Concept Note for Policy Focus Session:

"How to Stop Online Violence: Laws, Policies, and Principles"

Details

Date: Thursday, March 21th
Duration: 60 minutes
Type: Policy Focus Session
Location: NJV Athens Plaza Hotel
Time: 10:40 – 11:40
Co-host: Council on Foreign Relations
Participants: Open to all attendees of the WPL Summit

Summary

Participants will discuss their experiences and the various forms of online abuse and harm that are most common in their countries; the types of remedies that have been sought from tech companies; and what legislation has been proposed or passed to address these harms. This discussion will also consider key principles that could be incorporated into the U.N. Global Digital Compact.

Online harms

Women are disproportionately targeted with gendered, sexualized abuse, threats, and violence. Women in the public sphere experience the most online violence, and the more senior the politician, the more abuse she receives. Minority, ethnic and LGBT+ women receive higher levels of abuse. This online violence serves to reduce political participation and democracy as women self-censor, retreat, and choose not to participate in politics including running for office. The types of attack range from abuse and threats, stalking, doxing, impersonation, deep fakes, nonconsensual image sharing, and disinformation. Law enforcement agencies have documented the tendency of online threats and abuse to result in physical harm. Over 80 percent of women in parliaments report suffering psychological abuse, 65 percent have been threatened with physical violence or death, and 25 percent have been physically attacked.

Digital platform design and policies

Online violence is accelerated by the design of digital platforms and services such as search engines. Many large platforms have policies, but they are not enforced. Indeed, their recommender algorithms promote the most sensational, scurrilous material. The quality and quantity of content moderation varies widely: some companies invest little and react slowly to take down requests. User controls are cumbersome, hidden, and inadequate. Cross-platform cooperation to halt the viral spread of illegal or harmful content is limited. Content moderation is even less effective for non-English languages and colloquial or coded language. Synthetic media and artificial general intelligence are creating new forms of faked harm through creation of distorted or entirely false images, voice, video, and text using one photo or audio clip. Downloadable generative AI tools like ChatGPT and Dall-e allow users to create and propagate such material at astonishing speed, scale, and volume.

Laws and principles

Inadequate policies and enforcement by tech companies have led some governments to adopt laws that require platforms and services to take a more rigorous approach to preventing illegal and harmful activity. In addition, some countries have updated their laws on child sexual abuse, domestic violence, stalking, and hate speech to apply to online activity as well. Three laws that seek to address a range of harms are the European Union’s Digital Services Act, the recently passed UK Online Safety Act, and Australia’s 2021 Online Safety Act which updates its 2015 law. The session will discuss major features and principles that underlie these laws, and whether they may be helpful models for other countries and for formulation of the Global Digital Compact.

--- ENDs ---