Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

# Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust

Esther Keymolen & Simone Van der Hof

**To cite this article:** Esther Keymolen & Simone Van der Hof (2019) Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust, Journal of Cyber Policy, 4:2, 143-159, DOI: 10.1080/23738871.2019.1586970

**To link to this article:** https://doi.org/10.1080/23738871.2019.1586970



Published online: 01 Mar 2019.

JOURNAL OF CYBER POLICY
2019, VOL. 4, NO. 2, 143–159
https://doi.org/10.1080/23738871.2019.1586970

Routledge
Taylor & Francis Group



# Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust

Esther Keymolen [a] and Simone Van der Hof[b]

[a]Tilburg Institute for Law, Technology and Society, Tilburg University, Tilburg, The Netherlands; [b]eLaw, Center for Law and Digital Technologies, Leiden University, Leiden, Netherlands

**ABSTRACT**

The purpose of this article is to show how the smartification of children's toys impacts the concept of trust. We make use of the 4Cs conceptual trust framework – context, construction, curation, codification – to analyse how the technological, commercial and legal developments central to the arrival of the Internet of Toys have an impact on the trust relations of children, parents and the companies behind smart dolls. We found that the introduction of smart dolls brings forth several trust issues. First, important vulnerabilities, such as monitoring practices and data-sharing, take place *beyond the awareness* of children and parents. Even if they try to read the terms and conditions or look into the technical specifications of the toys, these products remain *black boxes* because the operating systems are proprietary and not all information is disclosed or understandable. Second, with the arrival of smart dolls, a form of *hybrid ownership* arises. Because of the networked character of the dolls, they remain under the influence and control of the company. Children and parents have to trust the companies not to abuse this connection. And finally, the regulatory framework that should protect children is not only inadequate, it might actually exacerbate trust issues.

**ARTICLE HISTORY**
Received 5 September 2018
Revised 12 November 2018
Accepted 11 December 2018

**KEYWORDS**
Trust; smart toys; regulation; internet of things; internet of toys; GDPR

## 1. Introduction

Almost all children in the Western world are online – and so are an increasing number of the artefacts that surround them. Not merely computers – including smart phones and tablets – but the mundane physical things around us, such as thermostats, television and washing machines, are increasingly connected to the network of networks to make our lives more fun and convenient. These interconnected items develop into what are called 'smart devices' that are capable of predicting individuals' preferences and needs based on their online and offline behaviour. The Internet of Things – as we call this phenomenon – is extending also to children's toys, i.e. smart toys. Smart toys are internet-enabled toys that interactively engage with children while they are playing.

**CONTACT** Esther Keymolen e.l.o.keymolen@uvt.nl

The best-known example to date is Hello Barbie, which is an internet-connected Barbie doll that talks to children and answers questions. When the doll is activated, everything the child (or anyone else present for that matter) says is transmitted to ToyTalk, a company that analyses the conversation and provides Barbie's response to the child within (milli)seconds (Gibbs 2015). Moreover, smart cuddly toys exist that also allow children to chat with them as part of their play.[1] The smart play experience can be augmented by apps on smart phones and tablets. Additionally, smart computing devices – such as smart phones, smart watches and tablets – have been developed as children's toys.[2]

The development of smart toys fits in with broader trends of hyper-connectivity, datafication and commercialisation (van der Hof 2017) and changes the trust relationship between toy manufacturers and consumers by adding new complexities that tie in with each of these tendencies. With traditional toys, trust is mostly a matter of expecting toys to be appropriate in terms of physical safety. Some toys or the materials they are made of are safe only for certain – mostly older – ages. Toys that become digitally connected devices – despite superficially resembling their traditional counterparts – have whole new trust dimensions added to the equation because the nature of the artefact changes considerably and these changes lead to increased complexities.

Smart toys come in different forms but they have one thing in common. The development of these toys is not just a feature of ongoing technological developments; their emergence also reflects an increasing commercialisation of children's everyday lives. Playing with toys is no longer *just that*; the purpose and meaning of the toy changes because its design changes – i.e. the artefact (in this case the smart toy) is augmented by digital technologies. In other words, the toy becomes part of a meticulously orchestrated game plan of companies in which they construct and script a world that may be fun and entertaining but, more sophisticatedly, serves their economic interests. Hence, a toy may – in the case of smart dolls – still *look* like its traditional counterpart, but in fact, below the surface of their cute appearances, the identity and intentionality of the artefacts have changed completely.

Trust in the relation between the manufacturer and the consumer starts playing a much more pivotal role because of growing uncertainties. How is the child's personal data used? Who has access to it? Will the data be safe?[3] Will the child or parent be informed when data is compromised? Will the product be safe (e.g. not overheat or emit harmful radiation) and secure? Can the child be manipulated by a talking toy? Etcetera. The answers to these questions are not always easy – or possible – to find, and companies have no incentive to be sufficiently open about some of them. Marketing works best, for instance, when people are not aware of being manipulated, and numerous ways exist to trick people's minds without them noticing (Kahneman 2011).

The purpose of this article is to show how the smartification of children's toys impacts the concept of trust. To set the stage for our analysis we first outline important technological trends (section 2). Then we will present the conceptual framework that will be used to analyse smart toys in relation to trust (section 3). This conceptual framework encompasses the four C's – context, curation, construction, codification – that will in the subsequent sections (4 to 7) be used as lenses for the analysis of the concept of trust in relation to smart toys. The article wraps up with conclusions in section 8.

## 2. Technological trends

Current smart toys are indissolubly linked to the arrival of what has been called the Internet of Things (IoT). The basic idea behind the Internet of Things is that by connecting physical objects, equipped with sensors, to the internet, it becomes possible to translate all sorts of actions into computer-readable data. This is also referred to as datafication (Mayer-Schönberger and Cukier 2013). The internet connection can be set up in different ways. For example, smart doll Cayla connects via Bluetooth, whereas Hello Barbie has a Wi-Fi connection. Based on data analytics and machine learning, the functioning of the device is adapted, blurring the boundaries between the physical and digital world (Floridi 2015, 2). In practice, this means that internet-connected devices can, amongst other things, communicate with each other, transfer data to third parties for analytic or other commercial goals, and proactively deliver services tailored to the needs of users.

By adding this computational component to artefacts, they are increasingly becoming 'smart' (also see Kopetz 2011, 308). Fuelled by data analytics, these smart devices can adapt their behaviour to their environment and users. In some instances, they can even display a – limited – form of autonomy. While the networks of information in which these smart devices are embedded are crucial for their functioning, they often remain invisible to the user (Keymolen 2016, 147)

The development of smart artefacts in an IoT ecosystem has led to all sorts of new services, which can be characterised as *personalized, proactive* and *persuasive*. The goal of *personalization* is to deliver content or services tailored to the explicitly provided or implicitly determined wishes of users by making use of a set of technological features (Thurman and Schifferes 2012, p. 776).

Hello Barbie, for example, makes use of speech recognition to adapt her answers to the questions of children. The services delivered by smart artefacts are not only personalised but also *proactive* or 'anticipative' (van den Berg 2009, 71), i.e. they precede the request of the user. Smart dolls such as Cayla and Hello Barbie are designed in such a way that children can, without extra action, just talk and interact with them. The smart dolls ask children, for example, to sing or play with them. As smart artefacts can proactively deliver personalised services, they can also become *persuasive*; they can 'explicitly influence the behaviour of users in specific directions, effectively persuading people to behave differently' (Verbeek 2011, 19). Particularly in relation to children, this element of persuasion – for example when children are influenced to buy certain products – may be a cause for concern.

All in all, these technological developments have led to a specific kind of Internet of Things, namely an *Internet of Toys*. Because of its 'natural, interactive, adjustable character', the child-smart toy interaction goes considerably beyond the interaction with classic toys (Chaudron et al. 2017, 14).

## 3. Conceptual framework: smart toys in relation to trust

Central to this article is the question how trust relations are shaped by the use of smart toys. Trust is generally perceived as an important strategy to deal with the uncertainty inherent in social life (Luhmann 1979; also see Möllering 2006). Early in life, children

develop a sense of basic trust by interacting with their parents and siblings (Harris 2012). They need to experience and learn that they can rely on others. This basic trust then serves as a stepping stone for relations outside the family domain, enabling them to interact and cooperate in society (also see Giddens 1990, 1991; Simpson 2012).

Although trust is a fuzzy concept, in the sense that it always seems to escape a final, all-encompassing definition (Simon 2013), we can identify a minimal set of key concepts we need to consider when analysing trust (Möllering 2006). First, we need to have at least two actors: a *trustor* who has positive expectations of the actions of another actor, a so-called *trustee* (idem 7).

Second, there needs to be something at stake for the trustor. She can be hurt – understood broadly – by the actions of the trustee (idem 8). Trust is a risky business (Luhmann 1979) and is intrinsically connected to *vulnerability* (Baier 1986). If there is nothing to lose, trust is redundant.

Third, trust cannot be enforced. The trustor is dependent on the actions of the trustee. To speak of trust, the trustee needs to have *agency*.

Fourth, the fact that trust cannot be enforced means that it is also closely connected to *uncertainty*. If you know for sure what the future will bring, trust is meaningless. Trust is a strategy for dealing with the complexity brought by an uncertain future (Luhmann 1979, 1988). Rather than trying to diminish this uncertainty, trust is a positive acceptance of the contingency of human life (Keymolen 2016).

Finally, trust entails a leap of faith. Although we don't know for sure what the future will bring, by acting *as if* we do know, social life is made possible. Möllering (2006, 6) states that trust is 'ambivalent', 'because it solves a basic problem of social relations without eliminating the problem'. Our interactions with others remain uncertain in a trust relation, but we don't let this stop us because we positively assume that this vulnerability will not be a problem and that no harm will be done (idem 9).

Trust is not merely a strategy to deal with uncertainty in social interactions. As our interactions are increasingly organised around, and moulded by, technologies, trust is also a crucial factor when it comes to accepting new technologies (Kiran and Verbeek 2010; McKnight and Chervany 2002; McKnight, Choudhury, and Kacmar 2002). It is important to acknowledge, however, that *trust in technology* is a too broad an idea to be meaningfully addressed. Trust therefore should be understood as *trust in specific artefacts* to perform a certain pre-defined task (Pitt 2010).

Simultaneously, the way in which trust is established is also shaped by the artefacts involved (Kiran and Verbeek 2010). Technologies are not neutral instruments, but rather they *open up* the world to us in a particular way; highlighting some parts of reality, while letting other aspects recede into the background (Ihde 1990). Technologies 'mediate what we believe to be the case, what we believe to be possible and what we believe to be desirable' (Swierstra and Waelbers 2012, 160).

In order to analyse how trust takes shape in the context of smart toys, it is important to take into account the networked quality of these smart artefacts. In general, end-users only perceive the application level of the internet – the apps, interfaces and smart devices – while other crucial but intangible aspects are hidden behind the interface, such as algorithms, databases, companies and regulators. To understand the impact smart toys have on trust, it is key to look not only at what end-users such as children and parents directly

perceive, but to include what takes place behind the interface, beyond their immediate awareness. Based on the layered character of the internet itself, we will therefore analyse trust on four different levels: *context, construction, curation* and *codification* (Keymolen 2016).

### 3.1. The 4Cs conceptual framework

*Context* refers to the first-person experiences that users have. These experiences include their interactions with others, with the smart toy they play with, and the relations mediated by the smart toy (also see Ihde 1990; Verbeek 2011). It is generally accepted that trust arises on this micro-level and can be seen as the starting point for understanding how users build and experience trust.

*Construction* refers to the design of the smart toy, including both software and hardware components. These technical components may present certain risks for the child and its environment, for example when a doll might easily be hacked to access data or can even be hijacked and controlled by a malicious actor. The way in which a smart toy is built to a large extent also determines what a child can or cannot do with it. The design of the artefact defines children's so-called *action space*. The design of a technology can be used to make certain unwanted behaviour impossible because the functionality of the artefact simply does not allow it ('techno-regulation') (Leenes 2011; Lessig 2006; van den Berg and Keymolen 2017; Yeung 2017). Or certain incentives can be built into it to persuade users to behave in a certain way ('nudging') (Thaler and Sunstein 2008).

*Curation* refers to the actors governing the smart toy. This may include: the company producing and selling the toy, the third parties who have digital access to the toy, and the data analytics company providing speech recognition. The interests of these curators do not necessarily align with those of children and their parents. When parents and children become aware of such conflict of interests, for example due to negative media coverage, their trust vested in the smart toy and its curators may be challenged.

*Codification* refers to the rules and regulations put forth by the curators as well as the legal frameworks and requirements they have to comply with. In theory, these rules and regulations might add to the trustworthiness of the smart toy. However, it is not always clear to parents and children what these rules and regulations – e.g. the terms and conditions of a certain service – actually mean in practice, because they generally don't read them and if they do read them, they might not understand the vague and complicated wording (see in general: Schermer, Custer, and van der Hof 2014).

## 4. Context

At the context level, we look at the way in which the user, from a first-order perspective, experiences the smart doll and how, also from a first-order perspective, the smart doll *mediates* relations with others (Verbeek 2010, 2009). In the case of the smart doll, the relation of the child with the smart doll and the relation of the parent/caregiver with the smart doll are key. Generally, in human-technology interactions, the interface plays an important role, as it is the point where user and device 'meet' each other. When it comes to the interface of the smart doll, two aspects stand out.

First, where the interface of data-driven devices is generally a screen, the smart dolls, being part of the Internet of Things, have a more tangible interface (Allen 2004). Hello Barbie has a small button you have to push in order to start the conversation. Whenever the child answers, the button has to be pushed again. It all is very easy to use. This is important when it comes to trust as the 'perceived ease of use' may influence potential users' decision to take on a certain device (Davis 1985, 1993; Venkatesh and Davis 2000).

A second aspect of the interface that stands out is that this tangible interface is not the only interface. Hello Barbie comes with an app. The app also provides parents or caregivers with an interface to interact with the doll. For example, all conversations the child has with the doll are recorded and can be listened to through the parental account. Research indicates that children are generally not aware of this second interface and its functionalities (McReynolds et al. 2017). In their interaction with the doll, children might therefore assume only that they are playing with the doll, while in fact the doll may also function as a monitoring device in the hands of their parents.

Next to the consideration of whether the doll is easy to use, there is also the question of 'perceived use' (Davis 1985, 1993; Venkatesh and Davis 2000) or, in other words, the question as to what can be done with the doll – which is also important when it comes to trust. Customer reviews[4] and research (McReynolds et al. 2017) indicate that the speech recognition technology is far from foolproof yet; the doll often goes into a loop and interactions with the doll are still limited to certain predetermined areas.

Interviews with parents suggest that this limited functionality leads them to think that control, for example on language use – what questions the doll should answer and in which way – is not such a pressing issue (McReynolds et al. 2017). In other words, although the limited functionality of the doll may be disappointing both for children and parents (idem), on the other hand, the rather restricted interaction with the doll also makes it more predictable and easier to trust.

### *4.1. Trust on the context level: some challenges*

When analysing trust at the context level, the ability to learn from their interactions with the user, and thus become smarter, is central to smart dolls given their machine-learning capacities. As the companies behind the doll (also see section 5 and 6) record all conversations with Hello Barbie, they can use this data to improve their speech recognition technology. By contrast with analogue dolls where the functionality remains the same throughout the whole life cycle, with smart dolls this is no longer the case. Current expectations of parents and children concerning the – limited – functionality of the smart doll may in the future no longer match the actual behaviour displayed by the doll after being further smartified. Consequently, a breach of trust may appear when this mismatch between expectations and actual functioning becomes apparent.

Next to trust in the functioning of the device, the smart doll also influences the trust relation with parents and caregivers. Generally, children are unaware of the possibility of their parents eavesdropping on their interactions with the doll. As a consequence, when they find out, this can be experienced as a privacy breach and additionally as a breach of trust. One child, after being told by his parent that all he had said to the doll was recorded on the computer and could be played back so they (parent and child)

could talk about it, responded: 'That's pretty scary' (McReynolds et al. 2017). One strategy to remedy this issue from a design perspective is to add recording signals to the device to make explicit for the user when sound is being stored and to enable the adjustment of privacy settings accordingly.

Finally, it has to be noted that trust on the context level is connected to what children and parents *perceive* to be at stake. Notably, with smart and connected toys, what actually *is* at stake – in other words, what makes users vulnerable – may to a great extent lie beyond the interface, out of reach of direct experience. When it comes to the sharing of data with third parties, data security and other privacy-related issues, users of the smart doll need to look beyond the interface and delve into terms and conditions, the website of the company and other sources to inform themselves. This crucial information is not integrated into the design of the smart doll as such.[5] As a consequence, the burden of being well-informed weighs heavily on the shoulders of users. And even when users take the time and effort to delve into the terms and conditions and privacy policies, these documents do not always disclose all information or are drafted in very technical and legal language (also see section 6 and 7).

## 5. Curation

Curation concerns the governance of a particular development by multiple actors, which in the case of smart toys shows two distinct shifts. First, smartification of toys entails a growth in the number of actors involved in offering and using the product as part of children's play experience. This results in a network of curators to operationalise the doll and enable more sophisticated business models.

Second, the actual number of actors involved may not be immediately conspicuous to consumers – parents and children – and their roles, responsibilities and mutual relations are likely to remain rather opaque to most consumers as well.

Third, a direct relationship between the child and company is created. Internet-enabled toys facilitate an – almost – continuous online connection between the child and the company. Whenever the child presses the 'on' button, the smart toy connects to the internet and, consequently, also to the company (or any other party to whom operational activities have been outsourced). This section will set out who these actors potentially are and what their role might be.

The most important actors are the companies developing, offering and operating smart toys to consumers. By determining the functionalities of the smart product they greatly influence how children play with them. These companies constantly need to come up with novel and – nowadays – more interactive toys that chime with the digital environments and experiences of children. Smart toys can thus potentially gather a lot of data about children. Children themselves – knowingly or unknowingly – impart data by signing up for an account with the company, by interacting with the toy, and by installing any other software – e.g. an app – that is necessary to properly use the toy. Smart toys can be fun, entertaining and instructive to children, but those things are incidental to the end of realising revenues by the companies. The objective of companies is first and foremost to make increasing profits. Both the development of new products as well as finding ways to collect and monetise personal data – or even better, a combination of these business models – further these aims.

The relationship between company and consumer may also become less straightforward if more than one company – or even a network of curators – is involved in developing smart toys and making them operational. Take Hello Barbie as an example.

Barbie is a brand owned by Mattel, a company which sells a wide range of Barbie dolls, play-sets and accessories, as well as the WiFi-enabled Hello Barbie. The interactive experience of the Hello Barbie doll is, however, provided by ToyTalk, a company that develops speech recognition technology. ToyTalk also stores recorded conversations between the child and the doll on their cloud servers and analyses these data to improve user experience.[6] Mattel, furthermore, engages service providers to help them operate and improve Hello Barbie. What is unclear is who exactly these service providers are and whether they include other parties besides ToyTalk (although their FAQs imply that they do).[7] In order to set up the doll, a smart device is required and software (from ToyTalk) needs to be downloaded in the Apple App Store, Google Play Store or Amazon App Store. On top of that, a WiFi-connection via an internet service provider is needed to take advantage of the full features of the doll.[8]

In addition, parents must get involved because they have to set up an account and give permission to activate the interactive features of the doll. Through their parental account, they can listen to and delete their children's conversations with the doll.[9]

Given the smart design of the doll, it must comply with privacy and security laws (see also next section), which may require the involvement of other third parties. Hello Barbie was certified by the kidSAFE Seal Program as being compliant with US law. The programme has been approved as a COPPA Safe Harbor Program[10] by the Federal Trade Commission, which is a US federal regulatory consumer protection and competition agency.

In other (particularly EU) countries, data protection authorities can have a role in ensuring the privacy and security of smart toys. Potentially, the interaction with Hello Barbie can also lead to the involvement of law enforcement, if a review of the child's conversation with the doll raises concerns about the child's or anyone else's safety.[11]

### 5.1. Trust on the curation level: some challenges

As a consequence of this network of curators, it becomes clear that the whole idea of ownership is changing. Although the smart doll becomes one's property and the user – in the case of the child – develops a personal and intimate relation with it, the doll never completely becomes one's own. Because of its networked character, the smart doll persists in the sphere of influence of the different curators, creating a so-called *hybrid ownership*. This poses two important challenges to trust.

First, taking into account the new business model underpinning smart toy companies, it becomes clear that the interests of the curators involved do not necessarily align with those of the end users. Where the latter want to have a fun experience playing with the smart doll, the former are mostly interested in monetising the data. Conflicting interests may have a negative impact on trust, as they hinder the trustor – the end user – to have positive expectations of the actions of the trustee – the company.

Second, hybrid ownership does not entail that each and every curator 'owns' the smart doll in similar ways. Whereas the company behind the smart doll can adapt the core

settings of the device through updates or change data flows, the control of end users is limited to what is allowed by the smart doll company. Or, to borrow a term from STS, the 'interpretative flexibility' – the room one has to tweak and adapt a device – is greater in the relation between the curator and the smart doll than in the relation between the consumer and the smart doll. This difference in control may result in trust issues when parents and children are confronted with changes carried through by the company that they dislike or even disagree with.

## 6. Construction

When we look at trust at the construction level – thus focusing on the technical aspects of the doll – we immediately encounter a crucial difference between the old-fashioned analogue doll and the smart doll. Safe use of the former focuses first and foremost on *physical* safety. Toys should, amongst other things, be free of small or removable parts, not have sharp edges and be free of toxic materials such as lead-based paint (Schmidt 2008; Taylor, Morris, and Rogers 1997). While these safety requirements obviously remain valid for smart toys, they are no longer sufficient given the new vulnerabilities that come with the data-driven nature of the smart doll.

Moreover, in trying to assess the safety of the data-driven nature of these dolls, we encounter the problem that smart dolls are powered by *proprietary systems*. Mattel and ToyTalk are not keen on issuing detailed technical and/or security information on their smart toys. As a consequence, these devices become so-called *black boxes*, inherently hard to scrutinise (Pasquale 2015).

Notwithstanding the difficulty of mapping information flows and security measures in smart toys, some information has recently become available through the work of independent white hat hackers who unofficially test the devices and warn of safety and security issues (Chaudron et al. 2017, 8). Although it is an essential legal requirement to ensure sufficient levels of security when processing personal data,[12] these hackers found that *device security* can be compromised on three different levels. First, the doll can be hacked and used as a surveillance device. Second, the doll can be hijacked to behave badly or erratically. Finally, the doll can be used to track the geo-location of children (Chaudron et al. 2017, 9; Holloway and Green 2016, 2). Notwithstanding these reported vulnerabilities, no malicious attacks involving smart toys have yet been reported.

The problem of device security stems from the fact that the microchips and sensors in connected toys 'are often cheaply made or manufactured without much apparent quality control' (Forbrukerrådet 2016, 34-35). In addition, another security study ordered by the Norwegian Consumer Council underlines that as Hello Barbie is Wi-Fi-enabled, she is in theory vulnerable to attacks from anywhere in the world. By comparison, other toys, such as smart doll Cayla, pair to a tablet or phone via Bluetooth. As a result, they can only be hacked when the hacker is in the close vicinity of the doll. However, when an attacker is able to reside in close range of the device, it becomes relatively easy to connect to it through Bluetooth (Bouvet 2016, 15). All in all, the connectedness, which is key to the optimal functioning of the smart doll, is in turn its weak spot from a security perspective.

Moreover, it is important to understand how the construction of the smart doll steers the interaction with the child and shapes its action space. The report of the Norwegian

Consumer Council indicates that smart toys are programmed in such a way that they confirm certain sexism biases. For example, Hello Barbie is much more interested in talking about clothes and toys, whereas the smart robot i-Que (targeting boys) 'steers the "conversation" towards science, lasers and silly jokes' (Forbrukerrådet 2016, 35). Gender stereotyping is worrisome because of its potentially negative impact on the social and cognitive development of children, given that 'if children choose or are offered almost exclusively gender-specific toys, they may only be able to build skills and competencies associated with such toys' (Weisgram, Fulcher, and Dinella 2014, 401). Moreover, in their technical tests the Norwegian Consumer Council found that the Norwegian version of apps accompanying the smart toys Cayla and i-Que blacklisted certain words and concepts, such as 'homosexual', 'bisexual', 'lesbian', 'LGBT' and 'atheism' (idem). They also uncovered a blacklist of crude words and concepts, which are deemed to be controversial, such as: 'menstruation', 'scientology member' and 'violence' (idem). All in all, these findings illustrate that certain norms and values are built into the technical design, guiding the interaction with the child. However, such values and norms by design are not apparent from looking at the toy; e.g. whereas a doll still looks like a girl's toy, gender bias may run much deeper now the child is able to talk to the doll and have conversations which further reinforce gender stereotypes. Such manipulation by the toys can have an impact on the trust relation with the end user.

### *6.1. Trust on the construction level: some challenges*

Due to their connectedness and data-driven nature, smart toys impose new vulnerabilities onto children and their parents. While it has always been part of the consumer-manufacturer relation that the former had to trust the latter to deliver safe products, adhering to the requirements set in relevant legal provisions on toy safety,[13] now the additional matter of device security, covering issues such as data integrity and the security of chips and sensors, is added to the equation. Consumers expect companies to take the necessary measures to ensure a safe and secure interaction with the purchased smart toys.

However, trust in the construction of smart toys is challenged in four ways. First, due to the fact that most smart dolls function as *black boxes*, hiding their proprietary data-driven systems from public scrutiny, it is unclear what is actually at stake for children and their parents (also see Pasquale 2015). As there are many possible points of access to the device or to the data collected through the device – from servers to Bluetooth connection – trust is actually distributed over a whole network of actors and is therefore much more complex than users are generally aware. Although trust is always blind to a certain extent – otherwise it would be redundant – it may be too blind on the construction level.

Second, what is secure now might not be so tomorrow. One of the challenges for IoT devices is that they constantly need to be updated and monitored to remain safe in the cybersecurity arms race. End users, therefore, not only need to trust companies to sell them safe products, they also have to trust them to keep these products safe throughout their complete life cycle.

Third, especially on occasions when risks materialise and end users are harmed, it becomes apparent whether or not trust was rightfully given. These moments of reflection are valuable, as they encourage people to rethink the trust they vested in others and, if needed, adapt their behaviour. However, it has to be noted that when end users are

confronted with a hacked smart toy, they might also face a problem of attribution. As is typical of cyber-related attacks, it often remains unclear who the attackers are, what their motives behind the attack were, and what the actual nature of the attack is (Singer and Friedman 2014). This uncertainty inherent in cybersecurity issues makes it hard for end users to determine if a smart toy has been compromised in order to gain access to personal information, to undermine the system of the company behind the smart toy, or to hinder users' handling of the toy. This attribution problem will only add to the decline of trust in smart toys and the companies behind them. While hijacking a smart doll and making it act erratically is definitely something which will make users explicitly question their trust in the doll, other forms of hacking may, however, be much more covert, leaving the trust relation inadvertently intact. For example, hacking a doll in order to harvest data or track a child will generally happen beyond the awareness of children and their parents. The absence of a feedback loop prevents users from being probed to evaluate their trust, where otherwise they might have been, had the damage they suffered been more evident.

Finally, in addition to the challenges of device security for trust, the way in which the doll is *programmed* also brings uncertainty. The ethical choices concerning topics that are deemed relevant and appropriate for the smart doll to address may have an impact on children's development. Therefore, parents have to trust the companies to make responsible decisions on this matter, as it is too cumbersome and complex to check all possible conversation interactions before handing over the doll to the child. Moreover, parents must trust companies not to manipulate children in ways that reinforce certain prejudices and curtail freedom of information.

## 7. Codification

Adequate legal frameworks are essential from a trust perspective. Both from a data protection and children's rights perspective, we can point to various issues that may undermine trust. The problem is not always that laws are not in place, but rather that currently they do not provide adequate protection – by definition or because of a lack of implementation or enforcement (see e.g. Forbrukerrådet 2016). This section will not provide a full-blown legal analysis of smart toys but will address some pertinent issues and opportunities.

As a result of the direct relationship between child and company, companies can *collect* – potentially very sensitive – *personal information* from children in ways that were impossible before the advent of networked technologies and smart toys. Protection of children's personal data is a crucial underlying legal interest in the General Data Protection Regulation, which entered into force on 25 May 2018 (see Recital 38).[14] Such protection is amongst other things intended to be achieved by providing parents with control over their children's personal data (or to be more precise by requiring them to consent to the processing of such data) (article 8, GDPR). Given the complexity of smart toys in terms of construction and curation, and the lack of meaningful choice in protection through parental control, it is essentially an illusion (Schermer, Custers, and van der Hof 2014; van der Hof 2017). Parents generally do not read privacy policies nor would they gain a meaningful understanding of what happens to their child's data if they did, given that the terms formulating data practices are often vague. Besides, free choice is illusory; choice only exists between using or not using the smart toy or its full array of functionalities (also see section 6 on hybrid ownership).[15]

Spaces to escape from parental surveillance can be part and parcel of children's perceptions of privacy, often even well before they become teens (Shmueli and Blecher-Prigat 2011). Children's rights to privacy (article 16, UN CRC) and play (article 31, UN CRC) go hand in hand, and require children to have intimate safe spaces free from – corporate or parental – surveillance in order to encourage and respect their right to optimal development (article 6 UN CRC) – yet another fundamental right of the child. However, in the case of for instance Hello Barbie, all conversations with the doll are stored by and made available to ToyTalk as well as to parents through a dedicated parental account.

### *7.1. Trust on the codification level: some challenges*

Inadequate legal protection raises uncertainty as children and parents cannot be sure that certain privacy and security risks are being mitigated on their behalf. Specifically, it exacerbates trust issues given the potentially sensitive information that is involved in playing with toys that interactively question a child in the privacy of their room, as well as possible security breaches that may occur with respect to data.

Moreover, the important role that has been assigned by the GDPR to the consent of parents and the control parents have – to a certain extent – over the data of their children may burden the trust between children and parents. Children have to trust their parents to make well-informed decisions on the processing of their data. However, as has been repeatedly argued in this paper, due to the complexity of both the construction and the terms and conditions accompanying smart toys, it is highly unlikely that parents fully grasp what they are actually consenting to.

Furthermore, children have a perception of privacy vis-à-vis their parents. Giving parents the ability to check their children's conversations with smart toys, potentially even behind their backs, raises new trust issues in their relationship. Knowing that their parents have full access to interactions with smart toys can have a chilling effect on children's playful activities. Some instruments – if implemented well – may, however, be able to encourage trust and mitigate some of the aforementioned legal inadequacies. First, the principles of privacy by design[16] and privacy by default[17], as recognised by the GDPR, can restore some of the power imbalance and surveillance issues between children and parents on the one hand and the array of commercial parties involved on the other (van der Hof and Lievens 2018, 35-38). Equipping smart toys with strong anonymization and data minimisation serves both the protection of children and their rights as well as supporting the security of the product, given that no personal data or merely data that is relevant to the use of the toy is processed by the company and only as long as that data is necessary.

Second, according to the UN Committee on the Rights of the Child, the children's rights framework requires an impact assessment with respect to any implementation of law and policy that has an impact on children.[18] In essence, this entails continuous monitoring of the interests and rights of children in relation to the protection of children against corporate and other forms of surveillance under the GDPR, potentially also as part of data protection impact assessments (van der Hof and Lievens 2018, 38-40).

Besides other rights already mentioned, most notable is the right of children to be protected from economic exploitation (see article 32 UN CRC). State parties in particular have an obligation to ascertain whether actions by the private sector are in the best interest of the child (and hence are in line with the rights of children and other protective legal

provisions). Moreover, such an assessment requires states to evaluate to what extent the legal protections in place are adequate and effective.

## 8. Conclusion

In this paper, we have analysed the way in which the use of smart dolls impacts trust. As smart toys are networked devices, bringing together a heterogenic web of actors and interests, we took a layered approach and examined trust on four levels: context, curation, construction and codification.

On the context level, we found that the trust of users in smart dolls is largely based on their first-hand experience. What happens behind the interface – data collecting and sharing, personalisation – often remains out of sight. As a result, trust vested in the smart doll often does not cover these actions; notwithstanding they do render the child and its parents vulnerable.

One of the challenges when it comes to trust in smart toys is that their 'identity' does not necessarily remain the same throughout their whole life cycle. Through machine learning and data analysis, their performance may evolve. This implies that trust in the smart doll should be approached as an *iterative process* rather than a one-time-only decision. Parents and children should on a regular basis confront their positive expectations of the doll with the actual functioning of the doll. As it is not to be expected that parents and children will do this proactively, this might require changes in the construction and codification of the smart doll. One could think of adding a warning signal to the design of the doll that notifies the user when a new stage of smartness is about to arrive, and to force companies to provide clear information on any new processing of personal information as well as to renew consent if necessary (although the latter strategy may have a negative effect on the trust relation between children and parents).

On the curation level we found that the networked character of the smart doll allows for a new form of hybrid ownership. As smart dolls remain under the control of the manufacturers, a shift in power occurs. Whereas with traditional dolls, after purchase the toy becomes truly one's own, with the smart version the doll remains under the control of the company. Children and parents have to trust the companies connected to the doll to act responsibly and to take their interests into account when for example updating the system or changing the settings.

That children and parents are vulnerable and dependent on the actions of the producers of the smart doll becomes conspicuously clear when looking at the construction level. As smart dolls are based on proprietary systems, companies are reluctant to share information on their functioning and security. In practice, smart dolls are black boxes and end-users simply have to trust that proper measures have been set in place to protect them.

One way of dealing with these new uncertainties is by installing and enforcing an adequate legal framework. Such a framework can ensure that companies and manufacturers perform in a predictable and trustworthy way. However, analysing trust on the codification level, we found that although the protection of children's personal data is covered by the GDPR, this is not sufficient and actually may exacerbate trust issues, particularly in the relation between children and their parents. The key role assigned to parental consent may have as an unintended consequence that children circumvent asking their parents for permission. Having a perception of privacy vis-à-vis their parents, children may find

themselves in the position that they need to breach the trust of their parents in order to make use of smart toys and online services they deem highly important to their social life.

Our analysis of trust and smart dolls shows that trust challenges are closely linked to the potential commercial, technical and legal issues arising from the smart and networked character of these dolls. As most of these issues are currently tucked away behind the interface, eluding the attention of parents and children, companies do not have a strong incentive to address them. However, we foresee that with the further growth of an Internet of Toys, the exposure of vulnerabilities will increase and so will awareness. An advancing political and legal interest in informational privacy and cybersecurity must lead to more stringent regulation and enforcement, which will require the hidden actors behind the interface to be more transparent about the processes in which they engage. Without transparency, sooner or later trust will evaporate.

## Notes

1. See http://www.ubooly.com/ and https://www.vtechkids.com/product/advanced_search/ft_keyword:cora_cody±ft_gender:both
2. See e.g. https://www.vtechkids.com/brands/brand_view/smartwatch
3. See e.g. https://www.cnet.com/news/hello-headaches-barbie-of-the-internet-age-has-even-more-security-flaws/.
4. See https://www.amazon.com/Barbie-DKF74-Hello-Doll/product-reviews/B012BIBAA2; accessed: 20 March 2018.
5. However, the principles of privacy by design and privacy by default entail that such transparency becomes a part of smart toys and that privacy-friendly settings become the default, particularly with respect to children, see Article 25, GDPR; see also van der Hof (2017).
6. Hello Barbie FAQ, Version 2, Mattel, 2015, http://hellobarbiefaq.mattel.com/faq/.
7. Ibid.
8. Ibid.
9. Hello Barbie FAQ, Version 2, Mattel, 2015, http://hellobarbiefaq.mattel.com/faq/.
10. See for more information: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Safe%20Harbor%20Programs.
11. Hello Barbie FAQ, Version 2, Mattel, 2015, http://hellobarbiefaq.mattel.com/faq/.
12. See articles 5(f) and 32 GDPR; see also recitals 39, 81 and 94. See also article 16 (2), UN CRC. Also see section 8 for a more detailed analysis of legal aspects.
13. See, for instance, Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys, OJ L 170, 30.6.2009, p. 1–37.
14. 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, OJ EU L119/1, 4.5.2016.
15. Note, however, that such a situation does not seem to be in line with the requirement under the GDPR that consent must be freely given, see Recital 42 and Article 4 (11) jo. Article 7 (4).
16. See article 25 (1), GDPR.
17. See article 25 (2), GDPR.
18. General Comment No. 14 on the right of the child to have his or her best interests taken as a primary consideration, CRC/C/GC/14, http://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf (last visited 18 September 2017).

## Disclosure statement

No potential conflict of interest was reported by the authors.

## Notes on contributors

***Esther Keymolen*** is assistant professor of Philosophy of Technology at Tilburg University (TILT). Her research and teaching is interdisciplinary in nature and focuses on: technology and trust as regulatory strategies (1), philosophical and ethical implications of the use of digital technologies (2), privacy (3), and the development and role of the iGovernment (4).

***Simone van der Hof*** is professor of Law and Digital Technologies and Director of eLaw – the Centre for Law and Digital Technologies, at Leiden University. Common thread in her research and education is the influence of technology on the rights of individuals in various capacities (eg citizen, child, patient and consumer) and the interaction between legal, technical and social regulation in safeguarding and strengthening their position.

## ORCID

*Esther Keymolen* http://orcid.org/0000-0002-1578-0789

## References

Allen, M. 2004. "Tangible Interfaces in Smart Toys." In *Toys, Games, and Media*, edited by J. Goldstein, D. Buckingham, and G. Brougere, 179–194. Mahwah, NJ: Lawrence Erlbaum Associates.

Baier, A. 1986. "Trust and Antitrust." *Ethics* 96 (2): 231–260. http://www.jstor.org/stable/2381376.

Bouvet. 2016. *Investigation of Privacy and Security Issues with Smart Toys*.

Chaudron, S., R. Di Gioia, M. Gemo, D. Holloway, J. Marsh, G. Mascheroni, J. Peter, and D. Yamada-Rice. 2017. *Kaleidoscope on the Internet of Toys*. Luxembourg: P. O. o. t. E. Union.

Davis, F. D. 1985. *A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results*. Cambridge, MA: Massachusetts Institute of Technology.

Davis, F. D. 1993. "User Acceptance of Information Technology: System Characteristics, User Perceptions and Behavioral Impacts." *International Journal of Man-Machine Studies* 38 (3): 475–487.

Floridi, L. 2015. "Hyperhistory and the Philosophy of Information Policies." In *The Onlife Manifesto. Being Human in a Hyperconnected Era*, edited by L. Floridi, 51–64. Cham: Springer.

Forbrukerrådet. 2016. *Toyfail. An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys*. https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf.

Gibbs, S. 2015. "Privacy Fears Over 'Smart' Barbie that can Listen to Your Kids." *The Guardian*, March 13, 2015. https://www.theguardian.com/technology/2015/mar/13/smart-barbie-that-can-listen-to-your-kids-privacy-fears-mattel.

Giddens, A. 1990. *The Consequences of Modernity*. Cambridge: Polity Press in association with Basil Blackwell, Oxford.

Giddens, A. 1991. *Modernity and Self-Identity, Self and Society in the Late Modern Age*. Stanford: Stanford University Press.

Harris, P. L. 2012. *Trusting What You're Told. How Children Learn from Others*. Cambridge, Massachusetts: Belknap Press of Harvard University Press.

Holloway, D., and L. Green. 2016. "The internet of toys." *Communication Research and Practice*. Accessed April 26, 2018. https://www.researchgate.net/publication/311771309_The_Internet_of_toys.

Ihde, D. 1990. *Technology and the Lifeworld: From Garden to Earth*. Bloomington: Indiana University Press.

Kahneman, D. 2011. *Thinking Fast and Slow*. New York: Farrar, Straus and Giroux.

Keymolen, E. 2016. *Trust on the Line. A Philosophical Exploration of Trust in the Networked Era*. Amsterdam: Wolf Legal Publisher.

Kiran, A. H., and P.-P. Verbeek. 2010. "Trusting Our Selves to Technology." *Knowledge, Technology and Policy* 23 (3-4): 409–427.

Kopetz, H. 2011. *Real-Time Systems. Design Principles for Distributed Embedded Applications*. New York: Springer.

Leenes, R. E. 2011. "Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology." *Legisprudence* 5 (2): 143–169.

Lessig, L. 2006. *Code: Version 2.0*. New York: Basic Books.
Luhmann, N. 1979. *Trust and Power. Two Works by Niklas Luhmann*. Translated by H. Davis. New York: John Wiley & Sons Ltd.
Luhmann, N. 1988. "Familiarity, Confidence, Trust: Problems and Alternatives." In *Trust: Making and Breaking Cooperative Relations*, edited by D. Gambetta, 94–107. Oxford: Blackwell.
Mayer-Schönberger, V., and K. Cukier. 2013. *Big Data: A Revolution that Will Transform How We Live, Work, and Think*. Boston: Houghton Mifflin Harcourt.
McKnight, D. H., and N. L. Chervany. 2002. "What Trust Means in e-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology." *International Journal of Electronic Commerce* 6: 35–60.
McKnight, D. H., V. Choudhury, and C. Kacmar. 2002. "The Impact of Initial Consumer Trust on Intentions to Transact with a web Site: A Trust Building Model." *The Journal of Strategic Information Systems* 11 (3): 297–323.
McReynolds, E., S. Hubbard, T. Lau, A. Saraf, M. Cakmak, and F. Roesner. 2017. "*Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys*." Proceedings of the 2017 CHI Conference on human Factors in computing systems.
Möllering, G. 2006. *Trust: Reason, Routine, Reflexivity*. Amsterdam: Elsevier.
Pasquale, F. 2015. *The Blackbox Society. The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.
Pitt, J. C. 2010. "It's not about Technology." *Knowledge, Technology and Policy* 23: 445–454.
Schermer, B. W., B. Custers, and S. van der Hof. 2014. "The Crisis of Consent: How Stronger Legal Protection may Lead to Weaker Consent in Data Protection." *Ethics and Information Technology* 16 (2): 171–182.
Schmidt, C. W. 2008. "Face to Face with Toy Safety: Understanding an Unexpected Threat." *Environmental Health Perspectives* 116 (2): A70–A76.
Shmueli, B., and A. Blecher-Prigat. 2011. "Privacy for Children." *Columbia Human Rights Law Review* 42: 759–795.
Simon, J. 2013. "Trust." In *Oxford Bibliographies in Philosophy*, edited by D. Pritchard. New York: Oxford University Press.
Simpson, T. W. 2012. "What is Trust?" *Pacific Philosophical Quarterly* 93: 550–569.
Singer, P. W., and A. Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.
Swierstra, T., and K. Waelbers. 2012. "Designing a Good Life: A Matrix for the Technological Mediation of Morality." *Science and Engineering Ethics* 18 (1): 157–172.
Taylor, S. I., V. G. Morris, and C. S. Rogers. 1997. "Toy Safety and Selection." *Early Childhood Education Journal* 24 (4): 235–238.
Thaler, R. H., and C. R. Sunstein. 2008. *Nudge: Improving Health, Wealth, and Happiness*. New Haven: Yale University Press.
Thurman, N., and S. Schifferes. 2012. "The Future of Personalization at News Websites: Lessons From a Longitudinal Study." *Journalism Studies* 13 (5-6): 775–790.
van den Berg, B. 2009. "*The Situated Self*." Doctoral dissertation, Erasmus University, Rotterdam.
van den Berg, B., and E. Keymolen. 2017. "Regulating Security on the Internet: Control Versus Trust." *International Review of Law, Computers & Technology* 31 (2): 188–205.
van der Hof, S. 2017. "I Agree or Do I? – A Rights-Based Analysis of the Law on Children's Consent in the Digital World." *Wisconsin International Law Journal* 34: 409–445.
van der Hof, S., and E. Lievens. 2018. "The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR." *Communications Law* 23 (1): 33–43.
Venkatesh, V., and F. D. Davis. 2000. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies." *Management Science* 46 (2): 186–204.
Verbeek, P.-P. 2009. "Moralizing Technology: On the Morality of Technological Artifacts and Their Design." In *Readings in the Philosophy of Technology*, 2nd ed., edited by D. M. Kaplan, 226–249. Lanham: Rowman and Littlefield.
Verbeek, P.-P. 2010. *What Things Do: Philosophical Reflections on Technology, Agency, and Design*. Pennsylvania: Penn State Press.

Verbeek, P.-P. 2011. *Moralizing Technology: Understanding and Designing the Morality of Things*. Chicago: University of Chicago Press.

Weisgram, E. S., M. Fulcher, and L. M. Dinella. 2014. Pink Gives Girls Permission: Exploring the Roles of Explicit Gender Labels and Gender-Typed Colors on Preschool Children's toy Preferences." *Journal of Applied Developmental Psychology* 35 (5): 401–409.

Yeung, K. 2017. "'Hypernudge': Big Data as a Mode of Regulation by Design." *Information, Communication & Society* 20: 118–136. http://www.tandfonline.com/doi/abs/10.1080/1369118X.2016.1186713.