Understanding Internet Censorship in Democracies

Jillian C. York, Director for International Freedom of Expression, Electronic Frontier Foundation

The idea of two competing visions for the internet—an authoritarian one and a democratic one—has persisted since the early days of the web. Indeed, the internet in Western democracies was, initially, somewhat of a wild west in which anything was possible—including, of course, some of society's worst ills. At the same time, some of the world's most authoritarian states—including China, Saudi Arabia, Tunisia, and Turkmenistan—had early on implemented measures to block any offending material, including dissent, information on human rights violations in their countries, religion, and more.

But not every authoritarian state engaged in such practices, nor did every Western democracy last for very long without trying to regulate the internet—often in deeply troubling ways. The original version of the US Communications Decency Act, signed into law by then-President Bill Clinton, is one example; the law was quickly deemed unconstitutional. The Digital Millennium Copyright Act of 1998 (still in effect) gave sweeping rights to copyright holders to demand the removal of copyrighted materials—even if those materials are not infringing on their intellectual property. Abuse of these rights by corporations and states alike is well-documented.

Over time, the lines between these supposed models blurred considerably, as corporate actors became more integral to the operations of the internet and the web. The declarations of Western states as protectors and promoters of a free and open internet fall flat in the face of ever-increasing regulations created without much (or any) input from civil society actors; regulations that are all too often copied by less democratic nations, which point to the practices of the US and Europe to justify their actions.

A Brief History

When, on January 27, 2011, the Egyptian government made the decision to shut down the internet, something shifted. In the years immediately prior, the internet had been celebrated by academics and the media as a liberating force. The internet—and particularly social media—was described in popular media as being able to bring about major social change, and perhaps even democracy.

The 2009 protests in Iran triggered a wave of support from US tech companies, including Twitter (which openly supported the movement by delaying planned maintenance so that Iranians could keep tweeting) and Google, which hosted a 2010 conference at Budapest's Central European University entitled "Internet at Liberty" that brought together companies, activists, and academics for two days of open discussions about internet freedom.

The movement also prompted declarations of support for internet freedom from the US government. Then-Secretary of State Hillary Clinton presciently referred to information networks in her 2010 remarks on Internet freedom as "a new nervous system for our planet" and declared the Obama administration's support for internet freedom, further calling on the public and industry to make information technologies "a force for real progress the world over."

And yet, just one year and six days later, foreign technology companies operating in Egypt heeded the call from then-President Hosni Mubarak to cut off connectivity to the nation's citizens amidst unprecedented protests, in an attempt to take away their ability to communicate with one another and the outside world. The effort failed—Mubarak stepped down less than two weeks later—but the action laid bare the fragility of Clinton's conception of internet freedom.

Here, it is important to note that those companies—including France Telecom (which owned Egyptian operator Mobinil), Orange, and Vodafone—defended their actions on the basis that they were simply following orders. Vodafone issued a statement saying that "Under Egyptian legislation, the authorities have the right to issue such an order and we are obliged to comply with it. The Egyptian authorities will be clarifying the situation in due course."

Egypt's internet shutdown was by no means the first. The governments of Myanmar, Maldives, and Nepal had all cut off access in the past by flipping a "kill switch"; that is, those countries' internet connections were more centralized, allowing greater government control. Egypt's more decentralized networks therefore required complicity from tech firms, including Vodafone. Although some companies—such as Twitter, which enabled its Speak2Tweet service to circumvent the shutdown—offered support to the revolution, the shutdown ultimately brought about a new awareness of the ways in which tech companies could be drafted to aid with internet censorship.

Opening up a Pandora's Box

In 2011, internet censorship was by no means a new phenomenon. In addition to the aforementioned internet shutdowns, numerous governments had employed a variety of techniques to censor information, from blocking websites to limiting search results. From Tunisia to China, Turkmenistan to Cuba, restrictions on access to information and communication had been the norm since the emergence of the world wide web.

Neither was collaboration between tech companies and governments new—rather, it was simply less apparent, as corporations sought to hide their complicity with authoritarian governments. But in 2008, a leak from US company Cisco showed that the company had worked with China on a custom censorship regime known widely as the "Great Firewall" in an effort to sell more routers.

Cisco's cynical ploy could have served as a warning, but instead it opened a Pandora's box. Governments quickly became aware that they could manipulate tech companies into removing content for them, thus making censorship and surveillance easier to implement. For instance, whereas previously governments seeking to block certain social content on Facebook or YouTube had to do so on their own, those companies soon realized that they could preserve the majority of their site's contents in a given country by participating directly in the censorship; that is, by removing offending content themselves or geo-locationally blocking it from a given jurisdiction.

This practice has since become the global norm; rather than block websites outright, most governments rely on cooperation with corporations, either issuing legal takedown orders or forming alliances with companies, most of which are all too happy to comply in order to remain active in as many locales as possible.

Corporate Controls

A decade ago, the methods used by governments to censor the internet were few: States could block individual websites, limit keywords from search results, tamper with the domain name system (routing internet traffic to a given site to a new destination), or block IP addresses (a technique that often comes with unintended consequences). Website blocking was by far the preferred method of most states; while democratic nations would typically limit blocking to illegal content (such as child sexual abuse imagery (CSAM) or gambling websites), more authoritarian states could use the technique to block anything they found undesirable. For instance, while Sweden maintained a blocklist of around 1,000 websites containing CSAM, Tunisia famously applied all four methods to limit access to information on human rights, and censor the country's active blogosphere, among other things.

Today, it is far more common for states to engage directly with companies, either by issuing legal (or not-so-legal) orders, or by striking deals to gain "trusted flagger" status, thus enabling them to directly report content for takedown through a designated escalations channel. These systems are rife with abuse; one recent example involved London's Metropolitan Police using their direct connection to YouTube to remove music videos.

In addition to one-off legal orders, a number of states have, over the past decade, enacted laws designed to censor or limit certain content. In the Middle East and North Africa, cybercrime-style laws are popularly used to stifle online expression. In Europe, notice-and-takedown laws have gained popularity in recent years.

But while such laws as Germany's Network Enforcement Act—designed to allow German authorities to be able to get illegal content removed in a short timeframe and without the onerous requirement of a court order—may be acceptable for limiting illegal speech in a democratic context, when exported or copied by less democratic states, they become censorial. For instance, Turkey's ever-increasing autocratic government passed a law that directly referenced Germany's; the law does not stop at the removal of illegal content, however. It also gives broad power to courts to throttle internet access and can be used to force platforms to remove content that violates the vague categories of "personal rights" and the "privacy of personal life."

Another recent, troubling trend is demonstrated by the UK's Online Harms Bill, which seeks to create a category of legal but harmful content that can be removed under the law. Put frankly, this Orwellian category allows the state to circumvent their own legal processes (and in some cases, their constitution) by designating certain speech as "harmful" when it cannot for whatever reason be outlawed. Similar laws have been proposed in Australia and Canada and are sure to be copied by other states.

When states rely on companies to restrict speech—whether by court order, law, backroom deal, or other private pressure—the process is almost never transparent. Although most companies issue transparency reports, they are often vague and rarely contain details of the content removed, the specific method used to remove it, or the government body which issued the mandate.

Furthermore, in an effort to save money, companies are increasingly reliant on automated systems to remove offending speech. These systems are entirely opaque; only the programmers can see inside the so-called “black box,” and users whose content is removed by automated technology under certain categories—such as “terrorist” content—are barred from appealing those decisions.

All of these various systems are used by democratic and authoritarian states alike, thus blurring the lines between a democratic and authoritarian model of the internet. The very idea that authoritarian and democratic nations have strongly conflicting ideas of the internet is an outdated one. Democratic nations act as censors, too; they simply have different ideas of what should be censored. And when they rely upon companies to do their bidding, the democratic protections that otherwise might have existed fall by the wayside.

This may sound hopeless, but it needn’t be. If democratic states are still interested in preserving and promoting a democratic model of the internet, it is incumbent on them to recognize the global nature of the web and set a positive example for the rest of the world by not passing regulations that allow them to sidestep their commitments to free expression. Furthermore, states should act to ensure that tech companies are fair, equitable, transparent, and committed to human rights.