Preventing Terrorist Content: Using Legal Liability to Incentivize Tech Companies to Develop More Effective AI

By Liz Bramley, J.D. Candidate 2021 | April 7, 2019

In the wake of the Christchurch shooting, The French Council of the Muslim Faith (CFCM) filed legal papers against the French branches of Facebook and YouTube for failing to remove related content fast enough. Under French law "broadcasting a message with violent content abetting terrorism, or a nature likely to seriously violate human dignity and liable to be seen by a minor" is punishable by up to three years jail time and $85,000 fine.

The shooting, which was initially live streamed on Facebook for seventeen minutes, was undetected by the platform's AI system and remained up for twelve more minutes. By the time Facebook removed the video, it had been uploaded to 8chan, a cite known for its white supremacist postings. From there, the video was disseminated across the internet, where both Facebook and YouTube failed to identify footage that remained up for hours.

CFCM's stance that tech companies have a responsibility to better prevent the upload of terrorist content was echoed by the chairman of the U.S. House Committee on Homeland Security, Bennie G. Thompson. In a letter to the executives of Facebook, YouTube, Twitter, and Microsoft, Thompson tells the tech giants they "must prioritize responding to these toxic and violent ideologies with resources and attention."

But unlike the European union, where Facebook's responsibility stems from public sentiment and corresponding legal liability, the US differs dramatically. American ideals of free speech and individual responsibility are distorted by political rhetoric that frames legal liability as a slippery slope to quashing free expression. This view is confirmed by our own legal system, which insulates Tech companies from facing recourse for the hateful content and subsequent violence enticed, in part, by users and content on their platforms.

American Courts have repeatedly dismissed lawsuits similar to the CFCM complaint at the pleading stage, ruling that Section 230 of the Communications Decency Act of 1996 bars these complaints. Section 230 states that providers of interactive computer services cannot be treated as publishers of user postings. This gives tech companies sweeping immunity from violent acts that are directly linked to user content. For instance, victims of the Pulse Nightclub shooting were barred from bringing a lawsuit against Facebook, Twitter, and Google for allowing violent and hateful videos that radicalize the shooter to remain on their platforms.

In some ways, this is a good thing. Sparing interactive internet companies from liability focuses fault on the individual perpetrator. Moreover, people are validity concerned about policing speech and

narrowing viewpoints. However, the flip side is a lack of civil recourse to address substantial wrongs and the resurgence of violent far-right ideologies.

Given that over 1.5 million attempts were made to reupload the video to Facebook alone, AI detection is the most viable way to stop violent content from being disbursed across the internet. Expanding legal liability has already proven to effectively block harmful user content. As shown by the FOSTA-SESTA ACT, making websites liable for illicit sexual activities taking place on their platform incentivized companies to develop effective technology to identify child pornography. A similar legislative act that expands liability to encompass the distribution of violent content could incentivize tech companies to develop more effectual preventative AI tech.

As modern day monopolies, Tech companies such as Facebook and YouTube have a responsibility to protect users from violent content. And as threatened by Thompson, if they are unwilling to make this goal a priority, our legal system should.