

Blocking social networks after terrorist attacks can do more harm than good



Imagine for a moment that you run a small country prone to outbreaks of sectarian violence. Terrorist attacks hit a series of churches and hotels in your country on a major religious holiday, prompting fears that violence will spread. Your citizens are using social networks to get in touch with their loved ones and you coordinate disaster response efforts – but they also appear to be using those same networks to plan further violence. It's your job to bring the situation under control in a way that balance speech rights with safety. Do you leave Facebook online, or do you shut it off?

That was the dilemma faced by Sri Lanka on Easter Sunday, when at least 290 people died in a series of bombings. The government decided to take the more restrictive approach: it blocked access to Facebook, Facebook Messenger, Instagram, WhatsApp, Viber, and YouTube. It was the second time in as many years that Sri Lanka temporarily blocked access to social

media sites. (Last year, it came in response to anti-Muslim violence.)

To some observers, the shutdown was a welcome move. Kara Swisher writes in the *New York Times*:

It pains me as a journalist, and someone who once believed that a worldwide communications medium would herald more tolerance, to admit this – to say that my first instinct was to turn it all off. But it has become clear to me with every incident that the greatest experiment in human interaction in the history of the world continues to fail in ever more dangerous ways.

In short: Stop the Facebook/YouTube/Twitter world – we want to get off.

But two questions present themselves whenever a government acts to restrict speech in this way. First, who will be harmed by the unexpected breakdown in communication infrastructure? And second, does it even solve the problem you want it to?

We're still in the immediate aftermath of the Sri Lanka attacks, so it's very difficult to say who may have been harmed by the social media ban. We often hear that in some developing nations, Facebook is synonymous with the internet itself. The company also makes tools designed to help disaster victims coordinate their response, including its safety check feature. For families who primarily communicate using Facebook's infrastructure, a service interruption can introduce more chaos into an already fraught day.

Moreover, social media gained popularity in Sri Lanka and elsewhere because it was more trustworthy than official government sources. As Megha Rajagopalan reported in *BuzzFeed*, Sri Lankans have good reason to doubt official sources of information:

For one thing, the country has a long history of heavy-handed media controls, and journalists have routinely faced violence and intimidation over their work. This means many Sri Lankans rely on social media for up-to-date information, including posts that debunk false claims circulated on both social and traditional media.

Pressure on journalists had somewhat let up since President Maithripala Sirisena entered office in 2015. But when a constitutional crisis broke out last fall, supporters of the country's former president, Mahinda Rajapaksa, seized control of state newspapers and stormed the offices of a state-owned TV station, temporarily forcing them off the air.

It's clear that extremists really have been using social networks to spread misinformation in the wake of the attack. It's also clear that Sri Lanka's government has itself been an unreliable narrator over the years.

But say you've made peace with the government blocking access to Facebook and its peers. Will that stop the spread of misinformation? But say you've made peace with the government blocking access to Facebook and its peers. Will that stop the spread of misinformation? There's reason for doubt. Last year, the *Times* reported that Sri Lanka's previous social media ban was easily circumvented:

One official estimated that nearly three million users in Sri Lanka continued accessing social media via Virtual Private Networks, which connect to the internet from outside the country.

Yudhanjaya Wijeratne, a Sri Lankan researcher and author, did a forensic analysis of the blockade and told *BuzzFeed's* Jane Lytvynenko that it was largely ineffective.

Wijeratne studied over 60,000 Facebook posts to understand

whether a social media block imposed by the government in 2018 was effective. Ultimately, he found that it wasn't.

"Not only did people circumvent it in a flash, anecdotal evidence suggests it did significant damage to tourism and e-commerce, both of which rely on Facebook ads," he said.

None of this is to suggest that social networks deserve the benefit of the doubt. Last April, civil society groups in Sri Lanka wrote an open letter to Facebook CEO Mark Zuckerberg outlining the company's failure to enforce its own community standards in the country, a likely consequence of hiring too few moderators who speak Sinhala, one of Sri Lanka's native languages.

But we ought to be wary of dramatic "solutions" that have no clear benefit. Instead of intermittently blocking access to social networks, Sri Lanka could always try ... regulating them? Develop standards around the identification and removal of harmful content, and hold companies accountable to them, the way Europe is now doing. Or, if you're worried that regulation will simply entrench incumbents, then take antitrust action that promotes competition. Both moves would likely do more to promote trust between the government and its citizens than simply shutting off Facebook whenever some cabinet minister gets nervous. (My colleagues Adi Robertson and Makena Kelly will have more to say soon about how groups can advocate government internet shutdowns.)

If the current US government blocked all access to social networks after a terrorist attack, we would rail against the move as an authoritarian outrage. When other countries do it, we ought to be just as suspicious.

Democracy

Facebook's new chief lawyer helped write the Patriot Act

Russell Brandom introduces us to Jennifer Newstead, a Trump appointee who served in the Justice Department under President Bush and who will soon be taking over as general counsel of Facebook:

As The Hill points out, a 2002 Justice Department press release describes her as “helping craft” the legislation. Notorious Bush administration lawyer John Yoo described her as the “day-to-day manager of the Patriot Act in Congress” in his 2006 book.

Passed in the wake of the 9/11 attacks, the Patriot Act greatly expanded the scope of the government’s surveillance powers, enabling new techniques like roving wiretaps and so-called “sneak-and-peek” warrants. Section 215 of the Patriot Act was used to justify the bulk collection of telephone records from US carriers, although both the ruling and the legal interpretation that justified it remained secret until the Snowden leaks.

After Social Media Bans, Militant Groups Found Ways to Remain

Sheera Frenkel and Ben Hubbard explore how Hezbollah and other extremist groups manage to stay on social platforms after getting banned:

Hamas and Hezbollah, in particular, have evolved by getting their supporters to publish images and videos that deliver their message – but that do not set off the alarm bells of the social media platforms. Today, the groups mostly post images of festive parades and religious celebrations online, as well as videos of speeches by their leaders.

That has allowed Hamas and Hezbollah, as well as groups like the East African-based Shabab, to proliferate largely unchecked on social media, even as a clampdown by Facebook and others has neutered the online presences of the terror organizations that are the most threatening to the West – the

Islamic State and Al Qaeda.

How WhatsApp, FaceTime and other encryption apps shaped the outcome of the Mueller report

Craig Timberg and Drew Harwell have a piece on how the special counsel's investigation was made more difficult by encrypted messaging apps that serves as a nice preview of something we are going to be talking about a lot as Facebook pivots to privacy:

Special counsel Robert S. Mueller III detailed multiple contacts among Russian operatives and associates of President Trump in the report made public Thursday. But Mueller repeatedly also lamented what he couldn't learn – because encrypted communications had put key conversations beyond his reach.

“The Office learned that some of the individuals we interviewed or whose conduct we investigated – including some associated with the Trump Campaign – deleted relevant communications or communicated during the relevant period using applications that feature encryption or that do not provide for long-term retention of data or communications records,” Mueller wrote in his executive summary.

36 Days After Christchurch, Terrorist Attack Videos Are Still on Facebook

Joseph Cox finds footage of the New Zealand attacks on Facebook – but it seems that in every case here, the footage was modified in an effort to evade detection.

Some of the videos, which are slices of the original 17 minute clip, are trimmed down to one minute or so chunks, and are open to be viewed by anyone. In one instance, instead of removing the video, which shows the terrorist shooting and murdering innocent civilians from a first-person perspective,

Facebook has simply marked the clip as potentially containing “violent or graphic content.” A video with that tag requires Facebook users to click a confirmation that they wish to view the footage.

How Facebook Fights Fake News in the World’s Largest Election

Saritha Rai profiles Boom, one of the third-party fact-checkers fighting misinformation in India ahead of its election this year:

A visit to Boom’s offices makes clear that the scale of Facebook’s response in India so far isn’t enough. The small team appears capable and hardworking almost to a fault, but given the scale of the problem, they might as well be sifting grains of sand from a toxic beach. “What can 11 people do,” says Boom Deputy Editor Karen Rebelo, “when hundreds of millions of first-time smartphone-internet users avidly share every suspect video and fake tidbit that comes their way?” Her team has been working for Facebook since a regional election last summer, and work related to the present election escalated earlier this year.

Federal investigation of Facebook could hold Mark Zuckerberg accountable on privacy, sources say

Tony Romm says the Federal Trade Commission might fine the Facebook CEO:

In past investigations of Facebook, the U.S. government opted to spare Zuckerberg from the most onerous scrutiny. Documents obtained from the FTC under federal open-records laws reflect that the agency considered, then backed down from putting Zuckerberg directly under order during its last settlement with Facebook in 2011. Had it done so, Zuckerberg could have faced fines for future privacy violations.

The Antitrust Case Against Facebook: a turning point in the debate over Big Tech and monopoly

Cory Doctorow writes about a new paper from Dina Srinivasan arguing that Facebook's data-collection practices grew more intense and user-hostile as its competitors in the marketplace diminished:

*Srinivasan's history of Facebook's surveillance rollout makes link between monopoly and surveillance clear. For its first ten years, Facebook sold itself as the pro-privacy alternative to systems like Myspace, Orkut, and other competitors, repeatedly promising that it wouldn't track or analyze its users activity. As each of Facebook's competitors disappeared, Facebook advanced its surveillance technology, often running up against user resistance. But as the number Facebook alternatives could go declined – because Facebook crushed them or bought them – Facebook's surveillance became more aggressive. Today, with Facebook as the sole dominant social network, people who leave Facebook **end up joining Instagram**, a Facebook subsidiary.*

So there's plenty of reason to think that Facebook's surveillance could be disciplined by competition. After all, Facebook's sole credible competitor is Snapchat: a company whose main value pitch is its privacy enhancements.

Stock Images of Beautiful Women and Border Wall Propaganda: The Trump Campaign's Facebook Ad Strategy

Pema Levy browses through the president's Facebook ads:

The numbers tell a story of a campaign investing heavily in Facebook, a platform where it can reach millions of voters and—just as important in this early stage of the race—test the performance of its ads. At the time of writing, the campaign and its associated fundraising committee have spent \$11,326,128 on 196,352 ads in just under a year.

That comes to less than \$58 per ad. The reason is that different iterations of the same content count as distinct ads. Many of the ads run for just a day and are identical or nearly identical to others. (Reporter Judd Legum, in his newsletter Popular Information, counted 217 ads asking supporters to wish Melania Trump a happy birthday later this month.)

EU tells Facebook's Nick Clegg to rethink ad rules for elections

In an effort to blunt the impact of foreign interference on elections, Facebook now requires advertisers in the European Union and elsewhere to register in the countries where they operate. The EU worries this will make some kinds of political advertising impossible. And for some reason the *Guardian* writes about this as if it's an embarrassment to global policy chief Nick Clegg. I don't get it.

China Bans the Word 'Leica' on Social Media

Beijing *really* doesn't like it when brands reference Tiananmen Square:

When a promotional video for German camera maker Leica hit the web this week, it looked like a bold statement about the hard work done by photojournalists around the world. But the company is now distancing itself from the 5-minute video after Chinese social media users cried foul and the word "Leica" was banned on social media site Weibo. The problem? The dramatic video is set in 1989 during the Tiananmen Square pro-democracy protests that are forbidden to talk about in China.

The video, titled "The Hunt," is a fictionalized montage of various conflict areas around the world. Its most controversial sequence shows an English-speaking photojournalist scrambling to find his camera and being

questioned by Chinese authorities.

Elsewhere

Silicon Valley Came to Kansas Schools. That Started a Rebellion.

Nellie Bowles writes about the latest school district to challenge the personalized learning software built by Facebook engineers. (New York wrote about a similar uprising in Connecticut last year.)

Many families in the Kansas towns, which have grappled with underfunded public schools and deteriorating test scores, initially embraced the change. Under Summit's program, students spend much of the day on their laptops and go online for lesson plans and quizzes, which they complete at their own pace. Teachers assist students with the work, hold mentoring sessions and lead special projects. The system is free to schools. The laptops are typically bought separately.

Then, students started coming home with headaches and hand cramps. Some said they felt more anxious. One child began having a recurrence of seizures. Another asked to bring her dad's hunting earmuffs to class to block out classmates because work was now done largely alone.

What it's like to be a female founder in the Instagram era

It's very stressful, Carrie Battan writes, but can also be a good fundraising tool:

Even when Instagram is being used to spread an empowering message, certain stereotypes are perpetuated. Often, female entrepreneurs must traffic in self-deprecation, conveying "a little bit of relatability," says cultural critic and brand strategist Aminatou Sow, cofounder of the popular Call Your

Girlfriend podcast. She has noticed that while male CEOs seem comfortable posting selfies taken aboard private jets, women tend to relegate posts that reveal their newfound lavish lifestyles to private accounts, or forgo them altogether. Outdoor Voices' Haney says she's conscious of not appearing too "daunting" on social media and avoids flaunting her success.

Launches

Byte, the follow-up app from Vine co-creator Dom Hofmann, is out in beta and he shared a preview on Twitter.

*the byte beta we've been running with friends and family *feels* exactly like the vine friends and family beta, down to the weird but appealing randomness of the videos. that'll change as we expand, but it's a pretty good sign*
pic.twitter.com/rBbQrNtTJ7

— dom hofmann (@dhof) April 22, 2019

Takes

"I, too, am Contrarian"

Alex Danco, who is one of my favorite Silicon Valley thinkers, bids farewell to the venture firm where he worked with a very funny post about how everyone tries to be "contrarian" on Twitter:

(As an aside; Silicon Valley is supposed to be somewhere where people think freely. You know what a place where people think freely looks like? It looks like somewhere with a cheap art scene; with a lot of musicians; somewhere where young people hang around and cause minor problems. It looks like what San Francisco used to be, for sure. But San Francisco

nowadays more closely resembles something like the TV show The Good Place.)

And finally ...

The CIA is joining Instagram

Instagram is no longer missing the one thing it was obviously missing, Makena Kelly reports:

An Instagram spokesperson told The Verge on Monday, "Our team worked with the CIA, as they do with many partners, to provide best practices and guidance when it comes to launching an Instagram account."

I'll throw in a couple. **Do:** enable two-factor authentication. **Do not:** send people your stories individually if you already posted them to your public story. Thanks in advance!

Talk to me

Send me tips, comments, questions, and ideas for what the CIA can do on Instagram. I mean *other* than surveilling all of us in real time: casey@theverge.com.

<https://www.theverge.com/interface/2019/4/23/18511812/sri-lanka-facebook-ban-easter-bombings-social-networks>