (Art. 8 GDPR).

[58] Harris, „Virtual Assistants such as Amazon's Echo break US child privacy law, experts say", The Guardian, 26 may 2016, available at: https://www.theguardian.com/technology/2016/may/26/amazon-echo-virtual-assistant-child-privacy-law.

[59] Art. 26 paragraph 1 UDHR, Art. 2 of Protocol No. 1 to the EHCR, Art. 14 paragraph 1 EU-Charter.

[60] Art. 26 paragraph 3 UDHR, Art. 14 paragraph 3 EU-Charter.

[61] Art. 26 paragraph 2 UDHR.

[62] Factsheet on Smart Toys by German Federal Ministry for Justice and Consumer Protection: „Smartes Spielzeug", 16 October 2017, p. 2, pointing out the USA, the UK, Japan, Canada and Germany as the top five marktes for networked toys quoting a study by Juniper

jurisdictions responsible for education and, as a consequence, bound to develop a keen public interest in availability and access to data sets collected by networked toys and devices during educational classes for scientific scrutiny and research.

There are currently two legal mechanisms at play for the protection of human development: *First*, the development of a human being is safeguarded by the fundamental guarantee of privacy for family and home[63] and by the right to protection of personal data[64] ensured by data protection legislation[65].

The *second* legal safeguard in this context is the regime for liability of toy manufacturers. The risk of monetary liability encourages manufacturers to indicate for which age group a toy is appropriate as far as the child's safety is concerned. Child's safety refers to the protection against unreasonable risks of injury and death associated with consumer products including toys.[66] However, for a manufacturer to be held liable for a product in court, sufficient evidence has to be provided that such physical injury was actually caused by the product. Providing such causal evidence already appears difficult even when a product contains hazardous substances. This difficulty becomes an insurmountable challenge when a product affects the cognitive development.[67]

II. Impact of Networked Toys in Society

The actual playground for networked devices including networked toys is society at large. Under the legal rules presented at I.2.a) and I.3. above, parents may provide their child at any age with "an interactive learning friend that talks, listens, and 'remembers' what your child says and even responds when spoken to"[68]. Parents may use networked devices themselves and provide their children and teenagers at any age with (at least access to) networked toys, smartphones, tablets and voice assistants.

The legal data protection regime regulates whose consent is required for gathering, storage and transfer of personal data. The legal regime for the protection of data and consumers also regulates what kind of information has to be provided for the decision whether to give such consent or not.

From an ethical and societal perspective, the appropriateness of networked devices including networked toys for the well-being of a child may be determined by the devices' impact on the physical, cognitive, emotional, and social dimension[69] of the child's development during the critical formative stages. This requires an

Research (2015) "Smart Toys: Do Toys Dream of Digital Lives?", available at: https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-to-hit-$2-8bn-this-year.

[63] Art. 12 UDHR, Art. 8 ECHR, Art. 7 EU-Charter.

[64] Art. 8 EU-Charter.

[65] GDPR in the EU and COPPA in the USA.

[66] See mission statement of the U.S. Consumer Product Safety Commission (CPSC, an independent federal regulatory agency established in 1973 by the Consumer Product Safety Act), available at: https://www.cpsc.gov/About-CPSC.

[67] In May 2017, the German Court of Appeal Frankfurt a.M. took the view that a smartphone does not endanger the wellbeing of an eight years old child (OLG Frankfurt, decision of 15. June 2018 in case 2 UF 41/18, only available in German at http://www.lareda.hessenrecht.hessen.de/lexsoft/default/hessenrecht_lareda.html#docid:8088521). In this family law matter, the lower court had ordered the mother to deny the child access to a smartphone until the child's 12th birthday and regulate fixed time windows for the child's use of all household media (TV, computer, game console, tablet). The Court of Appeal Frankfurt held that the lower court had no proof that mere possession of a smartphone was harmful to children. Rather, potential risks for the child only emanated from how the smartphone was actually used comparing the risk level to the risks of exposure to TV-screentime or junk food both of which fell within the scope of the parents' prerogative and fundamental right to protect and educate their child.

[68] Description of the Fisher-Price Smart Toy Bear, see: http://fisher-price.mattel.com/shop/en-us/fp/smart-toy/smart-toy-bear-dnv31.

[69] See I.1.a) above.

evaluation of the impact of technology on human behaviour which has to be backed up by science. If the physical dimension of child development is covered by medicine, the science most suitable for the remaining three dimensions is psychology. However, psychological evidence often involves long term studies[70] of the entire growth process to reveal the overall impact. Unfortunately, producing such hard scientific evidence does not keep up with the speed of technological development and, in the meantime, puts entire generations at risk. The best psychological evaluations available, therefore, are more like informed guesses and estimates of the most likely.

This involves the possibility that when some or even all effects of a technological phenomenon are understood, these effects may produce entirely unexpected results once taken together. Facebook for example is a highly popular platform for teenagers and (young) adults alike, but its impact as information system on a democratic electoral system was not foreseen until the 2016 elections in the USA although it was well known (i) to competitively dominate media distribution, (ii) to provide efficacy in elections, (iii) to circulate fake news and misinformation and (iv) to be infiltrated by Russian disinformation campaigns.[71]

Without long term studies and statistics, the difficulty of reliable evaluations is further complicated by the biologically evolved human capacity for self-deception when dealing with our experiences which lets life sometimes appear as riding a train while facing backwards.[72] Nevertheless, networked devices including networked toys already form part of the environment in which children and teenagers grow up in society and their impact on human development presented here draws heavily on results in the young field of cyberpsychology.

1. Impact of Currently Available Networked Toys

The impact of networked devices including networked toys on human development depends on the age group of the child. The following aims to outline what risks are involved for the cognitive, emotional and social dimension at four representative age groups:[73]

a) Impact on Babies (age 0-1,5)

Especially for the emotional and social dimension of child development, a baby seems to need one-to-one interaction and eye contact. A baby needs talked to, tickled, massaged, and played with by a human carer with eye contact.[74] These needs of a baby are remarkably similar to the needs a networked device imposes on its user. Parents have to be aware of their own use of a mobile phone when dealing with their baby. When a baby receives only infrequent human interaction and is deprived of tactile stimulation and exploration, the child may even fail to develop the neural pathways necessary for learning.[75] If tactile interaction and eye contact with the baby is reduced, then it may grow into a less sociable human being with less capability to form deep bonds with others as well as to feel or give love.[76] Reducing human eye contact with a baby even contains the risk of

[70] At least about two decades of observation.

[71] Madrigal, „What Facebook Did to the American Democracy – And why it was so hard to see it coming", The Atlantic, 12 October 2017, available at: https://www.theatlantic.com/technology/archive/2017/10/what-facebook-did/542502/.

[72] Trivers, „Deceit and Self-Deception", 2011, p. 321.

[73] An individual child's development may vary, but all children process through all stages described here.

[74] Aiken, The Cyber Effect, 2016, p. 90.

[75] Aiken, The Cyber Effect, 2016, p. 92.

[76] Aiken, The Cyber Effect, 2016, p. 94.

a domino effect that subsequent generations might be raised with increasingly less human interaction and eye contact.[77]

If parents expose their baby and young child to too much screen time in front of their networked device, then this exposure does not enhance the children's cognitive development because they do not truly understand what they are seeing on a screen.[78] Further, such screen time not only reduces the child's chance to learn by playing on its own, but also reduces how much parents speak to their child, negatively affecting their language learning as well as the amount of human eye contact and facial reading.[79] Besides language learning, the time window of the first two years in life is crucial in the creation of properly functioning eyesight (visual acuity) with depth perception and binocular vision.[80]

b) Impact on Toddlers (aged 1,5 – 3,5)

By playing, a toddler learns about the world. If toddlers spend more time playing with networked devices with a screen like smartphones or tablets, they are more likely to become overweight.[81] Networked toys may overcome the screen time aspect, but still bear the risk of lowering a toddler's developments of interpersonal social and emotional skills because they still reduce the amount of human eye contact and facial reading.[82] For toddlers it is essential to have a minimum of at least sixty minutes per day of *unstructured play* during which the toddlers explore their natural environment by themselves without any stimulation by adults or technology.[83] This is when the toddler uses imagination and creativity, both much needed for decision-making and problem-solving as well as providing the baseline for their later performance in math and science.[84] It has already been argued that as stimulation by technology ramps up, humans' emotional life ramps down.[85]

Concerning their cognitive development, networked devices with screens seem to put toddlers' understanding that a tangible toy continues to exist even if removed (*object performance*) entirely at risk[86] and networked toys still seem dangerously close to negatively affect (to a lesser degree) the *object performance* because they suddenly have their parent's voice.

[77] Aiken, The Cyber Effect, 2016, p. 94.

[78] Haughton/Aiken/Cheevers, „Cyber Babies: The Impact of Emerging Technology on the Developing Infant", Psychology Research, September 2015, Vol. 5, No. 9, p. 504, 507; Radesky/Schumacher/Zuckerman, "Mobile and Interactive Media Use by Young Children: The Good, the Bad, and the Unknown", Pediatrics 135 (1), p. 1; Aiken, The Cyber Effect, 2016, p. 100.

[79] Radesky/Schumacher/Zuckerman, "Mobile and Interactive Media Use by Young Children: The Good, the Bad, and the Unknown", Pediatrics 135 (1), p. 1; Aiken, The Cyber Effect, 2016, p. 100.

[80] Radesky/Schumacher/Zuckerman, "Mobile and Interactive Media Use by Young Children: The Good, the Bad, and the Unknown", Pediatrics 135 (1), p. 2; Aiken, The Cyber Effect, 2016, p. 96.

[81] Haughton/Aiken/Cheevers, „Cyber Babies: The Impact of Emerging Technology on the Developing Infant", Psychology Research, September 2015, Vol. 5, No. 9, p. 504, 506; on the increase of infant obesity see Roberts, "Child and teen obesity spreading across the globe", BBC, Health, 11 October 2017, available at www.bbc.com/news/health-41550159.

[82] Haughton/Aiken/Cheevers, „Cyber Babies: The Impact of Emerging Technology on the Developing Infant", Psychology Research, September 2015, Vol. 5, No. 9, p. 504, 506 and 507; Radesky/Schumacher/Zuckerman, "Mobile and Interactive Media Use by Young Children: The Good, the Bad, and the Unknown", Pediatrics 135 (1), p. 2.

[83] Radesky/Schumacher/Zuckerman, "Mobile and Interactive Media Use by Young Children: The Good, the Bad, and the Unknown", Pediatrics 135 (1), p. 2; Aiken, The Cyber Effect, 2016, p. 102.

[84] Radesky/Schumacher/Zuckerman, "Mobile and Interactive Media Use by Young Children: The Good, the Bad, and the Unknown", Pediatrics 135 (1), p. 2; Aiken, The Cyber Effect, 2016, p. 102.

[85] Turkle, "Alone Together", 2012.

[86] Aiken, The Cyber Effect, 2016, p. 103.

c) Impact on Children (aged 3,5 - 12)

If children of this age group have access to a networked device including computers, studies in the EU[87] and in the USA[88] have revealed that children in the upper age bracket from 8 - 12 spend most of their online time on social networking sites like Facebook and watching video clips on YouTube.[89] If children spend most of their time exposed to social networks like Facebook, Instagram, Snapchat, WhatsApp and Twitter,[90] they are most likely to have a lot more than 150 online "friends" which is the maximum number of social relationships a human brain can handle on average.[91] As a consequence, they may not develop enough social competence for handling social groups of any size.[92] The emotional competence of these children may also be harmed by cyberbullying aggravated by the *bystander effect* or *diffusion of responsibility* when everybody in a large group thinks that someone else will intervene against the bullying.[93]

Networked toys seem to cut out many of these risks for the child's development, but expose them to the risk of a stranger using the networked toy's bluetooth or WLAN connection for emotionally disturbing messages or either luring or pressuring the child into a real world meetings and activities.

d) Impact on Teenagers (aged 12 – 18)

Teenagers of this age group are forming their *self-concept*[94] and enjoy experimenting with boundaries and taking risks, while craving for feedback which helps them discover who they are.[95] The human *self-concept* much depends upon social feedback and individuals express their identity (their *self*) in different ways to different people.[96] The *self-concept* has been described as comprising three components: (i) the view one has of oneself ("self-image"), (ii) the value placed on oneself ("self-esteem") and (iii) what one wishes to be like ("ideal self").[97] The internet seems to add as another component (iv) who you are in a social network ("cyber self") which is a virtual self of a teenager constantly under construction.[98] The psychological and digital construction of the "cyber self" is constantly evolving and creates a constant feedback loop requiring more and more time.[99] The "cyber self" has the risk of increasingly deviating from the real self and emotionally taking

[87] Livingstone/Haddon/Görzig/Ólafsson, (2011) EU kids online: final report, EU Kids Online, London School of Economics & Political Science, available at: http://eprints.lse.ac.uk/39351/.

[88] Courtney/Blackwell/Lauricella/Conway/Wartella, (2014) "Children and the Internet: Developmental Implications of Web Site Preferences Among 8- to 12-Year-Old Children", Journal of Broadcasting & Electronic Media, 58(1), p. 1, 6, available at: http://cmhd.northwestern.edu/wp-content/uploads/2016/10/Children-and-the-Internet-Developmental-Implications-of-Web-Site-Preferences-Among-8-to-12-Year-Old-Children-3.pdf

[89] Livingstone/Haddon/Görzig/Ólafsson, (2011) EU kids online: final report, EU Kids Online, London School of Economics & Political Science, pp. 14 and 18; Courtney/Blackwell/Lauricella/Conway/Wartella, (2014) "Children and the Internet: Developmental Implications of Web Site Preferences Among 8- to 12-Year-Old Children", Journal of Broadcasting & Electronic Media, 58(1), p. 1, 6.

[90] "Under-age social media use 'on the rise', says Ofcom", BBC Technology, 29 November 2017, available at: http://www.bbc.com/news/technology-42153694.

[91] So called "Dunbar number", see: Hill/Dunbar, „Social Network Size in Humans", Human Nature Vol. 14, No. 1 (2003), 53, 69.

[92] Aiken, The Cyber Effect, 2016, p. 128.

[93] Aiken, The Cyber Effect, 2016, p. 129.

[94] Or identity.

[95] Aiken, The Cyber Effect, 2016, p, 166.

[96] Aiken, The Cyber Effect, 2016, p. 173.

[97] Aiken, The Cyber Effect, 2016, p. 173.

[98] Aiken, The Cyber Effect, 2016, p. 174.

[99] Aiken, The Cyber Effect, 2016, p. 174.

over "self-esteem" and the "ideal self". The "cyber self" seems to influence teenagers' choice of clothing which forensic psychology considers as behavioural evidence of intent and exposes them to clinical unhappiness with their physical appearance.[100]

2. Cognitive Dissonance in Society

The impact on these age groups reveals that networked devices including networked toys bear very high risks for human development. One way of explaining how such dangerous devices could nevertheless become so popular and widely spread in society, might be provided by the theory of *cognitive dissonance*.[101] The theory of *cognitive dissonance* suggests that humans have an inner drive to hold all their attitudes and beliefs in harmony and avoid disharmony (or dissonance).[102] This inner drive provides a powerful motive to maintain cognitive consistency which can give rise to irrational and sometimes maladaptive behaviour, especially when outer circumstances cannot be changed and the cost is irretrievably gone.[103] Knowing that networked devices including networked toys with access to the internet have the negative impacts on human development and society as described under 1.a) – 1.d) above, has to be resolved with all the positive and status enhancing aspects of this technology like Wi-Fi, connectivity, convenience, individualised learning, fun gadgets. Resolving this inconsistency may also be influenced by the *bystander effect*.[104]

Once a human being has resolved this conflict one way or the other, the need to reduce *cognitive dissonance* strongly affects the reaction to any new information.[105] Rather than changing one's mind, incoming information (like insights suggested here in this article) is filtered and manipulated until it seems to confirm one's prior biases (*confirmation bias*).[106] The stronger the bias is, the less informed and the more certain human individuals may become in their ignorance.[107]

This self-deceiving constant in human cognitive capacity is also at work in academia which is generally presumed to derive a theory of justice from a larger theory of the truth.[108] Among the natural sciences, physics rests on mathematics, chemistry on physics and biology on chemistry, while social sciences should rest on biology.[109] However, the more social content a scientific discipline involves, the slower it progresses because of the greater forces of deceit and self-deception involved.[110] Physics and mathematics probably have the least (scientific) content depending on human or social behaviour and therefore advance relatively unimpeded by the forces of self-deception.[111] Of course, any science has built-in mechanisms which guard against self-deception which ultimately outstrip competing enterprises, but progress is inevitably slower in psychology than in physics or mathematics. Networked devices including networked toys are engineered on knowledge emanating predominantly out of the fields of physics and mathematics, while their impact on human

[100] Aiken, The Cyber Effect, 2016, p. 178 and 186.
[101] Festinger, A Theory of Cognitive Dissonance, 1957; Aiken, The Cyber Effect, 2016, p. 135.
[102] Trivers, Deceipt and Self-Deception, 2011, p. 151-152.
[103] Trivers, Deceipt and Self-Deception, 2011, p. 152.
[104] Aiken, The Cyber Effect, 2016, p. 135.
[105] Trivers, Deceipt and Self-Deception, 2011, p. 152.
[106] Trivers, Deceipt and Self-Deception, 2011, p. 153.
[107] Trivers, Deceipt and Self-Deception, 2011, p. 153.
[108] Trivers, Deceipt and Self-Deception, 2011, p. 304.
[109] Trivers, Deceipt and Self-Deception, 2011, p. 306.
[110] Trivers, Deceipt and Self-Deception, 2011, p. 308.
[111] Trivers, Deceipt and Self-Deception, 2011, p. 307.

development and society at large is measured and evaluated by social sciences like psychology, economy and history. Perhaps this provides another reason why devices are developed and available for use and play in society although their impact on human development is as yet unknown.

3. Ethical and Societal Risks of Ideal Networked Toys

Returning to the advantages of networked devices including networked toys, modern technology based on artificial intelligence allows machines to learn about an individual child using them, by studying the data produced in the progress. Drawing on psychology, cognitive science and other disciplines, it is possible to imagine machines which are driven by practical insights into the science of learning. Such educational technology opens the door for computer-assisted and online learning which has been found more effective in recent studies comparing children learning with adaptive software with children taught by conventional means.[112] Computer-assisted learning is more effective because software can adapt instructions to a child's learning level, letting children learn at the pace that works best for them and essentially providing personalised tutoring on an individual level.[113] Not surprisingly, such educational technology seems particularly promising when used to support learning in language and mathematics. In more social subjects like history, however, a "comparative judgment" algorithm could help a teacher ranking children's performance.[114]

Against this promising background, it seems appropriate to consider ethical and societal risks of networked devices including toys which harmonise with human development and observe the legal framework for privacy and data protection. This necessitates a closer look into the technology with which networked devices operate:[115]

a) Algorithms and Machine Learning

Any networked device employs algorithms. Although an "algorithm" may formally be defined as purely *mathematical construct*[116], lay usage of the term "algorithm" also includes the implementation of the mathematical construct into a technology and an application of the technology configured for a particular task[117]. Whereas a strict wording would have to distinguish between constructs, implementations and configurations, for the discussion of ethical issues of networked devices generically referring to "algorithm" will suffice. Algorithms in this sense are found in any configuration of complex software running on the internet including search engines like Google, Bing, DuckDuckGo, Torch, Ahmia and others.

For the child, networked devices replace a parent or teacher at least to a significant extent by an algorithm. This replacement of a human carer may have the advantage that the analysis of the child's behaviour is

[112] Escueta/Quan/Nickow/Oreopoulos, "Education Technology: An Evidence-Based Review", NBER Working Paper No. 23744, August 2017, available at: https://www.nber.org/papers/w23744.

[113] Quan, „Exploring the promise of education technology", J-PAL, 5 September 2017, available at: https://www.povertyactionlab.org/blog/9-5-17/exploring-promise-education-technology.

[114] „Technology is transforming what happens when a child goes to school", The Economist, 22 July 2017, available at: https://www.economist.com/news/briefing/21725285-reformers-are-using-new-software-personalise-learning-technology-transforming-what-happens.

[115] The following overview draws on results of the work stream dedicated to the ethical, legal and societal impact of the project TENSOR funded by the EU under the Horizon 2020 programme, see http://tensor-project.eu/.

[116] Hill, "What an algorithm is", *Philosophy & Technology* [2016] 29 (1), p. 35 (p. 47).

[117] See Turner/Angius, "The Philosophy of Computer Science" in: Edward N. Zalta (ed.), *The Stanford Encyclopedia of Philosophy* (Spring 2017), available at: https://plato.stanford.edu/archives/spr2017/entries/computer-science/.

augmented by the scope and scale of data and rules applied. However, the algorithms are created by private manufacturers who not only select the data used by the algorithm for the decisions of the networked device/toy, but also define how the algorithm uses this data. The decision-making rules of algorithms may either be defined and programmed individually "by hand" (e.g. Google's PageRank algorithm) or rely on machine learning capacities which are also referred to as "predictive analytics"[118] and "artificial intelligence"[119] because these algorithms are capable of learning.[120] Networked devices like Mattel's Aristotle or Amazon's Echo have such capacities of machine learning. Machine learning generally means that the algorithm defines the decision-making rules to handle new inputs independently of any human operator.[121] Unfortunately, the impact of such autonomous learning capacities remain uncertain adding a potentially negative flavour to the algorithm's autonomy. Networked devices/toys with machine learning algorithms are, therefore, difficult to predict beforehand as well as difficult to explain afterwards and this uncertainty might inhibit the identification and redress of ethical challenges.[122]

b) Quality of Data Evidence Produced by Networked Toys

The first major ethical challenge posed by networked devices/toys employing decision-making algorithms emanates from the manufacturers choice of data training the algorithm for making decisions. Such training data may contain unwanted biases or may simply be inaccurate.

The second major ethical challenge concerns the quality of data produced and decisions made by the algorithm. This challenge can be divided into the following three components:[123]

aa) (In)Conclusiveness

Algorithmic decision-making and data mining of a networked device/toy relies on inductive knowledge and correlations identified within the data examined. The data evidence produced by an algorithm does not establish any causality to which educational value could be attached. The decision-making process is complicated by the phenomenon that correlations based on a sufficient volume of data could increasingly be seen as sufficiently credible to direct the learning process and actions of a child without seeking any causality.[124] Decisions based upon mere correlations may ethically be legitimate but require a higher threshold of data evidence to justify actions impacting on a child or teenager. The risk is that algorithmic categories signal certainty, discourage alternative explorations and create a coherence among disparate objects.[125] This leads to the danger that a child using the networked device/toy may be addressed via too simplified models.[126]

[118] See Siegel, "Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die", 2016.

[119] See Domingos, "The Master Algorithm: How the Quest for the Ultimate Learning Machine will Remake the World", 2015.

[120] Tutt, "An FDA for algorithms", *Administrative Law Review* [2017] 69, p. 83 (pp. 94).

[121] Matthias, "The responsibility gap: Ascribing responsibility for the action of learning automata" *Ethics and Information Technology* [2004], 6, p. 175 (p. 179).

[122] Mittelstadt/Allo/Taddeo/Wachter/Floridi, "The ethics of algorithms: Mapping the debate", *Big Data & Society* [2016] 3 (2), p. 1 (p. 3).

[123] Mittelstadt/Allo/Taddeo/Wachter/Floridi, "The ethics of algorithms: Mapping the debate", *Big Data & Society* [2016] 3 (2), p. 1 (p. 4) referring to the quality of evidence as "inconclusive", "inscrutable" and "misguided".

[124] Hildebrandt, "Who needs stories if you can get the data?, *Philosophy & Technology* [2011] 24 (4), p. 371 (pp.378-380).

[125] Ananny, "Toward an ethics of algorithms: convening, observation, probability and timeliness", *Science, Technology, & Human Values* [2015] 41 (1), p. 93 (p. 103).

[126] Barocas, "Data mining and the discourse on discrimination", p. 2 under section 2.3 on "faulty inferences", available at: https://dataethics.github.io/proceedings/DataMiningandtheDiscourseOnDiscrimination.pdf.

bb) (In)Scrutability

The scrutability of data evidence presents an essential ethical concern and addresses the transparency and opacity of an algorithm in a networked device/toy. The primary components of transparency are accessibility and comprehensibility of information. However, the information about the functionality of proprietary algorithms understandably is kept secret by the manufacturers to maintain a competitive advantage.[127] The transparency of an algorithm, therefore, involves conflicting ethical ideals which have to be balanced with each other.

Machine learning algorithms in networked devices/toys are especially difficult to understand because their learning process is a moving target.[128] The argument is that the opacity of machine learning algorithms inhibits ethical or any other oversight. According to one scholar, algorithms are opaque in the sense that the recipient of an algorithm's output rarely has any concrete sense of how and why a particular classification has been arrived at from inputs.[129] The opacity in machine learning algorithms appears to be a product of the high-dimensionality of data, complex code and changeable decision making logic.[130] If a networked device/toy had an informational advantage over the child and parents as human users, then meaningful oversight in algorithmic decision-making appears impossible.[131]

Even algorithms operating in networked devices/toys with individually "hand-written" decision-making rules appear highly complex and practically inscrutable despite their lack of machine learning.[132] No algorithm may be divorced from the conditions under which it is developed and, therefore, algorithms need to be understood as relational, contingent, contextual in nature, framed within the wider context of their socio-technical assemblage.[133]

Despite this similarity to traditional human decision-making, such algorithmic processing remains different and the rationale of the algorithm in a networked device/toy may well be incomprehensible to humans rendering the legitimacy of such algorithmic decisions difficult to challenge.[134]

In short: Algorithmic decision-making in networked devices/toys hardly appears transparent and the resulting opacity seems to prevent meaningful assessment of ethical risks.

[127] Glenn/Montieth, "New measures of mental state and behavior based on data collected from sensors, smartphones, and the internet", *Current Psychiatry Reports* [2014] 16 (12), p. 1 (p. 6).

[128] Burell, "How the machine thinks: understanding opacity in machine learning algorithms" *Big Data & Security* [2016] 3 (1), p. 1 (p. 4); Hildebrandt, "Who needs stories if you can get the data?, *Philosophy & Technology* [2011] 24 (4), p. 371 (pp.378-380); Leese, "The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union", *Security Dialogue* [2014] 45 (5), p. 494 (p. 502); Tutt, "An FDA for algorithms", *Administrative Law Review* [2017] 69, p. 83 (pp. 94).

[129] Burell, "How the machine thinks: understanding opacity in machine learning algorithms" *Big Data & Security* [2016] 3 (1), p. 1 (p. 1).

[130] Burell, "How the machine thinks: understanding opacity in machine learning algorithms" Big Data & Security [2016] 3 (1), p. 1 (p. 6).

[131] Matthias, "The responsibility gap: Ascribing responsibility for the action of learning automata" *Ethics and Information Technology* [2004], 6, p. 175 (pp. 182).

[132] Kitchin, "Thinking critically about and researching algorithms", Information, Communication & Society [2017] 20 (1), p. 14 (pp. 20 et seq.).

[133] Kitchin, "Thinking critically about and researching algorithms", Information, Communication & Society [2017] 20 (1), p. 14 (pp. 18).

[134] Mittelstadt/Allo/Taddeo/Wachter/Floridi, "The ethics of algorithms: Mapping the debate", *Big Data & Society* [2016] 3 (2), p. 1 (p. 7).

cc) Risk of Potential Bias

Networked devices/toys automate the decision-making process interacting with the child, but the automation may not be justified by an alleged lack of bias in algorithms.[135] An algorithm's design and functionality reflects the values of its designer(s) and intended uses, if only to the extent that a particular design is preferred as the best or most efficient option.[136] Because the development of an algorithm involves many choices between several possible options, the values of the algorithm's author(s) are woven into the code which in effect institutionalises those values.[137] Without knowing the history of an algorithm's development, it is most difficult to detect latent bias in the algorithm.[138] In the context of a child's behavioural data, the correlations presented by the algorithm might come to reflect the interpreter's unconscious motivations, socio-economic determinations and geographic or demographic influences.[139]

dd) Unfair Discrimination

Whereas bias is a dimension of the decision-making process itself employed by a networked device/toy, an algorithm contains the risk of unfair discrimination based on the algorithm's profiling. The algorithm infers a pattern by means of data mining and thereby constructs a profile[140] which may involve unwanted and undetected discrimination if the profile results from biased data evidence for the decision-making process.

III. Playful Learning – Together

Networked devices, including networked toys, involve complex ethical issues for parents and children. The neurological development of a human brain (see I.1.a) above) processes through four different psychological stages each of which involves vital windows for development in the cognitive, the emotional and the social dimension (see I.1.b) above). The development in these three dimensions is crucial for the individual as well as for society and, therefore, protected by fundamental rights and guarantees (see I.2.a) above). Networked toys seem to be at odds with privacy and data protection requirements (see I.2.b) above). They also involve the risk of negatively impacting the cognitive, emotional and social dimension of human development (see II.1. above). This probably has to do with cognitive dissonance in society and in science (see II.2. above). Even if the psychological risks for human development and the legal conflict with privacy and security are ironed out, significant ethical and societal risks of ideal networked devices/toys remain (see II.3. above). Like any other tool and technology however, networked devices, including networked toys, have a human user.

[135] Kitchin, "Thinking critically about and researching algorithms", Information, Communication & Society [2017] 20 (1), p. 14 (pp. 18); Newell/Marabelli, "Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datafication'", The Journal of Strategic Information Systems [2015] 24 (1), p. 3 (p, 6).

[136] Kitchin, "Thinking critically about and researching algorithms", Information, Communication & Society [2017] 20 (1), p. 14 (pp. 18).

[137] Macnish, "Unblinking eyes: The ethics of automating surveillance", *Ethics and Information Technology* [2012] 14 (2), p. 152 (p. 158).

[138] Hildebrandt, "Who needs stories if you can get the data?, *Philosophy & Technology* [2011] 24 (4), p. 371 (p.377).

[139] Hildebrandt, "Who needs stories if you can get the data?, *Philosophy & Technology* [2011] 24 (4), p. 371 (p. 376).

[140] So the broad definition by Hildebrandt/Koops, "the challenges of ambient law and legal protection in the profiling era", *The Modern Law Review* [2010] 73 (3), p. 428 (p. 431).

1. Information and Society

If the user is adequately informed about the various properties, risks and qualities of the networked device/toy, then the decision where and when to use it has a chance of becoming an informed decision. In this respect, legal requirements to provide certain information can help:

In France, TV programs aimed at babies were banned in 2008 by the High Audiovisual Council and foreign baby programs have had to appear on French cable channels since then with a subtitle explicitly warning parents that watching TV may slow the development of children under three, even if aimed specifically for this age.[141] While French schoolchildren had already been prohibited to use smartphones during class hours since 2010, this soft ban has become stricter in September 2018 prohibiting for all schoolchildren up to the age of 15 the use of smartphones also between classes and even during meal times (although schools have been given the option to make exceptions for 'pedagogical use', for extra-curricular activities or for disabled pupils).[142]

In 2015, Taiwan outlawed networked devices for children under the age of two and limited their use to reasonable periods of time for those under eighteen.[143] Parents who fail to comply with the Taiwanese Child and Youth Welfare Protection Act face the risk of a significant monetary fine.[144]

Other jurisdictions seem to prefer official recommendations for parents: The Australian Government Department of Health and Ageing[145] and the Canadian Paediatric Society[146] warn against screen time for children under the age of two. The American Academy of Pediatrics in the USA draws the line for children younger than 18 months and recommends to avoid use of screen media other than video-chatting[147], whereas the Internet Crime Complaint Center (IC3) of the Federal Bureau of Investigation (FBI) has issued a consumer notice warning about the cyber security of networked devices/toys[148]. The German Federal Ministry for Justice and Consumer Protection tries to raise customer awareness by informing in detail about advantages and disadvantages of networked toys and by pointing out where to get reliable independent information about

[141] Ollivier, "France bans broadcast of TV shows for babies", USA Today, 20 August 2008, available at: https://usatoday30.usatoday.com/life/television/news/2008-08-20-france-tv_N.htm.

[142] Shaban, "France bans smartphones in school", Washington Post, 31 July 2018, available at: https://www.washingtonpost.com/technology/2018/07/31/france-bans-smartphones-school/?noredirect=on&utm_term=.ad404da7d8bf; Filippidis, "France bans smartphones in schools", engadget.com, 1 August 2018, available at: https://www.engadget.com/2018/08/01/france-bans-smartphones-schools/?guccounter=1.

[143] Simons, "Why Taiwan is right to ban iPads for kids", CNN, 4 February 2015, available at: http://edition.cnn.com/2015/02/03/intl_opinion/taiwan-ipads-kids/index.html.

[144] Seok Hway, "Taiwan revises law to restrict amount of time children spend on electronic devices", The Straits Time, 24 January 2015, available at: http://www.straitstimes.com/asia/east-asia/taiwan-revises-law-to-restrict-amount-of-time-children-spend-on-electronic-devices#xtor=CS1-10.

[145] "National Physical Activity Recommendations for Children 0-5 Years", 2010 available at: http://www.health.gov.au/internet/main/publishing.nsf/content/9D831D9E6713F92ACA257BF0001F5218/$File/PA%20Rec%200-5%20yo%20-%20Web%20printable%20version.pdf.

[146] "Screen time and young children: Promoting health and development in a digital world", Position Statement, 27 November 2017, available at: https://www.cps.ca/en/documents/position/screen-time-and-young-children.

[147] "American Academy of Pediatrics Announces New Recommendations for Children's Media Use", 21 October 2016, available at: https://www.aap.org/en-us/about-the-aap/aap-press-room/Pages/American-Academy-of-Pediatrics-Announces-New-Recommendations-for-Childrens-Media-Use.aspx.

[148] Internet Crime Complaint Center (IC3), "Consumer Notice: Internet-connected toys could present privacy and contact concerns for children", Alert-No. I-071717(Revised)-PSA, 17 July 2017, available at: https://www.ic3.gov/media/2017/170717.aspx.

networked toys.[149] Such legal requirements and official recommendations may still face parental *cognitive dissonance*, but they create a different atmosphere and perhaps awareness in society.

On Safer Internet Day 2017, the European Commission, tech and telecoms companies, broadcasters, NGOs and UNICEF launched a major self-regulatory initiative called "Alliance to Better Protect Minors Online" to address harmful content, harmful conduct and harmful contact online.[150] This "Alliance to Better Protect Minors Online"[151] is a self-regulatory initiative aiming to improve the online environment for children and young people and has led to a Technical Report by the Joint Research Centre (JRC), the European Commission's science and knowledge service, inviting policy makers, industry, parents and teachers to study networked toys in more depth in order to provide a framework as guide for their design and use which ensures that these toys are safe and beneficial for children.[152]

Comparing this with the effectiveness of legislation introducing comprehensive smoking bans reducing exposure to tobacco smoke in the majority of EU Member States between 2004 and 2008[153], regulations of screen time with networked devices in most Member States of the EU still seem to have a long way to go. However, the ban on smoking could be based on medical evidence.

In contrast, hard clinical psychological evidence on the effects of networked devices and networked toys appears not yet available. Worse: Producing such hard evidence puts entire generations of children at risk. Hence, any legislation has to be based on up-to-date responsible ethical and moral thinking and research.

2. Educational Use

There are many educational benefits of computer assisted and online learning. Such educational technology appears most effective when used by adults and children together as an in-class tool or as mandatory homework support.[154] Because of personalised tutoring on a child's individual level, computer assisted and online learning seem more capable of tuning in with the idea of personalised learning promoted by *Maria Montessori* or *Rudolf Steiner* but currently involve more than twice the average spending per pupil in OECD countries.[155] This makes

[149] German Federal Ministry of Justice and Consumer Protection, "Verbraucherschutz Smart Toys – Worauf Verbraucherinnen und Verbraucher achten sollten", press release, 11 December 2017, availabe at: http://www.bmjv.de/SharedDocs/Artikel/DE/2017/121117_Smart_Toys.html.

[150] European Commission, "Safer Internet Day 2017: European Commission welcomes alliance of industry and NGOs for a better internet for minors", 7 February 2017, available at: https://ec.europa.eu/digital-single-market/en/news/safer-internet-day-2017-european-commission-welcomes-alliance-industry-and-ngos-better-internet.

[151] European Commission, "Alliance to better protect minors online", 7 February 2017, available at: https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online.

[152] EU Science Hub, "Connected dolls and tell-tale teddy bears: why we need to manage the Internet of Toys", 23 March 2017, available at: https://ec.europa.eu/jrc/en/news/why-we-need-manage-internet-toys; JRC Report "Kaleidoscope on the Internet of Toys: Safety, security, privacy and societal insights", p. 26 available at: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC105061/jrc105061_final_online.pdf.

[153] Origo/Lucifora, "The Effect of Comprehensive Smoking Bans in European Workplaces", IZA DP No. 5290, October 2010, available at: http://ftp.iza.org/dp5290.pdf.

[154] Quan, „Exploring the promise of education technology", J-PAL, 5 September 2017, available at: https://www.povertyactionlab.org/blog/9-5-17/exploring-promise-education-technology.

[155] „Technology is transforming what happens when a child goes to school", The Economist, 22 July 2017, available at: https://www.economist.com/news/briefing/21725285-reformers-are-using-new-software-personalise-learning-technology-transforming-what-happens.

it difficult for politicians to consider legislation introducing such technology assisted educational approach, but it reveals a positive ethical value of enhancing children's learning with networked devices.

3. Morris Theorem

From a historical perspective, the development of humans and their societies has been described as determined by two constants: "biology" and "sociology".[156] "Biology" takes into account our evolutionary roots as animals with built-in drives for survival, reproduction and tinkering with things for edibility, fun or improvement.[157] "Sociology" or rather sciences with social content[158] simultaneously explain what causes social change, on the one hand, and what social change causes, on the other.[159] As constants, "biology" and "sociology" both apply everywhere, in all times and places, but it is "sociology" which explains why social development takes place in humanity and at what pace.[160] The historian Ian Morris has put forward perhaps one of the best one-sentence summaries of the causes of social change, the Morris Theorem:

"Change is caused by lazy, greedy, frightened people (who rarely know what they're doing) looking for easier, more profitable and safer ways to do things."[161]

Greedy, lazy, frightened people seek their own preferred balance among being comfortable, working as little as possible, and being safe.[162] Such people are not the ones Friedrich Schiller had in mind when he developed his thesis of cultural anthropology and suggested play as therapy for society.[163] However, modern technology has developed networked devices/toys and human beings have started using them predominantly in the space of a decade. This is a social change. Do these people know what they are actually doing, especially when providing networked devices and networked toys to their offspring? The paradox of development[164] has slowed down further social development in the past.[165] Modern technology, however, might lead humanity to a stage at which human and machine intelligence will merge after which the constants of "biology" and "sociology" might cease to apply because artificial intelligence[166] will replace human beings as ruling species.[167] Up until this future stage, the development of human societies seems to depend on how well we humans as a group manage to observe and balance the insights and findings of all scientific disciplines for our benefit.

---

[156] Morris, „Why the West Rules - for Now", 2011.

[157] Morris, „Why the West Rules - for Now", 2011, p. 26.

[158] Including economics, political science and psychology.

[159] Morris, „Why the West Rules - for Now", 2011, p. 27.

[160] Morris, „Why the West Rules - for Now", 2011, p. 29.

[161] Morris, „Why the West Rules - for Now", 2011, p. 618.

[162] Morris, „Why the West Rules - for Now", 2011, p. 28.

[163] Safranski, „Schiller oder Die Erfindung des Deutschen Idealismus", 2004, p. 417.

[164] Success creates new problems and solving these new problems creates further problems.

[165] Morris, „Why the West Rules - for Now", 2011, p. 28.

[166] In 2015, the computer scientist and neuroscientist Naftali Tishby presented a procedure for machines ("deep neural networks") to compress noisy data while preserving information what the data represent ("information bottleneck theory"). This procedure appears to reverse-engineer the pruning process of the growing human brain (see I.1.a) above) helps to understand which kinds of problems can be solved by artificial networks, see Wolchover, "New Theory Cracks Open the Black Box of Deep Learning", Quanta Magazine, 21 September 2017, available at: https://www.quantamagazine.org/new-theory-cracks-open-the-black-box-of-deep-learning-20170921/.

[167] Morris, „Why the West Rules - for Now", 2011, p. 618 referring to Kurzweil, "The Singularity Is Near. When Humans Transcend Biology", 2005.

References

Aiken, Mary. The Cyber Effect. London: John Murray, 2016.

Ananny, Mike. "Toward an ethics of algorithms: convening, observation, probability and timeliness". Science, Technology, & Human Values [2015] 41 (1), p. 93-117.

American Academy of Pediatrics. "American Academy of Pediatrics Announces New Recommendations for Children's Media Use", 21 October 2016. Available at: https://www.aap.org/en-us/about-the-aap/aap-press-room/Pages/American-Academy-of-Pediatrics-Announces-New-Recommendations-for-Childrens-Media-Use.aspx.

Barocas, Solon. "Data mining and the discourse on discrimination". Available at: https://dataethics.github.io/proceedings/DataMiningandtheDiscourseOnDiscrimination.pdf.

BBC Technology. "Under-age social media use 'on the rise', says Ofcom", 29 November 2017. Available at: http://www.bbc.com/news/technology-42153694.

Blackwell, Courtney, K./Lauricella, Alexis R./Conway, Annie/Wartella, Ellen, (2014). "Children and the Internet: Developmental Implications of Web Site Preferences Among 8- to 12-Year-Old Children". Journal of Broadcasting & Electronic Media, 58(1), p. 1-20. Available at: http://cmhd.northwestern.edu/wp-content/uploads/2016/10/Children-and-the-Internet-Developmental-Implications-of-Web-Site-Preferences-Among-8-to-12-Year-Old-Children-3.pdf.

Buffington, Kimberly/Dharmadasa, Dinesh. "Keeping Up with Cayla: Concerns over Interactive Toys Spur an FTC Update of COPPA Guidelines", 24 July 2017. Available at: https://www.socialgameslaw.com/2017/07/coppa-ftc-interactive-toys-cayla.html#page=1.

Bundesnetzagentur. „Bundesnetzagentur geht gegen Kinderuhren mit Abhörfunktion vor", press release, 17 November 2017.

Bundesnetzagentur. "Bundesnetzagentur zieht Kinderpuppe „Cayla" aus dem Verkehr", press release, 17 February 2017.

Burell, Jenna. "How the machine thinks: understanding opacity in machine learning algorithms". Big Data & Security [2016] 3 (1), p. 1-12.

Canadian Paediatric Society. "Screen time and young children: Promoting health and development in a digital world" Position Statement, 27 November 2017. Available at: https://www.cps.ca/en/documents/position/screen-time-and-young-children.

Chaudron, Stéphane/Di Gioia, Rosanna/Gemo, Monica/Holloway, Donell/Marsh, Jackie/Mascheroni, Giovanna/Peter, Jochen/Yamada-Rice Dylan. Joint Research Centre (JRC) Report, "Kaleidoscope on the Internet of Toys: Safety, security, privacy and societal insights", p. 26. Available at: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC105061/jrc105061_final_online.pdf.

Cherry, Kendra. "Piaget's Theory: The 4 Stages of Cognitive Development", 14 May 2017. Available at: https://www.verywell.com/piagets-stages-of-cognitive-development-2795457.

Cohen, Kristin/Magee, Peder. "FTC updates COPPA compliance plan for business", FTC Business Blog, 21 June 2017. Available at: https://www.ftc.gov/news-events/blogs/business-blog/2017/06/ftc-updates-coppa-compliance-plan-business

Commonwealth of Australia, Department of Health and Ageing (2010). "National Physical Activity Recommendations for Children 0-5 Years". Available at: http://www.health.gov.au/internet/main/publishing.nsf/content/9D831D9E6713F92ACA257BF0001F5218/$File/PA%20Rec%200-5%20yo%20-%20Web%20printable%20version.pdf.

Darrow, Barb. "Amazon Wants More Kid-Friendly Alexa Apps", Fortune, 31 August 2017. Available at: http://fortune.com/2017/08/31/amazon-alexa-kid-friendly-apps/.

Domingos, Pedro. "The Master Algorithm: How the Quest for the Ultimate Learning Machine will Remake the World". New York: Basic Books, 2015.

Eagleman, David. The Brain. Edinburgh: Canongate Books, 2015.

Escueta, Maya/Quan, Vincent/Nickow, Andre Joshua/Oreopoulos, Philip. "Education Technology: An Evidence-Based Review", NBER Working Paper No. 23744, August 2017. Available at: https://www.nber.org/papers/w23744.

EU Science Hub. "Connected dolls and tell-tale teddy bears: why we need to manage the Internet of Toys", 23 March 2017. Available at: https://ec.europa.eu/jrc/en/news/why-we-need-manage-internet-toys.

European Commission. "Safer Internet Day 2017: European Commission welcomes alliance of industry and NGOs for a better internet for minors", 7 February 2017. Available at: https://ec.europa.eu/digital-single-market/en/news/safer-internet-day-2017-european-commission-welcomes-alliance-industry-and-ngos-better-internet.

European Commission. "Alliance to better protect minors online", 7 February 2017. Available at: https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online.

Festinger, Leon. A Theory of Cognitive Dissonance. Evanston, IL: Row & Peterson, 1957.

Forbrukerrådet. „#watchout – Analysis of smartwatches for children", October 2017. Available at: https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf.

German Federal Ministry of Justice and Consumer Protection. "Verbraucherschutz Smart Toys – Worauf Verbraucherinnen und Verbraucher achten sollten", press release, 11 December 2017. Availabe at: http://www.bmjv.de/SharedDocs/Artikel/DE/2017/121117_Smart_Toys.html.

Glenn, Tasha/Monteith, Scott. "New measures of mental state and behavior based on data collected from sensors, smartphones, and the internet". Current Psychiatry Reports [2014] 16 (12), 523.

Harris, Mark. „Virtual Assistants such as Amazon's Echo break US child privacy law, experts say", The Guardian, 26 may 2016. Available at: https://www.theguardian.com/technology/2016/may/26/amazon-echo-virtual-assistant-child-privacy-law.

Haughton, Ciaran/Aiken, Mary/Cheevers, Carly. „Cyber Babies: The Impact of Emerging Technology on the Developing Infant". Psychology Research, September 2015, Vol. 5, No. 9, p. 504-518.

Hildebrandt, Mireille. "Who needs stories if you can get the data?". Philosophy & Technology [2011] 24 (4), p. 371-390.

Hildebrandt, Mireille/Koops, Bert-Jaap. "the challenges of ambient law and legal protection in the profiling era". The Modern Law Review [2010] 73 (3), p. 428-460.

Hill, Robin K. "What an algorithm is". Philosophy & Technology [2016] 29 (1), p. 35-59.

Hill, Russel A./Dunbar, Robin I. M. „Social Network Size in Humans". Human Nature Vol. 14, No. 1 (2003), 53-72.

Internet Crime Complaint Center (IC3). "Consumer Notice: Internet-connected toys could present privacy and contact concerns for children", Alert-No. I-071717(Revised)-PSA, 17 July 2017. Available at: https://www.ic3.gov/media/2017/170717.aspx.

Juniper Research (2015). "Smart Toys: Do Toys Dream of Digital Lives?". available at: https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-to-hit-$2-8bn-this-year quoted according to German Federal Ministry for Justice and Consumer Protection, Factsheet „Smartes Spielzeug", 16 October 2017.

Kitchin, Rob. "Thinking critically about and researching algorithms". Information, Communication & Society [2017] 20 (1), p. 14-29.

Kress, Sonja/Nagel, Daniel. „The GDPR and Its Magic Spells Protecting Little Princes and Princesses". Computer Law Review International (CRi) 2017, p. 6-9.

Kurzweil, Ray. "The Singularity Is Near. When Humans Transcend Biology". New York: Viking Penguin, 2005.

Lawler, Richard. "Google opens up 'Family Link' parental controls for Android", engadget 29 September 2017. Available at: https://www.engadget.com/2017/09/29/google-family-link-controls-android/.

Lee, Dave. „Mattel thinks again about AI babysitter", BBC, 5 October 2017. Available at: http://www.bbc.com/news/technology-41520732.

Leese, Matthias. "The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union". Security Dialogue [2014] 45 (5), p. 494-511.

Livingstone, Sonia/Haddon, Leslie/Görzig, Anke/Ólafsson, Kjartan, (2011). "EU kids online II: final report". EU Kids Online, London School of Economics & Political Science. Available at: http://eprints.lse.ac.uk/39351/.

Macnish, Kevin. "Unblinking eyes: The ethics of automating surveillance". Ethics and Information Technology [2012] 14 (2), p. 151-167.

Madrigal, Alexis C. „What Facebook Did to the American Democracy – And why it was so hard to see it coming", The Atlantic, 12 October 2017. Available at: https://www.theatlantic.com/technology/archive/2017/10/what-facebook-did/542502/.

Matthias, Andreas. "The resonsibility gap: Ascribing responsibility for the action of learning automata". Ethics and Information Technology [2004], 6, p. 175-183.

Mittelstadt, Brent Daniel/Allo, Patrick/Taddeo, Mariarosaria/Wachter, Sandra/Floridi, Luciano. "The ethics of algorithms: Mapping the debate". Big Data & Society [2016] 3 (2), p. 1-21.

Mnemonic, Security Assessment Report. „GPS Watches for Children", The Norwegian Consumer Council, 18 October 2017.

Morris, Ian. „Why the West Rules - for Now". London: Profile Books, 2011.

Newell, Sue/Marabelli, Marco. "Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datafication'". The Journal of Strategic Information Systems [2015] 24 (1), p. 3-14.

Ollivier, Christine. "France bans broadcast of TV shows for babies", USA Today, 20 August 2008. Available at: https://usatoday30.usatoday.com/life/television/news/2008-08-20-france-tv_N.htm.

Origo, Federica/Lucifora, Claudio. "The Effect of Comprehensive Smoking Bans in European Workplaces". IZA DP No. 5290, October 2010, available at: http://ftp.iza.org/dp5290.pdf.

Quan, Vincent. „Exploring the promise of education technology", J-PAL, 5 September 2017. Available at: https://www.povertyactionlab.org/blog/9-5-17/exploring-promise-education-technology.

Radesky, Jenny S./Schumacher, Jayna/Zuckerman, Barry. "Mobile and Interactive Media Use by Young Children: The Good, the Bad, and the Unknown". Pediatrics 135 (1), p. 1-3.

Roberts, Michelle. "Child and teen obesity spreading across the globe", BBC, Health, 11 October 2017. Available at www.bbc.com/news/health-41550159.

Safranski, Rüdiger. „Schiller oder Die Erfindung des Deutschen Idealismus". München: Carl Hanser Verlag, 2004.

Schiller, Friedrich. "On the Aesthetic Education of Man in a Series of Letters", (letter 15), p. 107 cited according to Hoffmeister, "Wörterbuch der philosphischen Begriffe", 2. Edition, Hamburg: Felix Meiner Verlag, 1955 (p. 573).

Seok Hway, Lee. "Taiwan revises law to restrict amount of time children spend on electronic devices", The Straits Time, 24 January 2015. Available at: http://www.straitstimes.com/asia/east-asia/taiwan-revises-law-to-restrict-amount-of-time-children-spend-on-electronic-devices#xtor=CS1-10.

Siegel, Eric. "Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die". Hoboken, New Jersey: Wiley & Sons, 2016.

Simons, Jake Wallis. "Why Taiwan is right to ban iPads for kids", CNN, 4 Feburary 2015. Available at: http://edition.cnn.com/2015/02/03/intl_opinion/taiwan-ipads-kids/index.html.

Stiftung Warentest. "Kinderleicht zu kapern". test 9/2017, p. 34.

The Economist. „Technology is transforming what happens when a child goes to school", 22 July 2017. Available at: https://www.economist.com/news/briefing/21725285-reformers-are-using-new-software-personalise-learning-technology-transforming-what-happens.

Trivers, Robert. „Deceit and Self-Deception". London: Penguin Books, 2011.

Tsukayama, "Facebook's new messaging app deepens debate over kids' social-media use", The Washington Post, 4 December 2017, available at: https://www.washingtonpost.com/news/the-switch/wp/2017/12/04/facebook-now-has-a-messenger-app-just-for-kids/?utm_term=.76bb16fe8bff.

Tsukayama, Hayley. „Mattel has cancelled plans for a kid-focused AI device that drew privacy concerns", Washington Post, 4 October 2017. Available at: https://www.washingtonpost.com/news/the-

switch/wp/2017/10/04/mattel-has-an-ai-device-to-soothe-babies-experts-are-begging-them-not-to-sell-it/?utm_term=.d63f3e8642ff.

Turkle, Sherry. "Alone Together". New York: Basic Books, 2012.

Turner, Raymond/Angius, Nicola. "The Philosophy of Computer Science" in: Edward N. Zalta (ed.). The Stanford Encyclopedia of Philosophy (Spring 2017). Available at: https://plato.stanford.edu/archives/spr2017/entries/computer-science/.

Tutt, Andrew. "An FDA for algorithms". Administrative Law Review [2017] 69, p. 83-123.

U.S. Consumer Product Safety Commission (CPSC). Mission statement. Available at: https://www.cpsc.gov/About-CPSC.

Which?. „Safety alert: how easy it is for almost anyone to hack your child's connected toy", 14 November 2017. Available at: https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/.

Wolchover, Natalie. "New Theory Cracks Open the Black Box of Deep Learing", Quanta Magazine, 21 September 2017. Available at: https://www.quantamagazine.org/new-theory-cracks-open-the-black-box-of-deep-learning-20170921/.

Rocco Panetta, Federico Sartore:

Data protection for networked and robotic toys – a legal perspective

Abstract:

This paper is aimed to understand the state of the art and the resulting consequences of the legal framework in Europe, with regard to the protection of children's data. Especially when they interact with networked and robotic toys, like in 'My friend Cayla' case. In order to evaluate the practical implications of the use of IoT devices by children or teenager users, the first part of the paper presents an analysis of the international guiding principles of the protection of minors, a category which enjoys a higher level of protection of their fundamental rights, due to their condition of lack of physical and psychological maturity. Secondly, the focus is moved upon the protection of personal data of children. Only after confronting previous data protection legal instruments and having compared them with the novelties set forth in General Data Protection Regulation, it is reasonable to assume that new provisions such as "privacy by design" principle, adequacy of security measures and codes of conduct, can support data controllers in ensuring compliance (in line with the accountability principle) in the field of IoT toys. In conclusion, the paper supports a view of Data Protection Authorities as a relevant player in enhancing these renovated tools in order to achieve the protection of children's rights, as to ensure their substantial protection against the threats of the interconnected world.

Agenda:

Authors:

Rocco Panetta

- Managing Partner at Panetta & Associati law firm, International Association of Privacy Professionals, Country Leader Italy and Board of Directors Member. Email: r.panetta@panetta.net

Federico Sartore

- Associate at Panetta & Associati law firm, Ph.D. student at Maastricht University. Email: f.sartore@panetta.net

ISSN 1614-1687

Introduction

In February 2017, the German Federal Network Agency (*Bundesnetzagentur*) stated that 'My friend Cayla' – an interactive doll manufactured by an American company – constituted a perfect example of "*unauthorised wireless transmitting equipment*"[1]. Accordingly, German regulators feared that smart toys of this kind, with concealed microphones and cameras, may constitute a severe threat to fundamental rights of children and their families.

And there is more, no highly-sophisticated hacker attack was needed to breach security measures of the connected database: due to an error of configuration it started leaking children personal data, later estimated in around half a million records.

Moreover, the case of Cayla is not an isolated threat, security failures were discovered in the Furby Connect, i-Que Intelligent Robot, Toy-Fi Teddy and CloudPets[2]. In all these cases the vulnerability was represented by a flawed Bluetooth connection, resulting in a complete lack of security with the possibility for anyone to gain access – without pin, password or other forms of authentication – to the toy. Again, no sophisticated hacking techniques were needed to pose a serious threat for the security and privacy of kids.

Once again, public authorities and commentators have moved the spotlight of inquiry on manufacturers of the so-called IoT devices and on the fundamental role played by data controllers. In fact, dystopian sceneries of mass-surveillance are simply an actual threat to our rights and freedoms. Cases like the switch of 'My friend Cayla' into a disturbing and Orwellian Pandora's box have to be taken as the last call for investing economically and culturally on cybersecurity and data protection at societal level.

These alarming facts represent the tip of the iceberg of one of the foremost issues related to robo-connected-toys: guaranteeing the maximum level protection and safeguard for personal data collected during the interactions between children and toys.

Indeed, an interesting question consists in asking whether this should be addressed as an ethical or a legal issue, and to what extent.

Beside the endless debate on law and ethics, the protection of privacy and personal data has to be considered as a fundamental right and, for this reason, deeply permeated by natural law doctrines. And no substantial difference should be found in assessing the nature of this fundamental right for an adult or a child; at most, one could argue that the special declination of fundamental rights for children is provided by other fundamental rights, specifically addressing the condition of the child and thus combining themselves. In other words, the protection of children's data is both a matter of law and ethics; in particular, of ethics in their legal transposition by means of fundamental rights legal instruments.

Differently from what is commonly said and written, EU regulators have not been left behind by the fast-growing pace of technology development. Under this perspective, the Regulation (EU) 2016/679 (the '**GDPR**'), that will come into force from 25 May 2018, consolidates the fundamental data protection principles, confirms the utmost relevance of setting appropriate safeguards for childhood and – provided a number of guarantees

[1] The press release of *Bundesnetzagentur* on the point can be found at: https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/PressReleases/2017/17022017_cayla.pdf?__blob=publicationFile&v=2

[2] R. Smithers, *Strangers can talk to your child through 'connected' toys, investigation finds*, The Guardian, 14 november 2017, available at: https://www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children.

– lighten some burdensome obligations for data controllers under the threat of significantly increased pecuniary sanctions[3].

The purpose of this article is to sketch a map of the legal protection accorded to children's data. After a brief description of the traditional legal framework, the main novelties brought by the GDPR on the point will be analysed in order to set the stage for the current state of art of children's data protection.

Guiding principles for the protection of children

Although no doubt persists with regard to the full attribution of fundamental rights to children, these rights should be also considered and interpreted against the special situation and characteristics of childhood. In this sense, simplifying, legal systems are prone to consider the child in a double-faced perspective: static and dynamic.

Where the static nature is represented by the fact that the child is a person who has not achieved yet physical and psychological maturity, the dynamic aspect is reconnected to the state of constant development of the child toward adulthood. For this reason, any discourse over children rights should address and take into consideration both these perspectives, a sort of biphasic attention of the legislator.

Taking into account the fundamental principles regulating the rights of the child, while some of them are contained within the most fundamental applicable international instruments[4], other can be found in acts specifically drafted to protect the rights of the child[5]. Regardless to the source, they can be identified – within the purpose of this article – as follows.

Best interest of the child

The 'best interest of the child' represents the core principle with regard to children's fundamental rights. Enshrined in the UN Convention on the Rights of the Child (Article 3), it has been reaffirmed in other international instruments. Its rationale is strictly linked to the unachieved physical and psychological maturity. In such a situation, the interest of the child is a useful criterion in order to avoid harmful generalizations, concretely setting a balancing exercise.

Protection and care necessary for the wellbeing of the child

This principle and its fundamental role are extremely interlaced to the above-mentioned immaturity of the child and the deriving vulnerability. This status of being defenceless shall be therefore compensated by adequate

[3] Pursuant to art. 83 of the GDPR, infringement of the provisions of the Regulation may lead to different tiers of administrative fines. The first, for less serious violations, provides for fines up to EUR 10.000.000 or, in case of undertakings, up to the 2% of the total worldwide annual turnover. The second, for gross violations, provides for fines up to EUR 20.000.000 or, in case of undertakings, up to the 4% of the total worldwide annual turnover.

[4] E.g., articles 25, 26.3 of the Universal Declaration of Human Rights (1948), article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950) and article 24 of the EU Charter of Fundamental Rights (2000).

[5] *Inter alia,* the Geneva Declaration on the Rights of the Child (1923), the UN Convention on the Rights of the Child (1989), the European Convention on the Exercise of Children's Rights (1996).

care and protection. Consequently, the focus for the full realization of this principle should be moved upon the subjects entitled to guarantee this right: (from micro to macro level) family, State and society[6].

From a data protection perspective, the pursue of this principle may entail and require processing operations of personal data or, conversely, the protection from harmful processing activities.

Representation

As it is easily comprehensible, the exercise of children's rights needs some form of legal representation. However, the application of the corollaries of the dynamic nature of the legal dimension of the child requires children's consultation on matters impacting on them and their will should be taken into account, proportionally to their stage of development. In the context of the protection of children's data, the concept of representation is crucial because it identifies an interposed data subject who has the duty to understand the meaning of the information made available by the controller and to provide the consent where needed. In fact, the first line of defence for the protection of personal data of the child is represented by the awareness of parents and guardians of the fundamental role they play in guaranteeing this protection.

Right to participate

The other side of the right to be represented consists in the right to be consulted, in relation to the degree of personal development. This right of consultation can be addressed as a duty of taking into account the child's belief and opinion, without necessarily submit to them.

In data protection terms, the application of this principle may result in a duty of taking into account the child's will of making use of a certain good of service, that may entail processing activities on personal data. However, it is highly implausible that a child may really comprehend the meaning and relevance of sharing personal data.

The scope of traditional data protection legislation for children

In the context of the main directives composing the traditional data protection legal framework – the directive 95/46/EU (the "Data Protection Directive") and the directive 2002/58/EU (the "e-Privacy Directive) – data protection rights of the children are not mentioned. The subjective scope of application of the directives broadly refers to any 'natural person', therefore including also children, without distinctions in terms of legal discipline.

This lack of attention of the European legislator resulted in a number of open questions with regard to the peculiarity of the status of the child in the context of the protection of personal data, both in terms of the definition of the degree of individual maturity as well as the requirement for representation in legal acts. In other words, the traditional data protection legislation was in particular lacking on two different layers: (1) the floating degree of consciousness determining when children can start managing their own personal data and (2) the provision of *ad hoc* guarantees in order to reinforce the level of protection for children's data.

[6] The fundamental nature of this right is confirmed by the primary consideration given by the Universal Declaration of Human Rights (Article 25), the International Covenant on Civil and Political Rights (Article 24), the International Covenant on Economic, Social and Cultural Rights (Article 10.3), and the EU Charter of Fundamental Rights (Article 24).

Consequently, rules and regulations on the validity of consent provided by kids had to be drawn from national legislation and the regulatory vacuum had to be filled by the intervention at national or EU level of Data Protection Authorities of the Member States. In particular, the Working Party *ex* art. 29 – the advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the Commission – issued the Opinion 2/2009, specifically addressing the state of the art for the protection of children's personal data[7].

In particular, with regard to the legal requirements for obtaining personal data of children in the online environment, a recent study conducted across the EU Member States concluded that many countries have not developed specific legal requirements[8]. In Spain, it is foreseen an obligation for data controllers to obtain parental consent to process personal data of children under the age of 14[9]; while in the UK the age threshold is set at 12[10].

Increased data protection safeguards for children under the GDPR

The renewed importance of protecting personal data of children is mentioned several times within the GDPR. However, most of them merely represent programmatic statements and it is likely that most of the substantive limitations to the processing of children data will come from either existing or new national laws or codes of conduct.

Therefore, the scenario arising from the traditional data protection legal framework has been only partially innovated by the GDPR, considering how the provisions of the Regulation do not provide for particularly wider harmonisation on the point. Thus, the major provision that can be found regarding the processing of children data is Article 8.1 of the Regulation, which identifies a general obligation for data controllers of attaining the parental consent to lawfully process personal data of a child where (s)he is below the age of 16 years[11] and the request for consent applies in relation to the offer of information society services directly to a child. It is undoubtable that services provided by connected toys represent information society ones and, accordingly, the awareness and control abilities of parents over their children personal data will become a crucial factor when facing the robo-toys dilemma (i.e. how to protect the children from abusive technologies).

On the other hand, data controllers are asked, pursuant to Article 8.2 of the GDPR, to make 'reasonable efforts' in order to assess and verify that consent has been given or authorized by the holder of parental responsibility over the child, taking into account the current state of art for technology. Moreover, the applicability of the 'legitimate interest' of the controller – as legal basis to undertake processing activities – finds a narrower scope of application when conflicting interests, rights or freedoms pertain to a child[12].

---

[7] Opinion 2/2009 of the WP 29 on the protection of children's personal data (General Guidelines and the special case of schools), available at: http://194.242.234.211/documents/10160/10704/1619292.

[8] N. Fulford, '*Survey: Consent to the Processing of Children's Data Across the EU'* (2011) 11(2) Privacy and Data Protection 13.

[9] Royal Decree 1720/2007, of 21 December, which approves the regulation implementing Organic Law 15/1999, of 13 December, on the protection of personal data.

[10] Information Commissioner's Office, Personal Information Online Code of Practice (2010), 15.

[11] The provision applies where the processing activities of personal data are based on consent pursuant to article 6.1 (a) of the GDPR and Member States can set a lower age threshold as low as 13.

[12] Article 6.1, (f) considers processing of personal data lawful when "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*"

With regard to Article 8, some concerns were raised about the impact of this provision on key principles of human rights law[13]. In particular, three aspects of the provision were found to struggle with human rights principles: (1) the existence of a bright-line rule to determine the degree of maturity of the child; (2) the fact that Article 8 foresees no way for the child to express his own views regarding the data processing operation, leaving the responsibility to consent exclusively on parents; (3) the limitation of self-determination of the child reconnected to the invasion of their personal sphere by the parents in order to exercise their control. These criticisms are formally correct and embraceable; however, a certain degree of generalization cannot be avoided during the draft of a general regulation and the gap between the abstract and general rule and the actual behaviour of children and parents should be filled by soft law instruments – such as guidelines, recommendations and clarifications from the DPAs and other regulatory bodies.

Moreover, the GDPR also takes into consideration the provisions of concise, transparent and easily comprehensible information notices to data subjects, particularly with respect to children. Article 12 of the Regulation sets the principle that is further expanded in its meaning by Recital 58: "*Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand*". Given the well-known questions and doubts regarding the effectiveness of traditional information notices for adults, it is highly unlikely that children – even if teenagers or young adults – will benefit from simplified notices[14].

Finally, the processing of particular categories of children's data does not receive a specific and distinct regulatory framework due to the fact that processing of these categories of data involves a higher degree of risks for rights and freedoms of the individuals and, consequently, requires *per se* additional and enhanced safeguards, irrespectively to the status of the data subject.

Additional provisions regarding networked toys and IoT

The slightly different status of personal data of children is just a very limited part of the whole data protection legal framework, designed and implemented to protect individuals against the threats of an ubiquitous and always connected world.

In particular, the GDPR introduces the widely-discussed concept of 'Data Protection-by-design'[15]. In brief, data controllers – taking into account the state of the art, the cost of implementation and the nature of processing as well as the risks for rights and freedoms of natural persons – will be required to implement appropriate technical and organisational measures, designed to integrate data protection principles, such as data minimisation, necessity, transparency and connected necessary safeguards, into the processing operations[16].

Although the nature of the provision set by Article 25 is of being generally applicable, Internet-of-Things (IoT) represents the field on the front line to test the potentiality of embedding data protection and respect for data subjects' fundamental rights into the design of industrial processes and real objects. In these terms, the

[13] L. Jasmontaite, P. De Hert, "*The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet*", International Data Privacy Law, 2015, Vol. 5, No. 1.

[14] That would actually benefit data subjects as a whole in line with principles of transparency, extended user control and fairness of the processing.

[15] The origins of the concept can be found in the paper *Privacy-enhancing Technologies: the path to anonymity* (1995) by a joint team of the Information and Privacy Commissioner of Ontario, Canada, the Dutch Data Protection Authority and the Netherlands Organisation for Applied Scientific Research.

[16] See Article 25 of the GDPR.

circumstance of a good or service to be aimed to minor customers shall not be treated indifferently by the manufacturer. Curiously, while the obligation of implementing data protection by design features set by Article 25 is referred only to the controller, the Recital 78 sets a broader scope of application for the principle, encouraging also producers and manufacturers to design their products having in mind the respect for users' privacy, with special attention toward children. The choice of the legislator is clearly to identify in the controller the only subject directly responsible for the implementation of the "technical and organisational measures" required by the Privacy-by-Design principle. However, manufacturers and data processors should be prepared for a similar implementation because they will likely be asked by data controllers to act in this sense at a contractual level.

Therefore, the protection of children's data can be imagined as a multi-layered structure. The first basic level consists in the entire body of provisions generally applicable to any natural person. The second is represented by the ad hoc provisions for children with regard to consent and information notice to be provided. Finally, the top-level can be described as all the open provisions which require controllers and processors to adapt their processes to the movable parameter of adequacy of the safeguards to factual elements[17].

This third level is undoubtedly the context where relevant players will be asked to seriously take into account the general principles protecting the child. A strong link between the best interest of the child and these open provisions shall be established. Not only with regard to the above-mentioned Article 25 and its demand for a technological development able to adapt itself to the higher degree of risk posed by the interaction of a child with the "machine", but also referring to the important field of security. In particular, Article 32 of the GDPR, setting the general rule on security measures, openly refers to "*appropriate technical and organisational measures to ensure a level of security appropriate to the risk*", where the risk has to be assessed with regard to a number of factors and the fact that the data subject is a child cannot be excluded from consideration.

Furthermore, it has to be considered that the newly introduced tool represented by 'Codes of conduct' directly addresses the processing of children data. If well implemented and designed, codes of conduct may represent a form of proactive, ethical and competitive form of compliance for data controllers in the robo-toys market. Indeed, codes of conduct have been introduced by Article 40 of the GDPR and can be considered a form of *soft-law*, designed by the EU legislator in order to adjust the rules of the GDPR according to the needs and risks of specific sectors of the industry or categories of controllers or processors. The adherence to a code of conduct may be used by controllers and processors as an element whereby demonstrating compliance with the requirements of the GDPR. To this regard, the field of IoT and, in particular, IoT applied to toys may represent a perfect example of a sector which requires *ad hoc* specifications and differentiations of rules of detail in relation to the higher degree of risk necessarily implied by these technologies and categories of recipients.

Conclusion

The purpose of this brief analysis is to provide a sketch of the actual situation: the degree of risk for the rights and freedoms of children is certainly getting higher with the technological development, threatening those fundamental principles ingrained in our legal system. However, the reform of the legal framework for EU did not omit to update the rules, setting both specific provisions and open parameters to permit a better adaptability of data protection norms. As a result, from now on, a healthy and fast-growing market of robo-toys cannot

[17] Art. 25 of the GDPR sets as relevant parameters: (a) the state of the art, (b) the cost of implementation, (c) the nature, scope, context and purposes of processing, (d) the risks for rights and freedoms of natural persons posed by the processing.

neglect the respect of the specific provisions on children's data, the implementation of security measures, the principle of data protection by design and the opportunities provided by codes of conduct.

On the other hand, this open nature of important provisions – such as Article 32 on security measures – necessarily needs further specification by Data Protection Authorities in order to become really effective. Given the impressive sanctioning firepower provided by the GDPR to the DPAs[18], they should be in a perfect position to enact and make effective the provisions of the Regulation. In fact, cases such as 'my friend Cayla' are extremely serious and alarming, revealing that some players on the market still have not fully comprehended the importance of setting lawful processing activities and the actual level of risk posed by their misbehaviour for the special category of individuals represented by children. For this reason, it is important for DPAs to couple their guiding activity with effective enforcement toward those who violate the general rules of the Regulation and, more importantly, the specific rules regarding children's data.

References

Bundesnetzagentur. Bonn, 17 F Ebr Uary 2017 Page 1 of 2 Bundesnetzagentur Removes Children's Doll "Cayla" from the Market . 17 Feb. 2017, www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/PressReleases/2017/17022017_cayla.pdf? blob=publicationFile&v=2.

Fulford, Nicola. "Survey: Consent to the Processing of Children's Data Across the EU." Privacy and Data Protection , vol. 11, no. 2, 2011.

"Opinion 2/2009 of the WP 29 on The Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)." 194.242.234.211/documents/10160/10704/1619292.

Palfrey, John G., and Urs Gasser. Born Digital: Understanding the First Generation of Digital Natives. Read How You Want, 2011.

Smithers, Rebecca. "Strangers Can Talk to Your Child through 'Connected' Toys, Investigation Finds." The Guardian, Guardian News and Media, 14 Nov. 2017, www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children.

Acts and authorities cited

EU Charter of Fundamental Rights (2000).

European Convention on the Exercise of Children's Rights (1996).

Geneva Declaration on the Rights of the Child (1923).

Information Commissioner's Office, Personal Information Online Code of Practice (2010), 15.

International Covenant on Civil and Political Rights (1966).

International Covenant on Economic, Social and Cultural Rights (1966).

[18] See note 3.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

UN Convention on the Rights of the Child (1989).

Universal Declaration of Human Rights (1948).

Interview with Isabelle Moeller:

Ubiquitous and Positive Biometrics

Abstract:

In this interview with Isabelle Moeller questions surrounding the responsible use and development of biometric apps are explored. The use of biometrics - originally to digitally represent and authenticate an identifiable characteristic of a product or a person - have become so wide spread that they are capable of facilitating ever greater continuous surveillance of the what, how, when and where of life. The more biometrical data of a user is collected, the more the integrity of the underlying e-identity is open to fraud and being invisibly compromised. Ethical reflection is long overdue but a prerequisite of minimizing risk to the autonomy of the human person as well as to the integrity of his digital persona.

Interviewee:

Isabella Moeller, MA

- Chief Executive, The Biometrics Institute, London and Sydney.
  Email: manager@biometricsinstitute.org
- The Biometrics Institute - founded in 2001 - is an **independent** and **impartial international** membership organisation. It is a unique forum that brings together the whole of the biometrics industry – users, suppliers and researchers – while giving users more power in setting the direction of this not-for-profit membership organisation through double the voting rights and a majority on the Board of Directors.

ISSN 1614-1687

Introduction

For philosophers and social scientists, the exercise of power presents many challenges. The exercise of of arbitrary power especially raises concerns both about the purpose of arbitrariness as well as that of accountability. Ethics in implicit. The automated exchange of data and information by robots and strings of code without human intervention begs questions about arbitrariness and power. It also appears to objectify the human, incrementally removing human agency and potentially liberty and autonomy. The internet of Everything requires use to reconsider the scope of resulting challenges to our contemporary understanding of what it is to be human and what, when, how and whether the automated code embedded in everyday life is ethically aware or informed.

The challenges society faces go way beyond constitutional and legal issues: they demand an interrogation of the fundamental tension between the use and abuse of power for ethical and unethical ends by both knowing humans and human-coded machines invisibly qualifying human free choice and shaping the range of human choice. This tension was and remains at the heart of everything and every policy area. The question is what the development of digital life, digital traces and onward use of digitised information that is readily linked to an individual person – as in the case of biometrics – tells us about the nature of digital society and what it means to be a human in a society increasingly adapting to machines mediating our sense of beingness. This begins in babyhood and may have profound implications for our sense of self, autonomy, liberty and responsibility. Interaction with machines is not value-free. Nor is it confined to considerations about invisible ubiquitous tracking and surveillance, and the associated erosion of privacy and notion of informed consent. The digital world begs the question : has the transformative potential of automated data linkage in what is sometimes called an information society been realised, corrupted or (ab)used for (un)ethical ends?

The digi-power dilemma arises not simply from the existence of and accessibility to so much digitised information but from the invisibility of three things: (1) a recognisable and identifiable 'face' to show who is using information over which individuals have lost control, and (2) the invisibility of the fate of that information as it is (ab)used in full or in part by whoever accesses it for known and unknown purposes, often distinct from the purpose for which the information was first provided by, or *accumulated about,* the individual, and (3) most critically, the unknowability for individuals and society about the ultimate locus of both the information slices and whichever machine, contains them temporarily or as permanently as say processing and storage of an e-document trace allow.

Central to the question of identifying who or what is using information is the issue of responsibility and accountability for its use, handling and processing. That is a core principle of legal redress. It is key to concepts of transparency and public accountability in all domains. A lack of recognisability and identifiability of who or what is using information reveals a paradox. On the one hand, the individual must constantly assert and prove their claim to be the authentic owner of a digitized 'identity'. On the other, the human relies on a string of code to validate that claim, usually by linking it automatically and invisibly to some other bit of code. For the human, what is visible is rarely the code but instead some coded representation of an element of himself : a biometric token that trades in probability matching. The tools developed to get and use biometric information skew our understanding of the acceptable limits of public and increasingly privatised or semi-privatised and commercialised intrusion into the private sphere.

During the past decade, the term biometrics has been re-fashioned to conflate the original notion of an algorithm to digitally represent and authenticate an identifiable characteristic of a product or a person with practices that exploit both that identification mechanism and which rely on societal prioritisation of 'security and safety' in order to make such intrusion seem normal; render it so invisible to the individual and society as to encourage them not to think about it; and so facilitate ever greater continuous surveillance of the what, how, when and where of life.

Governments used to monitoring behaviour, see in 'biometrics' and research into biometrics, a short-cut to removing uncertainty by exploiting monitoring techniques to make the unpredictable predictable. Small scale biometric experiments, as in the case of automatic border controls, e-passports, e-visas and e-civil documents,

e-banking, e-health have been trialled and presented as convenience gains to citizens and administrative cost-saving gains to governments and commercial ventures alike. However, the accompanying rationale for ever greater surveillance and monitoring by means of linking-up the smaller scale trials is out of step with technological innovation. Technology's capacity to scale-up sometimes lags behind practices which in other contexts would have been deemed politically questionable and unacceptable. However, the opportunities for invisible tracking and linkage attract those who prioritise speed (and convenience) over careful consideration of the purpose behind them, much less the legitimacy or proportionality of such a purpose. The lure of doing something because it is technically possible to do so has held sway over other considerations.

Only more recently have privacy impact assessments become normalized. Even if desirable and necessary, by themselves they are not sufficient. Interoperability is still the holy grail, even if still compromised by significant technical problems. Even so, generating, acquiring, managing, possessing, accessing, splicing, sharing and selling ever more data information proceeds apace, accelerating so far beyond the capacity of data protection authorities and legislatures to protect personal data sufficiently and guard against individual and collective harm. Thus, the 'do no harm' principle of ethical codes is transgressed. The 'right to forget' is laudable but electronic trails remain somewhere that may be unknowable and those trails may become corrupted over-time leaving legacy traces that in turn are unreliable but may nevertheless be (ab)used. How much certainty can or should we attach to technical 'proofs' of the authenticity claim to own an identity, including one's personal identity? Can we develop an innovative identity ecosystem using novel technical capabilities to address more effectively the challenges posed by wrong identity, identity fraud and associated types of cyber and other forms of organized crime?

For industry, biometrics provides at least part of an affirmative answer: probability matching of a token to a person or commodity is enhanced under certain circumstances. But biometrics are not infallible. Yet they are increasingly key to how an algorithm links it automatically to other information and data, or uses it to 'make' automatic decisions about the fate of its subject – the human, a commodity, an animal, plant or mineral. This can of course be very useful. It can also be a double-edged sword. Direct and immediate human analysis is removed from real-time automatic machine decisionmaking in ways that may harm a person or at the very minimum inconvenience him.

The power of an algorithm is misunderstood and exaggerated. Assumptions made when fashioning algorithms and deductions made when employing them need to be better understood. The preconceptions and biases of who or whatever does either must be made explicit. Neither are value free. Neither are neutral. Neither are infallible. Both are likely to have potentially dangerous consequences when used or combined with other data and information or used for purposes which were not envisaged, or not the original purpose. Both human and automated machine analysis can be fallible.

One of the more intriguing challenges posed by artificial intelligence relates to how machine/robot – human interaction and human use of the machine may change the way in which the human relates to his environment. This is not just about 'out-sourcing' memories to the cloud and storing information, such as biometrics, on a mobile device. It is about the potential impact of the robot on human-to-human relationships and interaction. This has been typically described as a master-slave relationship, where the human is master and the robot a tool. This might be an appropriate analogy in a factory assembly line. But, it is questionable in the case of any automated sifting of information designed to match a pre-determined 'profile' with another one in a mass of information, as in the most obvious case of border controls and the use of biometrics to access services.

If, as a society, we are better to understand the impact of something that is rapidly becoming more widely used as a means to authenticating identity claims, it is important to be clear about purpose and about who or what is generating 'information' or 'decisions' (new algorithms derived from the first set of assumptions). What are the underlying assumptions and biases that inform how an algorithm is framed and then used both in real-time and 24/7 by both humans and other automated robots? Wherein lies the allure of biometrics?

Biometric apps are imperfect. Biometric attributes change over time: eg finger prints and voice prints degrade with age: for example, the former are less reliable after the age of 45. However, the idea of using a biometric from birth is gaining advocates. The child's toy that responds automatically to its voice relies on processing that

voice biometric and linking it to other strands of information. Alll can be re-used and re-purposed without reflecting on proportionality and purpose. Instead, priority has been attached to the question of how a person's claimed e-identity be made both secure and private. Creating an appropriate balance in the digital single market between privacy and security remains a core challenge and opportunity in developing and managing e-identity. Ensuring privacy and security for our digital persona has to be considered at all stages in the definition and design of any technological project. The more personal data about a user is collected, the more the integrity of the underlying e-identity is open to fraud and being invisibly compromised. E-identity is vulnerable. In that case, asking how to minimize associated risks should, but does not always, begin with reflection on the purpose(s) for which it is created and used. Purpose minimization is often incompatible with the wider commercial goals of interoperability. How, when, who, what and for how long algorithmic information empowers and disempowers needs to be better understood. Ethical reflection is long overdue but a prerequisite of minimizing risk to the autonomy of the human person as well as to the integrity of his digital persona.

In the following interview with Isabelle Moeller, CEO, Biometrics Institute (founded in 2001), Sydney and London, questions surrounding the responsible use and development of biometric apps are explored.

Ubiquitous and Positive Biometrics

Editors: *Why biometrics?*

Isabelle Moeller: Biometrics are everywhere. They are portrayed as the secure and convenient solution to 'proving' identity claims for all manner of transactions from accessing a mobile phone or bank account to paying for goods and services, and crossing international borders, notably at airports. Biometrics have become more widely deployed in all manner of apps, artificial intelligence, banking, travel, domestic robots, children's toys and used as the preferred means for authenticating children registering for school and paying for lunches, for example. This raises profound ethical questions about the nature of society that is being created. These questions dovetail with those around privacy, data protection and consent.

Editors: *why is interest in using biometrics rising?*

Isabelle Moeller : For consumers and industry alike, the asserted convenience and time gains seem persuasive enough to commend the more widespread use of biometrics to 'prove' an asserted claim - you are who you say you are – upon which entitlement to proceed with a transaction depends.

Editors: *Would you say that biometrics are just associated with 'Big Brother'?*

Isabelle Moeller: Not anymore. People who have passports and come across automated physical border management systems are usually familiar with wider uses of biometrics, such as payments. But how much society willingly accepts them varies from country to country.

Editors: *Countries and jurisdictions differ in how acceptable they find biometric identifiers in different contexts. What is the role of the Biometrics Institute in addressing the challenge? How can we try and move towards a consensus internationally about ethical use?*

Isabelle Moeller: It is vital to have a space where ideas can be challenged and an independent voice can emerge. The Biometrics Institute is the **independent** and **impartial international** not-for-profit membership organisation that offers a unique forum that brings together the whole of the biometrics industry – users, suppliers and researchers. It gives users more power in setting the direction of the organisation through double the voting rights and a majority on the Board of Directors. The mission of the Biometrics Institute is to promote the responsible use of biometrics as an independent and impartial international forum for biometric users and other interested parties.

Editors: *How does the Biometrics Institute begin to examine the social impact of biometrics?*

Isabelle Moeller: The Biometrics Institute created a Special Interest Group in January 2017 to help map out the environment. Organisations currently engaged include **DHS USA, UNODC, DIA New Zealand, Amber Alert, NCMEC and other**s. We are still scoping the focus. Social impact can be broken down on a policy specific basis like crime prevention or take a more holistic view to the role of biometrics in respect of social enablement (a basic human right).

Editors: *The two examples you give are not necessarily mutually exclusive are they?*

Isabelle Moeller: No indeed. If one looks at first world challenges like preventing child exploitation and child trafficking, it is tempting to legislate against such practices. Biometric identifiers may be used as a tool by those seeking to investigate, prosecute and prevent such crimes. Biometrics may be a means to help authenticate a child's claimed identity, for example, in natural disasters or war zones, in establishing origin and links in cases of migration, trafficking and modern slavery. But taking a wider view, legislation is not enough. Children are vulnerable in terms of their identity because in part they have to rely on adults providing one for them. These adults may be the perpetrators of crimes involving children. Can biometrics help to protect the child, for example, where modern slavery and cross border trafficking are concerned?

Editors: *so how do we confront the challenges posed by using biometrics to effect change for the good of society?*

Isabelle Moeller: The Biometrics Institute consults its members to define the focus area and assess what can be done to make a change. Do we need guidelines, a statement on research priorities, more of the think piece work to create debate, sponsoring an industry 'competition ' to encourage development of solutions, approaches to multilateral organisations/governments to encourage development of policy?

Editors: *If you begin with the issue of children's rights…*

Isabelle Moeller: having an identity is surely a human right for children. So for us the starting point might be to ask what stops the provision of such an identity. What are the barriers to solving this?

Editors: *presumably there is a lot of interest in how children's identity is authenticated online?*

Isabelle Moeller: Certainly, and also in preventing and resolving child exploitation online. Biometrics have a place in helping to pinpoint the criminals. A further question arises as to how biometrics can be exploited to prevent and resolve missing children and trafficking; create internet safety; combat exploitation of vulnerable people, including children, and illiterate people.

Editors: *Do you see biometrics as a means of enabling the excluded to become more included in society?*

Isabelle Moeller: yes. For example, biometric payment methods could be a safe way for illiterate people to make transactions, or make payments. What is it that inhibits this as a focus? How can biometrics have an ethical impact for sectors of society that are vulnerable and excluded?

Editors: *What is stopping this from being solved?*

Isabelle Moeller: Biometrics are a tool, part of a solution. We need to ask appropriate questions and then come up with some answers that reflect our values. We need to work together across sometimes competing sectors, industries, business models, governments and policy interests to focus on the needs of society in the 21st century and give voice to critical reflection that may challenge long-held assumptions and encourage innovation. If biometrics is an appropriate tool, how can we better use it?

Editors: *Thank you.*