Rebecca MacKinnon
Co-Founder, Global Voices Online
Director, Ranking Digital Rights at New America

Testimony to the House Committee on Foreign Affairs
Subcommittee on Terrorism, Nonproliferation, and Trade

"The Evolution of Terrorist Propaganda: The Paris Attack and Social Media"

January 27, 2015

The democratic world faces a serious challenge: how to fight terrorism and violent extremism in the Internet age while not undermining the core principles and freedoms of democratic and open societies.

Yesterday I returned from the Philippines where I participated in a conference of bloggers, activists, and citizen journalists from all over the world. Many members of this community face serious threats not only to their freedom of speech but also to their physical freedom. While some have been kidnapped or threatened by terrorists or religious extremists, many more are imprisoned and threatened by governments who have labeled them terrorists – not because they actually are terrorists under definitions that people in this hearing room would use, but because they have expressed views or reported facts that their governments find threatening.[1]

For example, in Ethiopia a group of bloggers and investigative journalists known as the "zone nine bloggers" are currently on trial for terrorism under a law that has frequently been used to silence journalists.[2] Last year the Russian parliament amended its anti-terror laws to include a set of draconian Internet controls that justify the jailing of opposition bloggers and activists, and require companies to keep data of Russian users in Russia so that they can be better surveilled.[3] In Turkey, the government has

[1] http://advocacy.globalvoicesonline.org/2015/01/24/global-voices-calls-for-immediate-release-of-jailed-online-media-workers-and-activists/
[2] http://www.voanews.com/content/court-adjourns-ethiopian-blogger-trial-15-times/2586428.html
[3] https://cpj.org/blog/2014/07/russia-intensifies-restrictions-on-blogs-social-me.php; https://www.aei.org/wp-content/uploads/2015/01/Internet-freedom-in-Putins-Russia.pdf

prosecuted journalists for “praising of violence and terrorist propaganda.” However an investigation by the Committee to Protect Journalists found that “Turkish authorities conflated the coverage of banned groups and the investigation of sensitive topics with outright terrorism or other anti-state activity.”[4] Last year Amnesty International reported that the Moroccan government uses anti-terror laws to target journalists.[5] Egypt has recently made similar use of anti-terror laws.[6]

In response to the tragic Charlie Hebdo massacre in Paris, last week the French government called for UN member states to work together on an international legal framework that would place greater responsibility on social networks and other Internet platforms for terrorist use of their services.[7]

In addressing the problem of terrorist use of social networking platforms, the United States and all other stakeholders committed to upholding international human rights norms, as well as a free and open global Internet, should adhere to the following principles:

1. Multi-stakeholder policymaking

Note that the countries mentioned above that abuse anti-terror laws to jail activists and journalists are all UN member states - along with a long list of other nations including China, Venezuela, and others whose definitions of terrorism are elastic enough to be used to keep incumbent regimes in power. The US has opposed UN control over Internet governance because a large number of UN member states seek a governance framework that would result in a global Internet that is much less free and open than it is today – for commerce and innovation as well as for political discourse. Instead the US supports a multi-stakeholder approach to Internet governance that includes industry, civil society, and the technical community alongside governments in processes that set policies and standards for the global Internet. Any international effort to address terrorism on the Internet should also be grounded in a robust multi-

[4] http://cpj.org/2013/02/attacks-on-the-press-misusing-terror-laws.php
[5] http://www.amnesty.org/en/for-media/press-releases/morocco-stop-using-terrorism-pretext-imprison-journalists-2014-05-20
[6] http://www.poynter.org/news/mediawire/250100/mediawireworld-3-journalists-in-egyptian-court-on-world-press-freedom-day/
[7] http://www.reuters.com/article/2015/01/22/us-france-security-internet-idUSKBN0KV2EK20150122

stakeholder approach to ensure that any solutions are compatible with innovation, the free flow of information, and universal human rights.

2. Human rights assessment of laws, regulations, and policies

Any national level laws, regulations, or policies aimed at fighting online terrorism (or any potential regulation affecting online speech or privacy for that matter) should undergo assessment, carried out in consultation with human rights experts and representatives of groups whose rights are potentially at risk of being violated, to identify any ways in which the new measures could have negative consequences for journalism, activism, and the free flow of information more broadly. Policies and laws should not be enacted without robust checks and balances, or if proponents cannot demonstrate how human rights risks will be mitigated.

Laws and regulations governing company actions should be vetted to ensure that they do not compel companies to violate core principles of freedom of expression and privacy, grounded in international human rights standards. Several major US-based Internet companies have made commitments under the multi-stakeholder Global Network Initiative to respect users' freedom of expression and privacy in a number of specific ways. These commitments include: narrowly interpreting government demands to restrict content or grant access to user data or communications; challenging government requests that lack a clear user basis; transparency with users about the types of government requests received and the extent to which the company complies; restricting compliance to the online domains over which the requesting government actually has jurisdiction.[8]

3. Limited intermediary liability.

A large body of research conducted around the world by human rights experts and legal scholars shows clear evidence that when companies are held liable for users' speech and activity, violations of free expression and privacy can be expected to occur for a number of reasons. Companies operating under strict or strong liability regimes generally over-censor in

[8] Global Network Initiative Principles: https://globalnetworkinitiative.org//principles/index.php; and Implementation Guidelines: https://globalnetworkinitiative.org//implementationguidelines/index.php

order to avoid legal and regulatory repercussions to their business. Strong liability regimes have also been shown to increase the likelihood that companies will comply with spurious demands for content removal made by governments as well as private parties in order to play it safe: there is no penalty for over-censoring while the legal consequences of under-censoring can be severe.[9] Limited liability for Internet intermediaries is an important prerequisite for keeping the Internet open and free.

4. Transparency, accountability, and stakeholder engagement in the development and enforcement of companies' Terms of Service and other forms of self-regulation.

In response to outreach from counter-terrorism authorities among others, some social networking companies are using their terms of service, community guidelines, and other self-regulatory mechanisms to shut down accounts and delete content that is technically protected by the first amendment, or whose removal has not been sought by any government or court through any formal legal process or mechanism. While this may have helped to prevent acts of violent extremism by terrorist groups, there are also many documented cases in which such self-regulation has resulted in censorship of activists, journalists, and political opposition groups. For example last year the SecDev Foundation, a Canadian non-profit that works with digital activists around the world, compiled a list of moderate Syrian opposition groups and citizen journalists whose Facebook pages had been shut down.[10]

More broadly, Facebook has come under fire from activists for enforcing its community guidelines in a way that sometimes silences voices and information that have few other outlets. For example, at the end of last year three Tibetans burned themselves alive to protest Chinese rule. Self-immolation is a gruesome but long-standing form of political protest in

[9] Selected sources: *Shielding the Messengers: Protecting Platforms for Expression and Innovation.* Center for Democracy and Technology. December 2012. https://cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf; *Closing the Gap: Indian Online Intermediaries and a Liability System not Fit for Purpose.* March 2014. https://globalnetworkinitiative.org//sites/default/files/Closing%20the%20Gap%20-%20Copenhagen%20Economics_March%202014_0.pdf; *Fostering Freedom Online: The Role of Internet Intermediaries.* UNESCO. December, 2014 http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

[10] http://www.theatlantic.com/international/archive/2014/02/the-syrian-opposition-is-disappearing-from-facebook/283562/

Buddhist societies. The Chinese government censors news of Tibetan protests generally and self immolations in particular. Facebook has deleted postings by Tibetan activists about the recent self-immolations, citing policies forbidding excessively graphic content. Facebook insists that enforcement of its own policies has nothing to do with the Chinese government.[11] While I am inclined to believe them in this case, the point is that *de facto* political censorship can happen – whether companies intend it or not – when companies lack sufficient mechanisms to ensure transparency about their policies and enforcement practices, and when their policies are developed and implemented without impact assessment or engagement with human rights groups about potential unintended consequences.

Any new self-regulatory mechanisms or procedures developed by companies to combat terror must be accompanied by an increase rather than decrease in the levels of transparency with users and engagement with key affected stakeholders and at-risk groups.

5. Clear and effective grievance and redress mechanisms

In order to prevent abuse of anti-terror laws or informal measures taken by governments or companies, it is vital that there be robust mechanisms and processes for accountability. In particular, governments as well as companies should provide effective, accessible channels for grievance and remedy for people whose rights to free expression, assembly, and privacy have been violated by measures taken to combat online extremism. Public and private entities that abuse these measures in a way that violates human rights must be held accountable.[12]

We live in a time of extraordinary threats to our national security. But the fight against terrorism online must be carried out in a way that also protects and respects human rights. If the US and other democracies cannot figure out how to do this, victories against violent extremism online are likely to be hollow and short lived.

[11] http://sinosphere.blogs.nytimes.com/2014/12/27/facebook-deletes-post-on-tibetan-monks-self-immolation/

[12] See the UN Guiding Principles on Business and Human Rights http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf