CINTOC

ESG SPOTLIGHT

Organized Crime and Terror on Facebook, WhatsApp, Instagram and Messenger

alliance to counter crime online

alliance to counter crime online

CINTOC

Key Finding

Facebook has failed to implement internal controls to restrict and respond to organized crime activity and terror content across its family of platforms. This approach is unsustainable and could lead to future liabilities as well as a reduction in future earnings.

Key Insights

Shortsighted Management Strategy

Facebook's failure to implement internal controls to restrict and respond effectively to illicit activity on its platforms is indicative of a shortsighted management strategy based on treating illicit and toxic content as merely a PR issue, and lobbying to perpetuate a regulatory status that appears poised to change. This approach will become more expensive over time and will leave the company unprepared when Congress does change the law.

Facebook's Unique Exposure

All top tech firms contend with toxic content however, the extent of it on Facebook's family of platforms, and the firm's nearly complete dependence on advertising, give the firm unique exposure to the accumulative risks of user and advertiser attrition.

Stakeholders Were Misled

Facebook's leadership has failed to advise advertisers, regulators and investors about the extent of toxic content on its platforms as well as its capacity to self-regulate.

A Problem That's About to Get Worse

Facebook's "pivot to privacy" positions its platforms to become the preeminent global home for online illicit activity, increasing the risk of regulatory scrutiny, costly legal battles, reputational damage, as well as user, staff and advertiser attrition.

Risky Business

The world's largest social media company does more than just connect people. Its platforms are also ground zero for organized crime syndicates to market their illegal goods, and move money, using the same ease of connectivity enjoyed by ordinary users. Designated terrorist groups have weaponized Facebook platforms to broadcast propaganda, recruit new members, and fundraise.

This illegal activity occurs out in the open, and also through private and secret groups, two staple features of the platform. Advertisements for major corporations run alongside illicit content. Facebook is not just a passive system that merely hosts this toxic content. The same algorithms the firm created to connect people also facilitate illicit activity by connecting criminals to buyers, and terrorists to their supporters. This happens far faster than Facebook's moderation systems can remove the material.

Section 230 of the 1996 Communications Decency Act (CDA 230) grants expansive safe harbor to any provider of an "interactive computer service" for user-generated content, but expects firms to moderate their platforms for illicit content. CDA 230 has been interpreted by courts as providing broad immunity to the tech industry, even in cases when firms knowingly host illicit content. Because of these court rulings, multiple tech firms, including Facebook, failed to establish internal controls to contain and remove illicit content. This decision is a liability today. Like chemical firms a half-century ago that were highly profitable so long as they could dump toxic waste with immunity, Facebook's failure to contain illicit content will cause a reduction in earnings, now that it threatens consumer safety, and has drawn regulatory scrutiny and legal challenges. As Facebook's own Transparency Project is forced to release more and more data about the vast scale of illicit activity occurring on its platform, in particular illegal drug sales and child pornography, the regular drumbeat of media reports and Congressional hearings could spark a long-term and steady decline in profitability.

alliance to counter crime online

CINTOC

Management Strategy Risk

Facebook has failed to develop a management strategy that effectively responds to the shifting legal and regulatory environment. CDA 230 immunities are now under threat in both houses of the legislature. Congress passed a carve-out for human trafficking content in 2017, and multiple lawmakers are now drafting further carve-outs related to drug and terror content. Moreover, the firm stands accused of being uncooperative with U.S. law enforcement sometimes even when subpoenaed, and of using any available tactic to retard the progress of cases through the courts.[1]

Facebook's strategy has been to deflect and delay legal reform through an intensive and expensive lobbying campaign. Embracing a strategy more concerned with delaying legislation, investigation, and litigation than in resolution is expensive – in 2019 Facebook spent more on lobbying than any other single firm besides Amazon – and this approach will become less viable over time. It also produces secondary effects. In one 2019 Texas case, Facebook's attempt to delay proceedings resulted in the judge issuing an order stopping the company's rollout of its "Clear History" tool across the US market, highlight the risk that litigation can pose to a company's freedom of operation. Facebook has already paid out handsomely for poor data management.[2] Recent court findings against Johnson and Johnson and Perdue Pharma over opioid sales suggest Facebook could also face legal battles for its role as a drug marketplace.

Consumer Welfare Risk

Facebook platforms appear to have been key facilitators in the opioid crisis that claims 130 American lives every day. Illegal pharmacies and drug dealers use Facebook and Instagram to peddle vast amounts of narcotics, benefitting from algorithms to connect with buyers. After immense pressure from the Department of Justice, Facebook began tracking drug postings on its platform in 2018. Within six months, Facebook admitted to removing 1.5 million posts selling drugs. To put that quantity in perspective, it's 100 times more postings than were ever carried by the notorious dark website the Silk Road. In November 2019, Facebook's Transparency Project released Q3 2019 data about drug sales postings removed; by then, the number reached a staggering 4.4M drug postings in just one quarter. The firm also faces consumer welfare risk around the high instance of child sexual imagery found on its platforms. In October, Mark Zuckerberg admitted in Congressional testimony that his firm had reported 16.8M images of child sexual abuse to U.S. authorities, since landmark legislation passed requiring tech firms to police their platforms and report instances of abuse. The New York Times published a disturbing report graphically detailing the vast scale of online child abuse and highlighting the "extent to which Facebook in particular failed" to enact early barriers to this illicit material. These revelations have led to angry responses from Congress and law enforcement that Facebook misled them about the scale of drug and child sex abuse content on their family of platforms. Misleading statements were also present in Facebook's SEC reporting.

Critical Incident Risk

It took more than 29 minutes and over 4,000 views before Facebook first removed the livestreamed Christchurch video, which Facebook's weak internal controls had failed to identify on their own. The video quickly went viral, and Facebook later admitted to removing another 1.5M copies over the next 24 hours. Facebook's year-long struggle to keep copies of the video off its platforms revealed the firm's inadequate critical incident management system. The Christchurch video case also highlighted the extent to which Facebook's algorithms are more effective at spreading toxic content than its own moderation systems are at removing it.

Business Model Risk

With 98.5% of its revenue derived from advertising, Facebook faces unique risk in the event of severe user and/or advertiser attrition. This risk exists if government substantially restricts user data resale, prompting advertiser attrition, and also if consumers and advertisers flee the platform as reports of toxic content come to light. Although advertising revenue is currently up – reflecting the ongoing migration of advertising dollars from traditional to digital platforms – stagnating user numbers in North America and Europe for multiple quarters in a row suggest a troubling trend since those users account for nearly three quarters (48% and 24% respectively) of Facebook's revenue, and since user numbers are growing for competitors like Snapchat and TikTok.[3] Each time news breaks of another illicit activity amplified by Facebook, or another #DeleteFacebook campaign goes viral, it raises questions for advertisers about brand security, including concerns about ad placement on pages featuring illicit content or ads inadvertently funding illegal or immoral activities. Other stakeholders have also exhibited dissatisfaction with the long-term ramifications: There has been a flux of mid- and high-level defections, with more possible, and public critiques by former allies. With internal morale low, Facebook's recruiting arm is struggling to attract top tier talent.

Making Matters Worse: The Privacy Pivot

In March 2019, Facebook CEO Mark Zuckerberg announced that the company would make protecting user privacy its new cornerstone, increasing the number of private groups and incorporating end-to-end encryption across all its messaging apps. This proposed change may be an attempt to legally insulate the firm, as Facebook executives can claim they can't possibly police content they can't read. However, this proposal should also be perceived as the digital equivalent of sweeping an enormous problem under the rug. As several recent reports and a class action lawsuit by former moderators have revealed, some Facebook groups contain such toxic content, they literally sicken those who patrol them. Greater encryption is likely to increase that problem, by helping illicit actors to cover their tracks. The pivot toward privacy – with full integration of Instagram, WhatsApp, and messenger, end-to-end encryption, in-app marketplaces, and possibly a cryptocurrency – could turn Facebook into a darknet that would effectively bring the Silk Road to Main Street. By building out private groups, encrypted chat, and anonymous payments, a 'privacy first' Facebook would optimize growth opportunities for marketing and selling illegal goods, threatening to make Facebook a pioneering digital benefactor for illicit groups around the world, enabling criminal actors to reach billions of customers with ease.

[1] In addition to the eleven open cases at the state and national level against it here in the United States, Facebook is facing calls for increased regulation around the globe including India, China, Russia and the EU.

[2] The FTC and SEC have each leveled fines on Facebook around its data management ($5B and $100M respectively), and with the EU preparing further sanctions, total penalties could mount to $8B, or $3.30 per Facebook Monthly Active User (MAU), a figure greater than the firm's Average Revenue per User anywhere but North America and Europe. The US and Canada have ARPU of $33.27, Europe has an ARPU of $10.70 while the ARPU of Asia Pacific is $3.04 and the rest of the world, $2.13.

[3] Despite the sluggish numbers, many analysts continue to view Facebook favorably, pointing to the potential for grown of Average Revenue Per User (ARPU) particularly in the fast growing Asian market where those numbers lag behind North America and Europe. But growth in those markets faces two major hurdles: Ongoing regulatory battles in India and recent threats by the Chinese government to sanction firms that pay to advertise on Facebook (Facebook does not operate in China but Chinese firms advertise on the platform to reach users in the rest of the world) could make those markets expensive or unpredictable or both.

CINTOC

About Us

The Center on Illicit Networks and Transnational Organized Crime (CINTOC) is a strategic intelligence organization that finds hidden criminal networks. We take on big, bold projects many consider unsolvable. CINTOC founded the Alliance to Counter Crime Online (ACCO), which brings together more than 30 academics, NGOs and citizen investigators, who are the world's leading experts on organized crime in cyberspace. Our experts work across multiple of sectors including human trafficking, drugs, wildlife crime, conflict antiquities and fraud. We produce investigative reports, develop tools and strategies to better detect and catalog online illegal activity, and we advocate to lawmakers, regulators and industry to enact more effective regulation of the Internet.

alliance to counter crime online