Cybersecurity in Children and Adolescents

David Alonso Santiváñez Antunez
December 2016

Introduction

In December of this year, the 11th IGF, a global meeting organized by the United Nations (UN) and the host Government, was held in Guadalajara, Mexico. It brings together the most influential and hardworking actors for the development of a better digital ecosystem. Each of those present, from attendees to speakers, play a very important role in the development of what I dare call, the new continent - or the eighth continent -, all united under a single idea, that is to generate Internet development policies and a stable and collaborative governance.

This time, thanks to Amazon® and the South School on Internet Governance, we were invited to participate in this important event, with the mission of not understanding the future changes and challenges, but also trying to understand on how to collaborate in this constant evolution.

The DNA of this event is teamwork and networking. All the stakeholders were present, private ones like AMAZON®, international organizations like the UN and the OAS, and civil societies and technical leaders like the Mexican Association of Internet, the South School on Internet Governance, among others.

This report is focused on the aspect of cyber security and children, which I consider being a gray area within the Internet and there is till a lot to explore.

The Internet of Toys

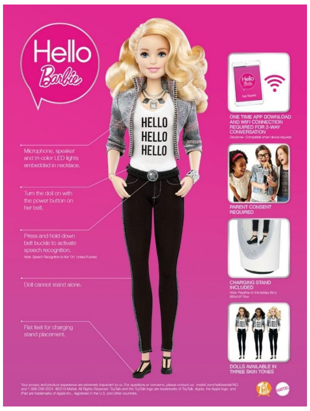
Technology and entertainment seeks to develop more and more products that are linked to the information society; more specifically to children.

It is not strange to start find information about the Internet of Toys, an Internet derivative of things (IoT) that connects children's entertainment with applications and has captured interest in the cyber security sector because of its few security measures. One of the products that encourages this debate is the doll called “My Friend Cayla®” manufactured by Genesis Industries Limited®, the competition of “Hello Barbie®”, the doll that talks from Mattel.

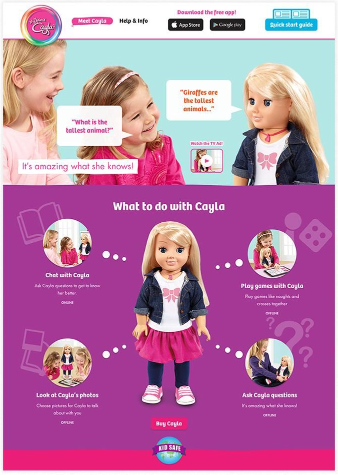
During the development of the IGF, a group of researchers from the major universities in North America, together with the United Nations Children's Fund (UNICEF), developed a web-based workshop on Toys and Internet, where they explained about the dangers of these new dolls which include Internet functionality and other applications. The debate began by wondering if this was the future of toys; for what seems to be not the future but the present, and that dolls like Barbie® or Cayla® should not be considered the first of its kind.

II

During the first minutes of the workshop it was made clear that there was nothing against the companies, but the concern was about the safety of minors. They pointed out that products such as these violated the Privacy Act of the United States, but they also did not perceive a greater responsibility with Internet-connected toys or toys online. Hello Barbie® may pose no danger beyond consumerism and fashion - emphasizing one of the inexhaustible jokes that were enjoyed at the meeting - but it is a new door on the subject of digital insecurity. In other words, computer insecurity specialists could access a lot of personal information about the children.


Hello Barbie
HELLO HELLO HELLO
Microphone, speaker and tri-color LED lights embedded in necklace.
Turn the doll on with the power button on her belt.
Press and hold down belt buckle to activate speech recognition.
Note: Speech Recognition Is Not 'On' Unless Pushed.
Doll cannot stand alone.
Flat feet for charging stand placement.
Hello Barbie
Get Started
ONE TIME APP DOWNLOAD AND WIFI CONNECTION REQUIRED FOR 2-WAY CONVERSATION
Disclaimer: Compatible smart device required.
PARENT CONSENT REQUIRED
CHARGING STAND INCLUDED
Note: Playtime on the battery life is about an hour.
DOLLS AVAILABLE IN THREE SKIN TONES
Your privacy and product experience are extremely important to us. For questions or concerns, please contact us: mattel.com/hellobarbieFAQ and 1-888-256-0224 ©2015 Mattel. All Rights Reserved. ToyTalk and the ToyTalk logo are trademarks of ToyTalk. Apple, the Apple logo, and iPad are trademarks of Apple Inc., registered in the U.S. and other countries.
ToyTalk
MATTEL

Hello Barbie®
Source: http://hellobarbiefaq.mattel.com/about-hello-barbie/



Ask Cayla questions to get to know her better.

Play games like noughts and crosses together

Choose pictures for Cayla to talk about with you

It's amazing what she knows!

My Friend Cayla®
Source: http://hellobarbiefaq.mattel.com/about-hello-barbie/

How does a doll like Hello Barbie® work and why it may be so dangerous? The wrist has the ability to talk with the children, so everything the infants says is sent to a server of the company and analyzed by voice recognition, so the doll can give the appropriate answers. Although in theory this sounds harmless, the company Bluebox has discovered certain security holes which motivated the discussion in the workshop. First, applications for IOS and Android, used for the connection with the wrist, always use the same keyword; second, the wrist is susceptible to being attacked with the Poodle exploit, a man-in-the-middle attack that helps make the wrist program weaker and easier to modify and receive an attack. This doll connects to any WiFi system, malicious programs may have access to information without consent.

The discussion remains in question in the United States. As concluded in the workshop, the intervention of the Federal Trade Commission (FTC) for this new type of doll is not ruled out, especially when there is already a case of attack on this type of product. The victim, the maker of educational games VTech, was hacked loosing information about birth dates, names and other data of more than six (6) million children.

III

Another issue that was discussed in the search for child protection was child abuse on the Internet in a workshop led by WeProtect, a global multistakeholder alliance that seeks to end the sexual exploitation of children online. The organization works on leading international practices; promotes global and regional partnership, integration and collaboration as ways to end child sexual exploitation online. It works in a way which respects and promotes the United Nations (UN) sustainable development goals and international and regional legal instruments aimed at ending sexual violence against children.

The workshop brought together representatives of WeProtect, Microsoft® and civil society organizations. Since 2014 WeProtect fights against the global crime, to eliminate the sexual material in Internet and to strengthen the global cooperation to trace and to catch predators. WeProtect is the only global alliance that takes a multistakeholder approach to this problem and is the central element in the implementation of the sustainable development objective. More than 70 countries, 20 companies and 17 international organizations are working with them.

There were three projects highlighted at the workshop. First, the National Center for Missing & Exploited Children® (NCMEC®), a non-profit organization whose mission since 1984 is to help find missing children, reduce the sexual exploitation of children and prevent child victimization. It received a record 4.4 million cyber reports in 2016 on child sexual exploitation material worldwide. Unfortunately it far exceeded the 1.1 million reports they received in 2014.

Fuente: www.weprotect.org

Fuente: www.missingkids.com

Fuente: www.iwf.org.uk

Secondly, Microsoft® spoke of the famous Microsoft's PhotoDNA which consist of a free Cloud Service that helps identify and eliminate photos with child sexual content. Since its inception in 2009, Microsoft's® PhotoDNA has been helping solve problems where NCMEC® had gained experience:

The last speaker was the Internet Watch Foundation (IWF), an organization focused on minimizing the availability of online sexual abuse content, specifically child pornography content hosted anywhere in the world, seeking the goal to make the Internet a safer place. In 2015, they contributed with the deletion of 68,000 web pages. Eighty percent of the victims detected were girls, and 69% were children under the age of 10.

IV

The UNICEF panel, UNICEF INNOCENT PANEL, was a very well attended workshop, along with the Internet of Things and Toys. It became clear that the relationship between children and the Internet has become an international trend, especially with the increase in the use of mobile phones, focusing on issues like cyberbulling and cyberstalking. It was of relevance the importance of finding ways to get children's to know about internet challenges and try to make them participants of the IGF. This goes hand in hand with the idea that Göran Marby pointed out at the beginning of the IGF, an idea that pleased the audience and made it clear that multistakeholder models should be more active with the community, but that their work should start from the bottom, forming generations of new leaders in Internet Governance.

Göran Marby is the current CEO and President of the Internet Corporation for Assigned Names and Numbers (ICANN), a multi-stakeholder global organization. Göran Marby longs for society to understand the power of the Internet and for each of the topics that are developed in it, so that future discussions have users as major participants, also aligning their commitment to its development.

What Göran Marby expressed at the opening was a focus on children and their increasing participation in these meetings. It is important to remember that the IGF began with young people, who were concerned about a better Internet, and the adult sector was coupled with the movement with experience and leadership, but little by little the youth sector, which is full of adrenaline and knowledge, went away.

The idea was materialized with the participation of the Hong Kong delegation. Children aged 12 to 15 were at all meetings focused on child protection, debating with members of UNICEF and other organizations, making increasingly complex questions one after another, avoiding repeating them, and demonstrating what Göran Marby released as a new requirement for the next IGF. No one knows better what a child needs but a child himself; nobody will know better their problems, their needs, their approaches and their wisdom if thay do not participate, if we do not listen, if we do not let them work with us for a better environment, because we are facing a divided generation, a generation that in a couple of years will control the Internet.

Conclusion

The purpose of this report was not only to gather information from meetings relevant to the protection of children on the Internet, but to learn more about the work of different organizations.

I can not fail to highlight each one of the works exposed and developed in each one of the workshops. Cyber-security of children and adolescents is a complex and gray field. I did not hear a single moment talking about preventive cyber security, a concept that is based on patterns followed by citizen. It is effective to combat these cyber criminals; but it is much more effective to prevent the problem and to give strategies that are not only based on the dependence of the technologies for a committed, beneficial or malicious. Criminals who have been sanctioned for committing child abuse have used social engineering before the Internet existed, except that the latter made their work more relaxed.

On the other hand, the participation of the children from the Hong Kong delegation continues to be admirable, as they demonstrated the concern of that generation which demands protection and does not want to continue in a gray present. However, I still consider that preventive work with parents, teachers and students can be one of the many keys we will have to improve cyber security in children and adolescents. I know that relying on technology has become a trend, but it should be a complement to this type of work before being the only tool.

I do not have the absolute answer and I am not the owner of the truth, but I want to contribute with what I consider correct for the sake of our digital community. Let us take our part. We are still on time to work in the cyber security of children. We are still on time to make a more equitable and developed Internet. We are still on time to change our reality.