



Livestreaming: An Attractive Tool For Attackers

Livestream videos of terror and other violent attacks will likely become more common because perpetrators have easy access to smartphones and social media platforms that enable threat actors to easily publicize their actions. Moreover, social media companies have difficulty policing live feeds and removing them from the Internet in real time. Since 2015, there have been at least nine attacks livestreamed by terrorists, criminals, and other violent actors.

- Livestreaming only requires a camera—often a smartphone or GoPro—and a social media account. It is easy to livestream and upload content and, once on the Internet, video is commonly and readily shared across multiple social media platforms; social media companies also encourage users to “like” or “share” content because ads and paid sponsorships are often linked to them, enabling the platform to earn revenue.
- Most perpetrators livestream their attacks to gain notoriety and establish a global platform to publicize and spread their message. For example, on March 15, Brenton Tarrant livestreamed on Facebook his attack on two mosques in Christchurch, New Zealand that caused 50 deaths and dozens of injuries. Despite Facebook, YouTube, and other social media companies’ attempts to block the video, it was shared approximately 4,000 times on Facebook before it was removed, and users attempted to re-upload the video more than 1.5 million times.
- The algorithms social media companies use are effective in monitoring and filtering text posts, but videos are more difficult to detect and filter. Clips and copies of videos can be shared easily and edited videos—filtered or zoomed in or out—can be re-uploaded without detection.

Timeline of Notable Livestreamed Attacks in the United States

