THE CRIME & TERROR THREAT ON SOCIAL MEDIA

“If it’s illegal IRL, it should be illegal to host it online.”

THE PROBLEM

Social media platforms provide criminal groups and terrorist organizations with an open marketplace infrastructure that is global, encrypted and highly lucrative.

Illegal groups don’t need to hide on the dark web, since social media platforms already provide substantial anonymity, peer-to-peer payment systems and a far greater reach of people – more than a third of the world’s population.

Outdated U.S. technology laws provide immunity to tech firms, creating an environment where social media firms generate billions of dollars in profit without accountability for the array of illegal activity occurring on their platforms.

THE SPECIFICS

Drug cartels and illegal pharmacies selling banned narcotics and fake pharmaceuticals

Designated terror groups openly fund-raising for attacks, and recruiting new members

Syrian rebels – some openly claiming allegiance to ISIS – selling plundered antiquities

Wildlife markets so large they are threatening key species including elephants, apes and cheetahs

Modern-day grave robbers selling human remains, from shrunken heads to babies in jars

Weapons dealers selling automatic rifles, explosives, and ammunition

Human traffickers trading men, women and children for sex and labor

THE SPECIFICS

HOW IT WORKS

First, create a post advertising goods. Upload it on an open part of the platform that does not require a password.

5 of 6 Steps take place on social media platforms!

Finally, the seller will deliver the illegal goods, typically using the postal service or a courier. Buyer and seller rarely meet IRL.

Build a community of buyers by creating forums, including closed or secret groups. Only buyers with ‘special access’ can enter.

Buyers ‘like’ images sellers post, and/or send DMs. In some cases, sellers will reach out to buyers to direct market based on the buyer’s past activity.

The buyer will send all or most of the payment up front, either using a linked payment app, or a separate payment service.

Seller and buyer negotiate the sale. This may occur directly on the social media app, or on a linked, encrypted chat platform.

LEARN MORE

Find ACCO research and media coverage at www.counteringcrime.org.
KEY FACTS AND FIGURES

Facebook admitted to removing 1.5 million postings that were selling narcotics. That’s more than 100 times as many drug postings ever carried by the Silk Road.

Hezbollah, which has linked to its Facebook and Twitter from its official websites, is one of many designated terror groups that have used social media to fundraise for terror attacks.

More than 2 million active users are members of Facebook groups where ISIS supporters sell looted artifacts.

Independent research indicates that terror content from groups like ISIS and al-Qaeda are removed approximately 38% of the time.

A quarter of British children have seen drugs for sale on Instagram, according to the UK’s health service.

Facebook’s algorithms autogenerate terror propaganda videos and groups that lure new recruits.

CURRENT LAW

Section 230 of the 1996 Communications Decency Act grants expansive liability to any provider of an “interactive computer service” for user-generated content. Courts have even found companies that knowingly hosted illegal content to be exempt from liability based on the broad CDA230 language. That’s nearly a quarter-century of unabated crime taking place on the Internet with no consequences to the tech industry!

PROPOSED LEGAL REFORM

It’s time for Congress to reform CDA230 and explicitly strip out immunities for crime and terror content.

By reforming CDA230, lawmakers could shift the responsibility for monitoring Internet platforms for illicit activity to tech firms, and regulate firms to hand over evidence of illegal activity to law enforcement. If this reform doesn’t occur, current campaigns to improve user privacy could have the unintended consequence of making the Internet a safer place for criminals and terrorists.

ACCO’S MISSION

The Alliance to Counter Crime Online is a team of security experts, academics, NGOs and citizen investigators that have come together to fight a serious societal threat. We aim to push organized crime and terror activity off Internet platforms.

Educating lawmakers, regulators and the public about the impact of online criminal networks

Driving media coverage of our investigations and the threats to consumer safety

Campaigning for legislative reform and effective regulation of the Tech Industry

Supporting international law enforcement bodies to act against illicit groups operating online

Protecting society from the dangers caused by unregulated, irresponsible tech firms

Coordinating the flow of information about illegal activity to social media companies and police

LEARN MORE

Find ACCO research and media coverage at www.counteringcrime.org.