Workshop Name: WS146 - Decrypting Sextortion

Date & Time: 7 December 2016 12:30‑1:35 pm

Organizer: Hanneke Luth

Moderator: Catherine Garcia van Hoogstraten

Rapporteur: Su Sonia Herring

Speakers:

Catherine Garcia van Hoogstraten, Researcher and Lecturer at The Hague University of Applied Sciences- Centre of Expertise for Cybersecurity and Women in Cybersecurity (WiCs)

Arda Gerkens, Senator at the Dutch Parliament and Managing Director Expertise Bureau Online Child Abuse

Hanane Boujemi, Hivos Senior Manager Internet Governance Programme MENA

Alejandra Cantón Moreno, CISO at Giesecke & Devrient

Maria Cristina Capelo, Public Policy & Government Relations at Google

Nicolás E. Díaz Ferreyra, PhD Fellow at the User-Centred Social Media RTG, University of Duisburg-Essen, Germany

Su Sonia Herring, ISOC IGF Ambassador 2016, Internet Governance Youth Delegate, Editor, Social Media Specialist

Ms Jamila Venturini, Researcher at Center for Technology & Society at FGV Rio Law School

Key issues focused on the workshop were;

- Disrupting the sextortion dialogue by implementing solutions that stems from interdisciplinary research, analysis of evidence based policy and effective multi-stakeholder good practices in tackling the problem.
- How self-disclosure behaviors affect sextortion.
- The challenges and opportunities of using preventative technology to deal with certain forms of harmful content.
- The challenges and opportunities around the criminalization of nonconsensual pornography.
- The role of internet intermediaries' good practices based on content monitoring and take down tools.
- The role of different social and cultural norms on criminalization and enforcement of sextortion cases.

Three presentations were made by Ms Garcia van Hoogstraten, Ms Alejandra Cantón Moreno, and Mr Ferreyra where the first one focused on describing sextortion as a phenomenon consisting of nonconsensual pornography which are images and videos obtained by stolen, leaked or shared photos. Going into further detail by stating how the current architecture of the internet and social media enable

increased forms of exposure and how these vulnerabilities can lead to scalability, replicability and searchability of private information.

Ms Moreno presented the results of the social engineering experiment she and her team conducted during the first days of the IGF where they asked more than 50 IGF participants for info such as their name, company, email address and only 6 people asked for detailed information from the surveyors and answered the questions after receiving superficial information. Only one person refused to provide personal information stating they already have during registration. This displayed how easy it is to obtain information through social engineering, highlighting the vulnerability of younger people as well as less digitally aware adults. Moreno underlined how a few pieces of personal info could lead to identity theft and other negative outcomes.

Mr Ferreyra introduced his research on online self-disclosure, stressing how people can be unaware or forget the fact that social media services and other online services used are not free of breaches like identity theft, stalking, information leakage and so on. He mentioned how everyone discloses vital, basic information and the fact that online and offline social norms of sharing information is not the same, users are emotionally unattached from the info they provide online compared to the real world. Ferreyra also talked about the importance of raising awareness of the possible dangers to information sharing online.

Later on in the session, Ms Arda Gerkens, went back to the issue of social engineering giving examples of how sharing seemingly trivial info can lead to contact by strangers looking to gain trust which may lead to sharing of photos and videos which will later can used for sextortion purposes. She also mentioned that young people couldn't think of the possible consequences when sharing sensitive images. While Ms Su Sonia Herring, added to the discussion quoting the research paper conducted in late 2015, where it was found that focus on negative outcomes is not very effective as a discouragement for youth and in fact, it has recently been shown to have the forbidden-fruit effect. She also noted that many young people were more aware of consequences of self-disclosure than their adult counterparts and this did not prevent them from sexting or similar online sexual behavior; concluding that instead of focusing on negatives education youth and adults to take part in safer sexual online expression could be more beneficial. A participant mentioned how research displayed young people in India who use sexting and similar practices are very aware of what they're doing, the possible consequences and stated how the term 'excessive self-disclosure' may conclude in victim blaming/shaming. Gerkens stressed the difference between consensual and non-consensual sharing while pointing out serious consequences of sextortion leading to suicide of victims.

Ms Jamila Venturini added how the language of these terms aren't easy to understand as they are mostly complicated and law jargon, which opens the way for companies to use data of their users more freely. The analysis also displayed common points between ToU in how they said the data provided may be shared with third parties, may be stored for a certain amount of time and so on. Help pages and videos that inform users were mentioned as good examples. She highlighted that when it comes to freedom of expression, ToU did not seem to address the subject as much as privacy, and when it does it usually refers to copyright issues. Ms Hanane Boujemi, brought up not only women but men are also victims to these crimes while touching on the fact of how having legislation wasn't always easy across different countries and cultures. She underlined taking down content may result in problematic

implications again across different cultures since it can be used to silence and censor LGBT or minority sexual expression online.

Next ways forward and possible takeaways mentioned in the session included, the importance of help pages and videos that enable users to better understand Terms of Use of online platforms, tools which ask for explicit consent prior to sharing sensitive information or videos/images, the importance of awareness and education in preventing sharing sensitive information online, education youth on safer sexual expression online instead of trying to ban and/or use scare tactics, the potential of giving all responsibility to the victim leading to victim blame in sextortion cases, more transparency in the process of taking down content; such as letting users know when, how and under which circumstances content take down occurs and the negatives of platforms not letting end users know when a takedown has taken place.

From the private sector perspective, the importance of dialogue between platforms and advocacy groups was mentioned as a good practice while the international aspect of things was highlighted as a big takeaway in dealing with cases swiftly as well as the general lack of explicit legislation of sextortion. The issue of cultural differences was mentioned as a major takeaway citing how some countries use legislation to silence and censor minorities and LGBT communities using same laws to address sextortion. The need for more comprehensive rules and guidelines on online platforms was stressed.

The suggestion of more widespread use of the hash technology was underlined to combat reuploading of known criminal content. The criminalization of sextortion in countries such as US, Israel, Canada, Japan, Philippines were cited as good practices while it was highlighted that the legislation shouldn't be limited to only former partners but anyone who shares explicit content without consent even if they do not know their victims personally. The need to look for offline solutions was stressed as there are the social and cultural aspects of the issue which make the tackling of the problem more complex.