

Workshop Name: Out of my Hands? (WS107)

Date & Time: 19 December 2017 11:50 – 13:20 pm

Organizer: Catherine Garcia van Hoogstraten

Moderator: Catherine Garcia van Hoogstraten

Rapporteur: Wilma Westenberg

Speakers:

- Arda Gerkens, Director of Expertisebureau Online Child Abuse, Dutch Senator, President of INHOPE
- Neil Walsh, United Nations Cybercrime Chief, UNODC
- Catherine Garcia van Hoogstraten, Technology, Internet Policy and Cybersecurity Consultant, Liaison and Associate Professor at the Faculty of Public Management, Law and Security -The Hague University of Applied Sciences, Visiting Faculty at the South School of Internet Governance
- Karuna Nain, Facebook's Global Safety Programs Manager
- Semanur Karaman, Coordinator Political Participation, Gender and Tech at Tactical Tech Collective
- Walid Al Sagaf, Vice Chair at ISOC Blockchain Special Interest Group* Renata Aquino, Researcher in Education, Communication and Technology, member of ISOC Blockchain
- Su Sonia Hearing, Mentor at Middle East & Adjoining Countries School of Internet Governance, Organizing Committee Member Youth IGF Turkey
- Gregory Mounier, Head of Outreach and Support at EUROPOL
- Claudio Lucena, Visiting Researcher at Georgetown University
- Olga Cavalli, Director of the South School of Internet Governance, ICANN GAC Advisor on the Special Group of Technology Affairs

Main goals:

- Explore key emerging exponential technology and user centered action being deployed by multistakeholders to counteract sextortion.
- Identify its challenges and opportunities and its implications for Internet Governance

Agenda:

Welcome and Overview - 2 minutes Moderator

Overview of the problematic through a video – 3 minutes

Speakers reacting to the 4 critical questions - 45 minutes

Open discussion among audience participants facilitated by Moderator and speaker acting as discussion Facilitators - 40 minutes

Summary:

A 40 seconds video was shown by speaker Gregory Mounier, Head of Outreach and Support at EUROPOL. The video called 'Say no!' was created for a campaign against online sexual coercion and extortion of children (more info, click [here](#)).

> Question 1: Can AI, blockchain or encryption based technology enable an effective response to sextortion?

Karuna Nain, Facebook's Global Safety Programs Manager

Facebook has **policies** about what is allowed to be shared on the platform. Sending naked images is not allowed. Facebook provides **tools**. Based on age, education, place, they provide relevant information to

stop grooming. In March they announced a new tool allowing users to report intimate pictures. A database with all the reported pictures will prevent pictures from being uploaded again. It will automatically be taken down when re-uploaded.

Walid Al Saqaf, Vice Chair at ISOC Blockchain Special Interest Group

Walid Al Saqaf briefly explained blockchain. Blockchain is created by Bitcoin and is peer to peer without a central bank. Nothing can be altered or be frauded. Back to the question: blockchain cannot directly be helpful. But it can be useful to track the identity of people who posted the pictures as nothing gets hidden or deleted.

Claudio Lucena, Visiting Researcher at Georgetown University

Claudio Lucena wonders how fast and easy the processes of deploying this software actually is. Article 13 enables and stimulates platforms to use automation of content recognition. One exception in the Brazilian market is images of intimate nature. Content recognition is a tool to be used here. Trust as a problem. There is a revolution in trust and Blockchain is the closest solution that is possible regarding trust issues.

Arda Gerkens, Director of Expertisebureau Online Child Abuse, Dutch Senator, President of INHOPE

Arda Gerkens is happy with the step Facebook took to stop re-uploading pictures. In the Netherlands something called 'exposure' is happening mainly to girls from Islamic cultures. Those girls never dare to share intimate pictures to the before mentioned tool of Facebook. There is no trust. We need to do something. The technique is there. The money is there. How can we get it to be established?

> Question 2: Sexual coercion and extortion. Will machine learning tools require that one have a clear definition as to what this sextortion content is?

Karuna Nain, Facebook's Global Safety Programs Manager

Karuna Nain states it's important to address it before sexual content even shared on Facebook. People could misuse the system by uploading other images. Also, often people who spread naked images, perform this act on different platforms as well. Facebook focuses on how they can build trust so people reach out to them or their friends, parents, etc.

Woman from the audience: it's always necessary to know the content. An innocent picture can still be used in a sextortion way so we need machine learning that also looks at the context.

Woman from audience: I do believe machine learning tools and blockchain can help prevent these sort of situations.

Woman from audience: Can Facebook staff assess the pictures that are reported? How do we make sure that everyone is cool with that and that we can safely report pictures?

Renata Aquino, Researcher in Education, Communication and Technology, member of ISOC Blockchain

Renata Aquino states the private sector needs help to create software like this. There should be a database where pictures are uploaded and the system recognizes what is erotica etc. We need dialogue with programs to make this work.

> Question 3: co-creation & control over tech. Can users participate in the use of automated tools content moderation? Do we need to embed accountability by design approach?

Male from audience: China has a system that allows users to flag content. Users vote on whether content should be deleted. Can this be done in this case, what will happen? Will you show naked pictures to users? What system do you have in mind?

Renata Aquino, Researcher in Education, Communication and Technology, member of ISOC Blockchain

Renata Aquino wonders how we can use technology in general for this problem. Users are never consulted. It's cheaper and faster to build a blockchain app that can do actions in bulk. Where are the case studies about this topic? We move on without any study that shows a system is working.

Arda Gerkens, Director of Expertisebureau Online Child Abuse, Dutch Senator, President of INHOPE

Arda Gerkens talks about a campaign in the Netherlands in which the focus was educating the community to stop spreading pictures.

> Question 4: Digital divide: Policies on new technologies may need to compass provisions on infrastructure, trust, security, and skills

Comment from the audience: 'Telling people we shouldn't post intimate things may cause people post more of such pictures because they seek danger and do things that are not okay'

Arda Gerkens, Director of Expertisebureau Online Child Abuse, Dutch Senator, President of INHOPE

Arda Gerkens thinks it's good to educate. She states we should not blame the victim. There are pictures that are intentionally being put online or being stolen. We can even use Photoshop, we don't even need actual pictures. A head can be pasted on another body.

Claudio Lucena, Visiting Researcher at Georgetown University

Different generations use the platforms in different ways. The problem is hard to tackle and from an evolutionarily perspective.

The session ended with a statement from the audience.