IGF 2106 DC COS	05-09 December 2016	Guadalajara, Mexico	Report submitted by Marie-laure Lemineur, ECPAT International 23 December 2016 on behalf of the DC COS. V1.
Speakers and moderators	• Mr. John Carr - Expert Adviser to the European NGO Alliance for Child Safety Online. Writes and consults about Internet safety and security. • Mr. Maarten Botterman - Chair of the Dynamic Coalition on Internet of Things • Ms. Sonia Livingstone - Full Professor in the Department of Media and Communications at London School of Economics • Ms. Jutta Croll - Managing Director, German Centre for Child Protection on the Internet • Ms. Arda Gerkens - Member of the Dutch Senate and Director of the Dutch "Meldpunt kinderporno" (hotline for child pornography) • Moderator: Ms. Marie-laure Lemineur, ECPAT International		
Session title: THE INTERNET OF THINGS AND THE RIGHTS OF THE CHILD Thursday 8 December 2016 10:15 am - 11:45 am (Workshop Room 8)	The session addressed the linkages between the Internet of Things (IoT) and the rights of the children. The Internet of Things is defined as "a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction." (1) Millions of users all over the world, from all age ranges are provided with the opportunity to be connected to the Internet through objects. This happens not only via cars, watches and fridges but it also concerns the toy industry in a major way (2) as well as the manufacturers of others goods that may be widely used by children. Additionally, there are devices like cameras embodied in other objects used by children of all ages or in close proximity to them. This evolution entails societal and economic challenges, and triggers questions around privacy and data collection among others. "…With multifunctional devices, going online does not need to be a conscious decision….". (3) There is an obvious need to look at the implications of this, specifically with regards to children as recipients/users of these connected objects or as recipients/ users who will or may habitually be in close proximity to connected devices. It has been conducted as a Q&A session. After 5 minutes introductory remarks by each speaker, the following questions were asked to the presenters: A-**SECURITY** - It is now a well-known fact that many IoT devices send some or all data in clear text rather than in an encrypted form. And communications in clear text can be observed by other devices or by an attacker. I am thinking of the example of a toy called Teddy the Guardian who transmits the child´s health data to its parents. Any thoughts on the implications that that can have for children as users. B-**PRIVACY** - Data leaks from and between devices: in some cases, devices on the same network or on neighboring networks may be able to observe data from other devices such as the names of the people in the home, the precise geographic location of a home. Once again, hypothetically a predator interested in seeking a house where a child is left alone could easily spot such a house, find out the name of the child and easily go there to try to harm the child. We could envisage a scenario where there is potential service disruption as another security issue, allowing IoT to be deactivated such as		

	alarm systems remotely. SCENARIO 2: In our case, why not imagine a child predator hacking a toy connected to the internet and recording live the image of the child in his room. Which would be the implications for a child as end user in this case? C. **RIGHT TO BE DISCONNECTED** - Parents potentially will use IoT devices to increase the supervision of their children as a mean to ¨better protect them¨ and avoid harm being done to them. Those parents will use features and applications such as geolocations, videos devices inserted in objects, etc. If we think of this from the child perspective, let´s say an post pubescent child, an adolescent, this scenario can raise issues regarding a legitimate claim that this child has the right not to be watched constantly 24/24 hours 7/7 or not to be connected permanently taking into consideration the fact that with IoT being connected will not be a conscious decision. Any thoughts on this? D. **ETHICS AND RIGHTS-ENABLING IoT** - In the child rights activists community how do we define what an ethical IoT would be? Is this vision compatible to what the private sector? E. **AGE DIFERENTIATION**: The age range of children as end users is wide, security and privacy standards might not need to be the same for all age groups? We intuitively assume that the younger the child user is the tougher the security standards need to be. If that were to be the case, would that be manageable from a business perspective technically and form a cost perspective? F. Do you think that the concept of **SAFETY BY DESIGN** offers a reasonable answer to the speed of innovation? G. **MONITORING MECHANISMS** - What kind of mechanisms should be set up to monitor if the industry/IoT Device sector is complying with security and safety standards deployed that are generally agreed upon in the community? H. **ENFORCING STANDARDS** - Which would be the anticipated best mechanism to enforce those standards that are gradually emerging in the business community? Is it advisable to rely on a voluntary enforcement if we look at other experiences with the private sector such as the ISPs and blocking/filtering? END OF QUESTIONS
	Summary of comments/remarks made by presenters and participants: **OPENING REMARKS**: **<u>Maarten Botterman:</u>** IoT is penetrating life at any level. It is already there and is moving at a very fast pace. Since it has a global reach, not one single jurisdiction can control what is happening. Technologies themselves are neither good nor bad. It is all about how we use them. We need technologies for a wide series of purpose and in a dense society we cannot manage without technologies. This is valid both for the developing and the less developed world. There are examples of good practices. We need to develop IoT products, ecosystems and services taking into account ethical considerations from the onset and at all levels; in the development phase, deployment and user phases. Transparency is also important for the commercial sector as well accountability. It is also a joined

	stakeholder responsibility to ensure that there is clear choice for key IoT services. **Sonia Livingstone:** It might not be obvious to all why we should bring the question of child´s rights perspective into this debate about IoT. It first gives us away of thinking more broadly about a child-centered perspective on many of the issues that Maarten raised and others are concerned about the Internet of Things. A child rights framework begins by saying that children are independent right bearers. It gives us a broad focus. There is need to always think in this context of the best interest of the child from a holistic perspective and not a top down perspective. A child rights perspective is related to protection but also to a set of rights around provision and participation. Debates around children and technology often focus on protection issues at the cost of participation issues or other ways in which children benefit. It concerns children from cero to 18. In light of what Maarten said, it is very obvious that IoT, speechless children, also concerns babies. In the Convention on the Rights of the Child, the role of governments, parents and duty bearers is clear. They are also linkages with the broader human rights context. While protection is key, children have their own rights to freedom of expression, privacy, dignity, non-discrimination and so forth. Internet adds a kind of new layer of challenges to a child rights framework and the internet of things crystallizes many of the anxiety that people or struggles that people already have in articulating children's rights in relations to the digital environment. There is the debate around the right to internet access since internet is a crucial means though which children´s rights are enabled and through which children´s rights are infringed. The online world, in a way intensifies all kinds of phenomena we´ve already been struggling with in the offline world. Children gain many kinds of benefits and the harm is intensified. The ways children´s online activities are under the radar of the supervision of the parents and teachers and now companies have unprecedented access to children´s data- Everything they do begins to be tracked which forces us to re-examine considerations related to children´s rights in the digital environment. Another challenge is knowing how many children are online. It is not clear who is a child online. There are many ongoing debates about boundaries, in the general data protection regulation, we see debates about pornography, about strangers who can contact children and so forth. Also debate about age verification and privacy. Finally, the new ways in which bringing child rights and cutting edge internet developments in bringing new kinds of conversations into governance spaces. This issue of IoT illustrates well this point. **John Carr:** The IGF and the real world are two parallel worlds. There are those preaching in the internet governance system for more standards but in the outside world, and I am not sure companies do listen to the things discussed here. In October 2016, a number of internet businesses went offline because of a DDOS attack. It included Twitter and Spotify. No one anticipated such a possibility and certainly not those who created those platforms/systems. They are already millions of devices connected part of the IoT and botnet that can´t be patched. The problem is the lack of foresight on the part of people who make the devices. Some of those devices are and will be toys. There is a special search engine called shodan and it shows anybody who uses it to identify devices connected to the Internet, which have got a username and a password. It enables anybody including hackers to locate devices. And some of these devices are/will be toys. With manufacturers of IoT toys, this is a matter of incompetence and cost cutting. It is good that we

	are talking about ethics. Maybe in 10 years time it will be working. Because of the DDOS attack, the issue of liability becomes much more immediate to manufacturers and distributors. There is a mixture of things to be said about IoT and not all of them are good. With regard to the Internet of Things and toys. Parents want to give their children connected devices. Up to now, toys were not connected to the internet. You can now have toys and baby monitors connected to the network. There has been reports of incidents of those devices hacked where predators were talking dirty to the baby. We also need to consider what the companies will do with the data collected via toys for the purpose of marketing and others and who will analyze it. A consumer union in the Netherland already asked companies to withdraw toys from the shops. The carelessness of the industry is impressive and has a huge potential to do damage. **Jutta Croll:** On the screen you can see the image of Teddy the Guardian, a toy that is connected to the Internet and monitors the child´s hear rate, blood pressure and oxygen rate and its has a little camera inserted. All the data collected is transferred to the cell phone of the parents so that they can monitor their child health and well-being. Of course, parents will use this toy thinking it is in the best interest of their child. But most of them won´t realize the implications of being connected to the Internet. I would not blame the parents for not realizing that the health and geolocation data is going to be used by the company most of the time via a not so secured internet connection. Parents need to learn and to be supported by the industry for that. With devices such as a smart TV I can configure and somehow set my preferences but how do we do the same with Teddy the Guardian? My organization has done some research into the topic of safety by design and we think it would be a solution to address two aspects: 1/since the conception phase, foresee what would be the implications of children using the device in terms of putting their safety at risks and than determine how to address those. 2/Than take a second step, have a very high degree of usability of the device and its interface by setting the configuration. Having a higher degree of usability implies the toys could be better marketed. What would happen if someone accesses the algorithm that has set up the alphanumeric strings? Another aspect is that when children use those devices, it is obvious that we cannot rely on education only to enhance safety. We cannot pretend to educate a baby to be careful when using a toy. We cannot pretend that the parents prevent a child from using such toys because it would deprive them from educational opportunities and benefits. In that sense, industry has a role to play in those cases. They are some initiatives but they need to go a step further. **Arda Gerkens:** In the old days, children were not a target for advertisement as much as nowadays. Youth became a target around the 80s. Data collected from children is gold for companies. The IoT will bring us a world we cannot imagine. It will go extremely fast. How can parents keep up with all those things? Not so long ago, tablets appeared and children could play with them. As a result, sometimes, your credit cards were overcharged. But this is the tip of the iceberg of what is coming to us. We need to realize that the developers are here to develop. New gadgets and new things this is what they are all

	about. They don't think about safety and security even if they should and we want them to do so. I find it troublesome that those developers do not have any sense of what is needed to ensure safety and privacy. Also, the children will be watched 24/7 with all these toys. What does that do to a child? We need to strengthen the right to be disconnected and also discuss the right of the data. We should make sure the children start at 18 year old with a clean sheet. There should be laws indicating what kind of data can be collected from children. One of the challenges is to be sure how old is the child online. The case of the consumer's rights organization on KALA is a good thing. Even if education is important, you cannot educate a baby and it is hard to educate all parents. Hence, we have to be loud and tell parents what is wrong with some toys, tell them not to buy them so that all together we can put pressure on companies or get the toys revoked from the shops. Finally, the IoT should be multi-stakeholder. We need the industry to get engaged and think about privacy and security. Policy makers are also key as well as legislators. There should be more and stricter laws on IoT regarding toys used by children. We cannot say that it is the sole responsibility of the parents and we cannot expect all parents to understand and we cannot put all the blame on them either. There is a responsibility for the legislator. **COMMENTS AND QUESTIONS FROM THE FLOOR:** • There are cases in Brazil where toys have been commercialized without many instructions. But we must bear in mind that the IoT regarding children is not only about baby toys. The use of smart clothing for teenagers, smart basketball, etc. that will also raise issues; • We cannot predict the future so we have to create our future. There have been debates in the last ITU meeting held in Tunis about the ethical challenges that the IoT will bring. Manufacturers and private sector are pushing for small things to be connected to the Internet. IoT is going to create many ethical challenges. Today we need to discuss how we can save the Internet from these machines. But we cannot take it away from the Internet. There is a strong call for securing the Internet but we cannot see the problem in isolation. Some argue it is not the IoT but the Internet of everything. The industry, consumers, regulatory bodies and policy makers must be aware of the implications of IoT and discuss how to address them; • As a teenager from Hong Kong, I would like to if parents have the rights to "have" their kids privacy, for example through a toy like Teddy the Bear, what kind of people can have access to the sensitive information that will be collected through those toys? • The question above refers to looking at the issue from the protection perspective but also from the rights perspective; IoT triggers many queries especially for devices handled by young people: at what point young people can claim their own data that has been collected for years? Are these tools going to report whatever the child says? The concept of disposable devices can be a solution. They can be used for a number of years and than thrown away. But even if I throw the device away, the collected data of the child will still be there. It will be stored by the company and exploited by the company. Who are the people employed by the companies who will process and analyze all this data?

	• In Japan the government is promoting the use of bar codes on the fingers and toes of the elderly suffering from dementia. This illustrates that human beings will be part of the IoT; • We need to avoid "predator panic". It is important to discuss safety issues and also to discuss solutions that a tech neutral so that when technology evolves, the laws are still valid and we do not stifle innovation. We should discuss protection to create a safe environment while avoiding sensationalism or tech panic; technology is here to help us, it is not a danger in itself; It is key to understand what technology can or can not do so that we learn to use its features to protect ourselves or create a safer environment; • Unfortunately, technology companies do not always offer the functionality that would allow parents to make enabled choices in the best interest of the child. Generally speaking, a lot of options offered to the parents and actually to all of us, is "take it or leave it". For example, parents cannot easily opt out of the health benefits proposed through devices for their children even though this comes with the companies doing data collection and monetizing it. Additionally, not all parents have the time or knowledge to fully understand the risks and dangers. So it is about making the companies work in the best interest of the child and bring technology to help us rather than neutral technology itself; • Privacy and safety go hand in hand especially when it comes to children. We need to focus the topic from a multi-disciplinary and multi stakeholder perspective. Preventive technology might be the way even if not the absolute solution. PhotoDNA is an positive example of this type of technology; • There is a need to look at the issue from a safety, privacy and safety by design perspectives and refrain from only looking at it from a legal perspective; a positive example of how safety by design can work is Illustrated by the car industry and how all sectors came together to find proper solutions to put an end to so many cars being stolen: • It is also key to look at the topic thinking of it from the perspective of the psychological development of the child. There is need for the research community to find out more about this aspect. Because so far we do not know the kind of impact that the interaction with interactive toys will have on the children's brain development and behaviors; • On data protection and data sharing: the questions we should ask are: what kind of data for children should be kept? What legal jurisdictions will prevail? Depending on where companies are located and where their servers are will impact of the legal treatment of the data collected from children. It is likely that there will be clashed depending on the laws in place and the different perspectives when it comes to privacy laws in particular. Data sharing is also beneficial for society and should not be considered only as a threat. For example, it can help prevent disasters, and diseases. In the US Silicon valley many companies in the field of IoT are choosing not to retain data at all to avoid liability and legal pressures deriving from it • Ethical aspects should also be raised: In Germany there is an ethical commission on the medical environment. We need to reflect on what kind of society do we want to live in? How do we want our future to be? • The IOT will not replace the relationship between the parents and their children; • Age differentiation is also one aspect we need to look at. Age categories of end users are to be taken into account. Appropriate solutions might vary according to the end users' age. Whether the user

	is a speechless baby or an adolescent does have an impact on the type of solutions that might be implemented; • There is a consortium of universities called PETRAS well funded. It stands for privacy, trust and responsibility around the issues of IoT. It is mainly doing test bed things. There is an ethical working group. Industry is aware of the dangers and risks. • The debates we are having are affecting all of us as adults and not only children. As Internet users we are all anxious about these aspects and all have rights at stake. END
Gender	45 participants: 17 female and 28 male
Link to transcripts	DC COP session: 1/**TRANSCRIPT**: http://tinyurl.com/zafkoxx 2/**VIDEO**: https://www.youtube.com/watch?v=BCLzNsQflQ8