Published on *The Parliament Magazine* (https://www.theparliamentmagazine.eu)

In conversation with... Lucinda Creighton

Written by The Parliament Magazine on 22 November 2019 in Interviews
Interviews

The Counter Extremism Project (CEP) works to combat extremist ideologies, including tackling terrorist content online and has actively followed the discussions on the proposed Terror Content Online regulation, says Senior Advisor, Lucinda Creighton.

Photo credit: Adobe Stock

What is the current status of the terror content online regulation?

The terror content file has just entered trilogues under the Finnish EU Council Presidency and we remain optimistic that it can be finalised before the end of the year.

At the moment, discussions are focusing on the inclusion of a provision on proactive measures and the scope of cross-border jurisdictions.

RELATED CONTENT

- **EU foreign and defence policy must be effective** [1]
- **Finding common ground** [2]
- **New opportunities** [3]
- **Security in cyberspace requires a comprehensive EU approach** [4]
- **Parliamentary leadership for the Digital Age** [5]

Why are proactive measures such a sticking point?

The inclusion of proactive measures in the text would require online platforms and companies to proactively deploy automated filters and algorithmic tools to identify and prevent the upload of content designated, under the Regulation, as terrorist.

The European Parliament removed the provision on proactive measures in its text on the basis of fundamental rights, arguing that upload filters lack the ability to understand the context or detect satire in content.

There have been claims of censorship which is not the case. If you consider that upload filters are already deployed by all platforms to prevent the dissemination of child pornography, this argument becomes redundant.

We have a duty to protect citizens from terrorism, just as we have a duty to protect against child exploitation.

We have watched companies self-regulate but it hasn't worked. It is now time for clear rules and sanctions for those who continue to fail in their duty.

The requirement for proactive measures facilitates that, we cannot afford to wait on removal orders for every piece of content, particularly when the same content appears time after time. There is no excuse for this.

We need companies to be required, under legislation to do more. They need to take responsibility for the content hosted on their platforms.

> "We have watched companies self-regulate but it hasn't worked. It is now time for clear rules and sanctions for those who continue to fail in their duty"

Are proactive measures the only way forward?

Yes. Technology companies pledged to be more effective in removing extremist content when they were threatened with fines and regulation.

However, we have yet to see this translate into measurable, systematic and transparent actions which will see this content permanently removed.

Content which has had a demonstrably tragic impact on the lives of people across the world. We are forced to believe that companies do not care about the way their platforms are used.

If technology companies want to be seen as part of the solution and as normal reputable businesses, they must acknowledge their role and make dramatic efforts to stop their platforms being used by extremists to recruit individuals and spread harmful content.

This year demonstrated a new facet of the threat of online content. We saw several horrific live-streamed attacks take place across the world.

The speed and volume with which content is shared online makes radicalisation extremely difficult to control.

No attack reflected this more than the Christchurch mosque shooting in New Zealand and the more recent attack in Halle in Germany.

In the case of Christchurch, 1.5 million videos containing footage of the shooter's livestream attack were detected and removed by Facebook. Around 1.2 million of these videos were screened by Facebook's software and were blocked from being uploaded.

But that still means that around 300,000 videos made it online and were seen by a large percentage of users.

Given the content was the same, you have to wonder how those 300,000 made it through and onto the platform and remained there for quite some time.

And this is just Facebook. All other social platforms have similar stories, with people radicalised every day, and little being done to curb it.

Proactive measures would mean that the risk of exposure to terrorist content would be dramatically reduced.

> "Clear measures, particularly monitoring and filtering obligations for companies operating online, need to be included in the final text"

Can technology help prevent the dissemination of terrorist content and respect fundamental rights?

Doctor Hany Farid, a senior advisor to CEP and digital forensics expert at the University of California, Berkeley, believes that it will be around 10-15 years before Artificial Intelligence will be ready to work without human verification.

In the meantime, advanced hashing technology will provide the best solution. Hashing technology, like CEP's eGLYPH, alongside appropriate legislation and education around tolerance and critical thinking online, must form the backbone of the overall solution in the fight against online terrorism.

eGLYPH is a technology, developed by Farid, that recognises duplicates of images, video or audio recording by hashing, identifying a digital fingerprint in each.

The technology is capable of swiftly comparing uploaded content to a database of known extremist content and can disrupt the spread of that content.

Disruption is critical, as videos and images can spread onto smaller, encrypted platforms in a matter of hours.

Here at CEP, we have worked hard to highlight the lack of accountability and responsibility that companies take on extremist content.

Results from a 2018 study on YouTube showed that from a subset of 229 known ISIS terror-related videos and 183 keywords identified as indicative of pro-ISIS sympathies, eGLYPH, with the help of a WebCrawler, found that 91 percent of videos identified were uploaded more than once.

This proves that YouTube's claims of proactive removal were nothing more than hearsay.

What do you hope will be included in the final text of the regulation?

A clear definition for terrorist content allowing a database to be created where this content can be 'hashed' or categorised, compiled and shared with internet service providers, who can ensure that the content is permanently removed.

Through proactive measures, once the content is hashed, technology can then be used by platforms to prevent that content appearing on their platform again.

We have an obligation to ensure the safety and security of Europe's citizens and if the companies cannot be trusted to do this then regulation will have to do. This is why clear measures, particularly monitoring and filtering obligations for companies operating online, need to be included in the final text.

Tags
Digital Agenda [6]
Foreign Affairs [7]
Justice and Rights [8]
Categories
Copyright [9]
Data privacy [10]
Digital single market [11]
Internet of Things [12]
Defence and Security [13]
Public order, justice and rights [14]
Science, technology and research [15]

- Climate Crisis
- Editorial Calendar
- Policy Events
- Event Coverage
- MEP Awards 2020
- Contact Us

Services

Dods PeopleDods
MonitoringDods
ResearchDods
EventsDods
Training

Media & publishing titles

Politics HomeThe
HouseThe
Parliament
MagazineHolyrood
Total PoliticsPublic
Affairs NewsCivil
Service
World
PublicTechnology
Training
JournalDods
Parliamentary
CompanionVacher's
Quarterly The
European Union and
Public Affairs
Directory

Dods events

Westminster
BriefingDigital
Health & Care
ScotlandMEP
AwardsThe Skills
SummitScottish
Public Service
AwardsPublic Sector
Procurement
SummitPublic
Sector ICT
SummitCyber
Security
SummitCyber

Security 2017Training Journal Awards

Partnership events

The Health and Care Innovation ExpoCivil Service LiveCivil Service AwardsChief Nursing Officer for England's SummitWomen into LeadershipThe Youth Justice ConventionSocitm Spring ConferenceNHSCC Annual Members' EventDods at Party Conference

---

---

[11] https://www.theparliamentmagazine.eu/categories/digital-single-market
[12] https://www.theparliamentmagazine.eu/categories/internet-things
[13] https://www.theparliamentmagazine.eu/categories/defence-and-security
[14] https://www.theparliamentmagazine.eu/categories/public-order-justice-and-rights
[15] https://www.theparliamentmagazine.eu/categories/science-technology-and-research