Turning Tech Companies into Spies Won't Work

By: Lee Rowland
December 2015

Source: American Civil Liberties Union
Available at: https://www.aclu.org/blog/free-speech/internet-speech/turning-tech-companies-spies-wont-work?redirect=blog/speak-freely/turning-tech-companies-spies-wont-work

Imagine that before engaging in an attack, a terrorist sent an anonymous handwritten note to a local newspaper. Would politicians scramble to demand that we burn all paper, ban all anonymous mail or install government cameras in every newsroom? Of course not.

Yet following the revelation that one of the San Bernardino murderers pledged support for ISIS on social media, we are seeing a renewed flurry of politicians, both established and aspiring, calling for increased censorship of the Internet. Proposals include demands that companies scrub their platforms of terrorism-related content and a federal bill that would turn social media companies into state-mandated reporters of "terrorist activity."

These responses are deeply misguided. A good two-step framework for evaluating any policy proposal is to ask: 1) is it consistent with our laws and values and 2) is it effective in achieving its goals? Applied to censorship of online speech, the answer to both questions is an emphatic no.

First, pure censorship of speech is just a very bad idea. Whether it's labeled "hate speech" or "terrorist speech," silencing speech that is not itself illegal cuts directly against our free speech values (only a very a narrow and carefully-defined band of speech is itself illegal, like threats, incitement to violence or child pornography). There's a reason that our First Amendment protects even the vilest speech. It's not just lawyerly paranoia about slippery slopes—it's because transparency itself has immense value. Censorship makes censored speech all the more dangerous because we lose our most powerful tool in combatting evil ideas: the ability to identify them and respond with better ideas.

Mandating tech companies to report on "terrorist activities," which Sen. Dianne Feinstein (D-Calif.) proposed in a bill she introduced Tuesday, is a flawed idea as well. Social media companies should and do notify the government if they learn that a user is threatening immediate violence. But we should be wary of proposals that go beyond that. Perhaps the most obvious reason is the simplest: online service providers are not experts on terrorism. They're businesses, not intelligence agencies. And there's no magical bright line that separates "good" from "bad" speech, no mystical algorithm possessed by Facebook to figure out exactly what speech—speech that is not already illegal—should be reported to the state.

Let’s say you work on the front lines of Facebook’s censorship team. Which of these do you report to the feds: someone who retweets ISIS, someone who writes that they sympathize with ISIS’s foreign policy goals, someone who “likes” an ISIS Facebook page? How about a page dedicated to a mass murderer? Does it matter whether that murderer’s name is James Holmes or Abu Bakr al-Baghdadi? These are not simple decisions. Imagine the pressure of a government mandate on Facebook’s censors. There’s only one option, really—to report it all. Asking non-experts to help build a massive and meaningless haystack of offensive speech isn’t a great counter-terrorism strategy if we ever need to find a needle in a hurry.

More important, it would be terrible for political speech. Speech *supporting* terrorism lives across a razor-thin margin from speech *about* terrorism, foreign policy, drones, the Middle East and Islam. The idea that speaking to such controversial and important policy issues might get you swept into a government dragnet would be enough to chill many from engaging in the sort of speech that’s at the heart of the First Amendment.

These concerns aren’t merely theoretical. Private companies have a history of censoring speech for reasons that turn out to be misguided. For example, Apple voluntarily blocked applications that permitted users to identify sites of U.S. drone strikes for including “objectionable material.” Drone strikes are certainly objectionable. But providing information about our own government’s actions is emphatically *not*; our democracy functions best with public oversight and accountability. Apple’s decision wrongly cut off access to information critical to a foreign policy debate of immense public concern.

Finally, censoring and monitoring social media speech simply isn’t an *effective* remedy for radicalization. Social media companies are not omniscient—they do not and cannot monitor every bit of speech that is posted on their networks. Even when social media companies are determined to shut down particular speakers or accounts, those speakers can often circumvent the rules and open new accounts faster than companies can keep up. Shutting down the accounts of terrorist organizations would actually deprive the government of an important source of intelligence. And it would certainly deprive Americans of the ability to see and challenge the views of terrorist organizations—without any demonstrable upshot.

It is a grave mistake to expect or require private social media companies to act as arms of the national security state, just as it is a grave mistake to scapegoat the Internet for laying bare the darkest thoughts of the soul. The Internet is made up of ones and zeros. It does not organically create hate. The hate is, sadly, in our human minds and human hearts. Denying that won’t get us anywhere in the battle for winning those hearts and minds — but sunlight will. For hundreds of years, we’ve been a nation that is determined to stay safe *and* free, to hew closely to our values even in times of war, fear, and terror.

So, politicians: don’t blame the medium for the message. Especially when the medium—the Internet—may be the greatest asset we have in the fight against terror.