Five Excuses Governments (Ab)use to Justify Internet Shutdowns

By Deniz Duru Aydin

Global Research, November 07, 2016

Access Now 6 October 2016

Theme: Police State & Civil Rights

Together with more than 100 organizations around the world in our #KeepItOn campaign, Access Now is fighting to keep internet shutdowns from becoming the new norm. Today, we're participating in a talk at the Brookings Institution about how this dangerous, rights-harming practice impacts local economies (connect to the live webcast here).

Another way we're fighting shutdowns is by documenting the justifications governments use to carry out shutdowns and impose blanket restrictions on platforms for expression. Orders to block, throttle, or disrupt communications networks almost always fail to comply with local law. They also face growing international condemnation as an interference with human rights that's not justified even in times of conflict.

Here's a look at what governments say, versus how internet shutdowns truly affect people.

1.) National security

What the government says: It's for "national security"

National security may be the most frequently cited justification for internet shutdowns globally. It's also the broadest and most vague. In Pakistan, the government has made localized mobile network shutdowns justified on these grounds a standard practice, cutting people off from the network during Islamic holidays such as the day of Ashura, while citing concern about terrorist attacks. Orders for the shutdowns are meant to cover a relatively small area, but it usually becomes necessary to "shut down a wider area than specified, to ensure there is no 'spillover' of service," according to the Institute for Human Rights and Business. This means that the majority of mobile internet users in Pakistan are often affected. State authorities have also cut off the internet for "security" during a wrestling event and Independence Day celebrations. In Turkey, during the *coup d'etat* attempt in July 2016, social media sites were throttled.

What really happens

Shutdowns imposed in the name of "national security" have the opposite effect on the people cut off from communications platforms and online resources. People don't feel "secure" or safe when they can't figure out what's going on, can't get access to important news or reach emergency services, and can't check in on their loved ones.

2.) Elections

What the government says: It's to fight election "fraud" or stop the spread of

"misinformation"

Shutting down the internet or otherwise controlling the free flow of information online during an election period is a profound violation of human rights and a threat to democratic processes and government legitimacy.

Fighting shutdowns during elections is part of Access Now's DNA. When the government ordered a disruption in Iran during the 2009 elections, it convinced a small group of activists and technologists to found our organization. Sadly, Iran is far from alone in this practice. In 2010, Myanmar repeatedly shut down the internet in the months surrounding its first elections in 20 years. In October of last year in India, the government used local elections to justify a day-long shutdown in Garo Hills region.

Worryingly, there has been a series of shutdowns during or around elections over the past two years in countries in East and West Africa, with governments disrupting the internet, cutting access to social media, or carrying out full blackouts in Chad, Togo, the DRC, Congo-Brazzaville, and Uganda. Citizens are fighting back. In Uganda, when the government blocked Facebook, Twitter, and WhatsApp on election day, people circumvented the blocks using VPNs and other circumvention technologies, making the government's crackdown on free expression less effective. Yet as a result, we estimate that the mobile banking sector — a popular form of exchanging money — lost $23 million per day over a weekend.

At Access Now, we're continuing to fight this trend through the #KeepitOn campaign, and we're starting to see progress in Africa. Civil society won a hugely important victory when the president of Ghana told voters that the government has no intention of shutting down social media on election day, even though the police had been openly considering it.

What really happens

Shutdowns prevent journalists, election monitors, and ordinary citizens from reporting fraud or irregularities at polling places. Opposition candidates and parties cannot communicate with supporters or expose and document illegal activity.

3.) Protests

What the government says: It's to keep citizens "safe" or "restore order"

Governments that want to quell dissent or stop protests use internet shutdowns as an extreme form of censorship, often while claiming that they are working to restore order or keep people safe. Many governments did not learn from Egypt's experience in 2011, when its internet blackout drove more people into the streets. Countries that have used shutdowns to control information during protests include:

> Bahrain, Cameroon, Chad, Democratic Republic of Congo, India, Iran, Kazakhstan, Libya, Mali, Myanmar, Sudan, Syria, Uganda, the United States, and Venezuela.

From A to Z, these countries are blocking services or conducting full network shutdowns, with rationales such as "stopping the rumors" (in India) to the classic "ensuring public safety."

What really happens

A violent protest might theoretically justify extraordinary security measures, but imposing internet blackouts when people are protesting doesn't increase safety. It stops important information from reaching citizens — like how to find areas of safety or contact emergency services. It also prevents people from documenting human rights violations such as the disproportionate use of force by the police or military.

4.) School exams

What the government says: It's to stop cheating on exams

An increasingly popular form of shutdown is one aimed at stopping students from cheating on exams. The first one that we're aware of happened two years ago in Uzbekistan during university entrance exams. At the time, the government did not admit that school exams were the reason for the shutdown, instead citing "urgent maintenance work on telecommunications networks."

After that, in June 2015, Iraq shut down the internet for national exams, and did so again one year later. This year, a full-blown trend emerged, with governments in India, Algeria, Ethiopia, and Iraq each turning off communications networks during national exams.

What really happens

This type of shutdown is a clearly disproportionate practice, impacting the free expression rights of millions of people to stop cheating by a few students — who might nevertheless develop other ways to cheat.

5.) Visits by government officials

What the government says: It's to keep the dignitaries safe.

Governments sometimes see a national security risk when government officials or foreign political leaders are visiting, and use the risk to justify shutting down the internet. One of the earliest examples we're aware of took place three years ago in Pakistan when the government ordered a disruption during the visit of the Chinese Premier Li Keqiang.

More recently, authorities in the Indian state of Jammu and Kashmir blocked mobile internet during Prime Minister Modi's visit to the Kashmir Valley. The people of Kashmir have experienced more shutdowns than those living in any other state in India, but this may have been the first time justification was tied to a high-profile visitor.

Similarly, in the Philippines, the only shutdown we recorded took place last year during a visit by Pope Francis. It was supposed to be a targeted disruption of the area along the Pope's travel route, but other areas were impacted to prevent spillover of signals. And in May, the Vietnamese government blocked Facebook when U.S. President Obama visited.

What really happens

Disruptions like these interfere with our right to receive and impart information, a right that is not suspended when dignitaries visit. And the rationale is questionable. In Vietnam, for

instance, did the government impose a shutdown for "national security," or to censor news about the protests that were happening at the time?

How we can fight back

As these examples show, countries use a variety of rationales for internet shutdowns, and depend upon different laws to legally justify those reasons. In some cases, what makes the difference for whether an internet shutdown will be implemented is the licensing requirements between a government and a telecommunications company. These requirements can create "excessive intermediary liability," where a company is compelled to comply with shutdown orders even when they are extralegal. Yet push-back remains possible, through industry-led coalitions like the Global Network Initiative, and by appealing to national parliaments and other institutions.

A key victory on the international front came when the United Nations passed a resolution in June 2016 that specifically condemns internet shutdowns. This demonstrates the growing global consensus that internet shutdowns are a human rights violation that cannot be justified even in times of conflict. It is now up to us to help establish new norms and laws that disallow shutdowns regardless of rationale, with the support of civil society, industry, academia, and individual internet users from all around the world.

As we note above, there are now more than 100 organizations that back our #KeepItOn campaign to fight internet shutdowns. You can pitch in by joining our pledge here and, if you represent an organization, you can sign up at

https://www.accessnow.org/keepiton.

And if you personally experience a shutdown or hear about one, you can report it by emailing us at shutdowns@accessnow.org.

The original source of this article is Access Now
Copyright © Deniz Duru Aydin, Access Now, 2016

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Deniz Duru Aydin

For media inquiries: publications@globalresearch.ca