

# Facebook Shielded by CDA Immunity against Federal Claims for Allowing Use of Its Platform by Terrorists

**New Media and Technology Law Blog** on August 9, 2019

In recent years, there have been a number of suits filed in federal courts seeking to hold social media platforms responsible for providing material support to terrorists by allowing members of such groups to use social media accounts and failing to effectively block their content and terminate such accounts. As we've [previously written about](#), such suits have generally not been successful at either the district court or circuit court level and have been dismissed on the merits or on the basis of immunity under Section 230 of the Communications Decency Act (CDA).

This past month, in a lengthy, important 2-1 decision, the Second Circuit affirmed dismissal of federal Anti-Terrorism Act (ATA) claims against Facebook on CDA grounds for allegedly providing "material support" to Hamas. The court also declined to exercise supplemental jurisdiction over plaintiff's foreign law claims. ([Force v. Facebook, Inc.](#), No. 18-397 (2d Cir. July 31, 2019)). Despite the plaintiffs' creative pleadings that sought to portray Facebook's processing of third-party content as beyond the scope of CDA immunity, the court found that claims related to supplying a communication forum and failing to completely block or eliminate hateful terrorist content necessarily treated Facebook as the publisher of such content and were therefore barred under the CDA.

This is a noteworthy decision, as an influential circuit (and one that has issued only a few CDA-related decisions) enunciated an interpretation of robust CDA immunity. In particular, the court applied CDA Section 230 to Facebook's decisions of how to structure and operate its platform. It specifically focused on Facebook's use of friend and content suggestion algorithms that arrange or distribute third party information to form connections among users or suggest third-party content to other users. Beyond this case, such automated processes are an integral part of many social platforms or media sites, and as such, the *Force* decision is significant. Moreover, as many sites or services continually struggle with how to remove objectionable content of any type from their platforms (while balancing free speech concerns), the decision also underscores that an online provider is still entitled to CDA immunity for hosting third-party content even when such a provider has affirmatively implemented processes to eliminate abhorrent or dangerous content but has not been entirely effective or consistent in those efforts.

In *Force v. Facebook*, the plaintiffs are the victims, estates, and family members of victims of terrorist attacks in Israel. They asserted various federal anti-terrorism claims against Facebook based on allegations that Facebook supported the terrorist organization Hamas by allowing that group and its members and supporters to use Facebook's platform to post content that purportedly enabled the attacks and furthered their aims. In 2018 the lower court [dismissed](#) the suit, ruling that "Facebook's choices as to who may use its platform are inherently bound up in its decisions as to what may be said on its platform," and so liability imposed based on failure to remove users necessarily involves publishing activity protected under the CDA. Echoing the lower court's holding, the appeals court [affirmed](#) the lower court's holding, stating that plaintiffs' claims were barred by the CDA.

The plaintiffs' principal argument was they are seeking to hold Facebook liable for its own content, and not that generated by another "information content provider," i.e. Hamas and related entities. The argument was based on Facebook's alleged role in "networking" and "brokering" links and communications among terrorists, and not simply based on its failure to "police its accounts" and remove terrorist-affiliated users. Under plaintiffs' theory, Facebook does not act as the publisher of Hamas's content within the meaning of CDA Section 230(c)(1) because it uses algorithms to suggest content to users, resulting in "matchmaking," that is, that Facebook's "newsfeed" uses algorithms that show the third-party content that is most likely to interest and engage users and also provides friend suggestions based upon similar data analysis.

The Second Circuit rejected plaintiffs' contention that Facebook's use of algorithms renders it a non-publisher, finding no authority for the proposition that an "interactive computer service" is not the "publisher" of third-party information when it "uses tools such as algorithms that are designed to match that information with a consumer's interests." The court likened such automated processing and prioritizing of third-party content to a newspaper placing certain content on the front page or a website displaying content on a certain page to reach a desired audience, that is, inherent "publishing" activity protected under the CDA. According to the court, Facebook's algorithmic handling of certain content could be considered "neutral tools" akin to the [platform design in the Herrick case](#) that included features that matched users of a dating site or ["automated editorial acts" in the Marshall's Locksmith case](#) that involved conversion of third-party location data into map pinpoints.

"[P]laintiffs' argument that Facebook's algorithms uniquely form 'connections' or 'matchmake' is wrong. That, again, has been a fundamental result of publishing third-party content on the Internet since its beginning. Like the decision to place third-party content on a homepage, for example, Facebook's algorithms might cause more such 'matches' than other editorial decisions. But that is not a basis to exclude the use of algorithms from the scope of what it means to be a 'publisher' under Section 230(c)(1)."

The court also rejected plaintiffs' argument that Facebook's automated processing of the Hamas-related content should make it the "developer" of such content because its automated systems allegedly assisted in placing it in front of potentially likeminded users. The majority opinion was not persuaded by the plaintiff's argument (and the dissent's suggestion) that Facebook's use of algorithms is outside the scope of publishing activity under the CDA because the algorithms automate Facebook's editorial decision-making and facilitate Hamas's ability to reach an audience – instead, the court concluded that "so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific edit[orial] or selection process."

Ultimately, the court held that Facebook's automated activities do not make it a "developer" or render it responsible for the Hamas-related content:

"Merely arranging and displaying others' content to users of Facebook through such algorithms—even if the content is not actively sought by those users—is not enough to hold Facebook responsible as the 'develop[er]' or 'creat[or]' of that content."

"[M]aking information more available is, again, an essential part of traditional publishing; it does not amount to "developing" that information within the meaning of Section 230."

The presence of terrorism-related content on social media sites brings up a host of legal, moral and technological issues for social media platforms. After calls for stricter monitoring of extremist content – and after having to defend multiple lawsuits over such content – the major social media platforms have taken greater action to combat the spread of online terrorist videos and other material. Known terrorist images or posts that signal support for terrorist groups are typically filtered out before they ever reach users and platforms are using artificial intelligence and machine learning to block or remove pro-terrorist content and automatically detect terrorist-related accounts. According to the court, Facebook itself also employs thousands of people to respond to user reports of extremist content and it has announced new initiatives in the past year to clean up its platform and try to stay ahead of the terrorists who try to evade the controls. Still, the problem remains a serious issue, as evidenced by Facebook and other companies having just [testified in June before a Congressional committee](#) about the removal of terrorist content from their platforms and the EU Parliament in April having backed a [proposal](#) to require platforms to remove terrorist content within one hour after receiving an order from a national authority.

The political winds in Washington seem to be supporting a [reevaluation of the scope of Section 230](#). This decision is likely to add strength to those winds.

[View original](#)

#### [Related Professionals](#)

---

- **Jeffrey D. Neuburger**  
Partner