The internet of toys

Home   About   **On our minds**   From our notes   Around the world   Publications   Resources

Subscribe   🔍

With the rapid expansion in 'smart', interconnected toys, what is being done to regulate, for example, the data they generate? Giovanna Mascheroni looks into some of the hopes and concerns surrounding the internet of toys. Giovanna is a Lecturer in the Department of Sociology, Università Cattolica, Milan and visiting fellow in the Department of Media and Communications at the LSE. She part of the EU Kids Online research team and of the COST Action DigiLitEY. [Header image credit: L. Proppe, CC BY-NC 2.0]

Along with smartphones and tablets, we can assume that Internet of Things (IoT) toys concurred to make last Christmas a digital Christmas. Indeed, the sale of smart, internet-connected toys was already expected to reach US$2.8 billion in 2015. Hatchimals topped the list of searches on Google and were sold out in most retail stores.

As Donell Holloway and Lelia Green pointed out, the Internet of Toys refers to a quite diverse typology of toys, including:

- toys based on voice and/or image recognition (e.g. Hello Barbie™ or the Hatchimals)

- app-enabled robots, drones and other mechanical toys (e.g. Dash and Dot)

- toys-to-life, which connect action figures to video games (e.g. Skylanders or Lego Dimensions)

- puzzle and building games (e.g. Lego Fusion).

New experiences

In opening up new experiences of connected play, these toys provide children with new, embodied ways of being online at a very young age. They also promise educational benefits: from literacy and numeracy skills to digital literacies and coding skills. Further opportunities include collaborative play, creative and rational thinking, and specific knowledge gains such as 3D printing.

However, these toys have also raised concerns about the potential threats to children's data protection, as IoT toys expand the range and quantity of children's everyday life practices that can be tracked, recorded and analysed.

Complaints

Subscribe

While children's play practices and personal information are recorded, datafied and stored in corporate platforms, children and their parents know little about how their personal data is treated, as the #toyfail campaign launched by the Norwegian Consumer Council in November 2016showed. Following their assessment of My Friend Cayla and i-Que, BEUC (a European consumer organisation) filed a report to the European Data Protection Supervisor and the International Consumer Protection and Enforcement Network (ICPEN). US consumer associations and NGOs have filed similar complaints to the US Federal Trade Commission.

The complaints identified a number of serious issues that *compromise children's rights to privacy and personal safety*, including:

- *Lack of personal safety:* for example, the two Genesis Toy products allow unauthorised Bluetooth access from any smartphone or tablet within 50 metres, thus potentially allowing strangers in the immediate surroundings to talk to children.

- *Non-transparent and illegal terms and conditions:* as with many other IoT toys (as already pointed out by media scholars Donell Holloway and Lelia Green in their 2016 article), parents are forced to agree with all the terms of use in order to fully realise the affordances of Cayla and i-Que, for example. In requiring consent to terms and conditions being changed without further notice, and to personal data being shared with third parties and used for targeted marketing, the terms of the service are openly violating the EU Data Protection Directive.

- *Lack of control over access to personal data:* the toys encourage children to disclose their personal information (the name of their parents, home address and school, etc.) which is later shared with Nuance, a software recognition company, and potentially other third parties without parental consent.

- *Hidden advertising:* pre-installed phrases sponsor specific products and media content, thus advertising brands with which Genesis Toy has developed commercial relations, for example.

Privacy

Risks for children's rights to privacy are the most visible and immediate consequences of the *datafication of childhood* by means of IoT toys, education platforms and apps (read about the privacy concerns posed by ClassDojo on this blog), and other IoT devices (including smart assistants such as Amazon Echo).

These technologies also normalise surveillance as a cultural and social practice, in the context of the parent–child relationship or children's relationship with institutional and commercial actors. Children are monitored or encouraged to monitor their own activities (be it health, school performance and/or play practices).

Growing up in a culture where (self-)surveillance is normalised is likely to shape children's future lives in ways that it is hard to predict.

Future research

A group of researchers within the COST Action DigiLityEY is currently looking at the way IoT toys have been incorporated into the play discourses, by examining the media and commercial representations of such toys during the last Christmas season across Europe and Australia. The research will analyse the opportunities and risks of the toys as represented on news media, tech, blogs, mummy bloggers and parenting websites/communities, advertising etc.

However, privacy and safety risks are not the only consequences of the datafication of childhood. Together with (self-)tracking apps of various kinds, IoT toys further concur to normalise surveillance as a cultural and social practice, be it in the context of the parent-child relationship, or children's relationship with institutional and commercial actors. Children are increasingly monitored (by parents, caregivers, educators, and commercial companies) or encouraged to monitor their own activities (be it health, school performance and/or play practices). Growing up in a culture where (self-)surveillance is normalised is likely to shape children's future lives in ways that it is hard to predict.

Subscribe Ⓠ

January 27th, 2017 | Featured, On our minds | 0 Comments