

PRESENTED TO

UNITED NATIONS SPECIAL RAPPORTEUR ON THE
PROMOTION AND PROTECTION OF THE RIGHT TO
FREEDOM OF OPINION AND EXPRESSION

SUBMISSION

Disinformation and Freedom of Opinion and Expression

Introduction

ICNL is grateful for the opportunity to provide input regarding measures to address disinformation and implications for the protection and promotion of the right to freedom of opinion and expression. This month, ICNL has issued *Legal Responses to Disinformation - a Policy Prospectus*, which sets forth information and analysis concerning available legal and regulatory measures to combat disinformation. Through this prospectus, ICNL aims to inform policymakers and empower civil society actors working to advance regulatory responses that will limit the spread and amplification of disinformation while fully respecting and protecting freedom of expression.

This submission summarizes the information and analysis set forth in *Legal Responses to Disinformation - a Policy Prospectus*, which primarily addresses the first, second, fourth, and fifth questions raised in the Special Rapporteur's call for submissions. A copy of *Legal Responses to Disinformation - a Policy Prospectus* also accompanies this submission. We hope the Special Rapporteur will find this submission helpful in preparing the upcoming report to the 47th Session of the Human Rights Council.

Definitions

Disinformation is false or manipulated information that is knowingly shared to cause harm or is made with reckless disregard of likely harm. **Misinformation** is the unintentional dissemination of false or misleading information, while **mal-information** is truthful information presented deceptively in an attempt to mislead.

The term "**fake news**", although widely used, has no accepted definition and is vulnerable to political manipulation. It is a term that should be avoided, in favor of defining relevant content as disinformation, misinformation or mal-information.

The Nature of the Problem

While not a new problem, disinformation today poses a new kind of threat because new technologies have enabled individuals and groups to spread messages faster and to a wider audience than ever before. Disinformation campaigns mobilize large numbers of individuals or groups to interact with, share, and post content.

Social media platforms and internet companies cannot be relied upon to curb disinformation. Their first priority is to generate profit. Their business models thrive on engaging users with disruptive and exciting content, which relies on the use of algorithms and massive collection of user data to create a perfect ecosystem for disinformation. At the same time, social media companies do not want to be viewed as propagators of disinformation and misinformation.

Although **messaging applications** like WhatsApp, Telegram and SMS/text messaging do not have the same reach as social media, individuals use messaging apps to spread disinformation and misinformation, sometimes to large groups. Messaging apps often contain end-to-end encryption, which protects individuals' privacy. Weakening or prohibiting end-to-end encryption methods is not a viable option because it will impact all services that rely on it for protection of the privacy of its users.

Problematic Responses to Disinformation

Many democratic governments have been reluctant to regulate the social media landscape, in part due to fear of being accused of restricting free speech. Where governments have enacted laws, however, they have often proved problematic.

"Anti-Fake News" laws that seek to directly counteract disinformation do so with general prohibitions on the dissemination of information based on vague and ambiguous concepts, including "false information", and provide authorities with broad powers to act as "arbiters of truth", in violation of Article 19 of the ICCPR.

Cybercrime laws or penal codes often contain provisions criminalizing categories of speech online, including disinformation, but again do so too often with overly broad and vague language. Such laws and provisions do not comply with Article 19 of the ICCPR, and therefore impermissibly restrict freedom of expression.

The **COVID-19 pandemic has led to emergency measures** that impose heavy penalties or long jail sentences for spreading "false information" or "rumors" about COVID-19 on social media, while lacking sufficient safeguards to protect freedom of speech.

Principles for Appropriate Regulation of Disinformation

Government regulation is needed to limit the spread of disinformation, misinformation and mal-information. Social media platforms and other internet companies have not

previously acted, and are unlikely to act, in the interests of the public without regulation by law. But **governments should not be the arbiters of truth**, and citizens should be able to access true and false information and then assess the validity of that information.

Regulation must comply with international norms relating to freedom of expression and privacy. Restrictions on expression are only permissible when they satisfy Article 19's three-part test, so that any restrictions on expression must be provided by law and necessary in a democratic society in furtherance of legitimate government aims.

Legal and Regulatory Responses to Disinformation

Government responses to disinformation may rely on: (1) existing laws, not designed to combat disinformation, which nonetheless address the problem in part; (2) laws modeled on recent measures targeting disinformation; or (3) new legal or regulatory approaches that provide innovative solutions to the problem.

EXISTING LAWS

The existing laws in many countries may be an important part of the legal response to disinformation. While not designed to address disinformation in the digital realm, they could be, and in some cases have been, applied to combatting disinformation.

Tort laws can be used to provide reparations to victims and deter engaging in disinformation. Relevant tort causes of action include: intentional infliction of emotional distress (in the United States); defamation, which has been used as the basis for suits countering disinformation in the U.S., South Africa, India, and Finland; and unlawful act, which has been used in anti-disinformation suits in the Netherlands and Brazil.

Cyber-bullying and cyber-stalking laws are similar to anti-harassment laws, and prohibit harassing individuals online. Such laws have been enacted in the U.S., Australia, the United Kingdom, Singapore, and Ireland. In Uganda, however, a cyber-harassment law has also been used to punish government criticism, suggesting that such laws must be narrowly drafted and implemented based on objective standards.

Fraud statutes may exist for both offline and online "fraud", and in certain instances could be used to punish actors that intend to harm via false information.

LAWS TARGETING DISINFORMATION

Recently enacted or proposed laws have sought directly to combat disinformation.

Actors pushing disinformation often use so-called automated bots, such as fake accounts on social media that are programmed to look human and cause a certain message. **Anti-bot laws** – such as the July 2019 measure in California requiring bots (or the person controlling them) to reveal their "artificial identity" when they are used to

sell a product or influence a voter – can be used to limit the spread of disinformation because these laws make it more difficult to push content through bots.

Transparency laws aim to make social media users aware of where content comes from and the entities supporting the production and publication of that content. The U.S., France, and Ireland require social media companies to collect and disclose information to users about who paid for an advertisement or piece of sponsored content, and to share information about the audience that advertisers target. EU Member States have adopted national approaches to regulating political advertising on social media. And proposed measures in the U.S. and EU would set out additional requirements regarding the disclosure of entities supporting advertisements on platforms.

PROPOSED REGULATORY RESPONSES

Other regulatory responses that have not yet been enacted or implemented could impose mandatory requirements on or create accountability mechanisms for social media platforms and messaging apps in order to combat disinformation.

As part of the “**terms of service**” or “**community standards**” that users must accept to use their services, social media platforms require users to acknowledge the right of the company to restrict a user’s speech and abide by the rules set by the social media platform. However, social media companies implement their terms of service or community standards in arbitrary and subjective ways, and without transparency. New measures could push social media companies to take a stronger stance against disinformation by requiring them to develop and implement their terms of service or community standards in an open and transparent way, with oversight from regulators.

States could establish **independent regulatory agencies** to ensure that social media platforms are complying with internal policies or national laws on an array of issues, such as fact-checking, advertisement disclosures, use of bots, due diligence, consumer responsibilities and worker protections. Such agencies must be sufficiently independent and appropriately staffed to avoid unwarranted government interference leading to the curtailment the freedom of expression, as has been observed with the Tanzania Communications Regulatory Authority and the Press Council in Nepal.

Private rights of action could be created that allow citizens to file suit alleging platform violations of regulatory requirements, thus creating a class of private attorneys general ensuring compliance with legal requirements. **Administrative tribunals** could be established to hear such claims, in order to avoid overwhelming court systems with new claims, and to ensure adjudicators have adequate expertise on disinformation.

Platforms with a minimum number of users could be required to establish transparent **complaint-and-review or notice-and-action mechanisms** enabling platform users to submit complaints about certain content for review, adjudication and corrective action.

Education and literacy are widely acknowledged as crucial to being able to navigate the information space and recognize disinformation. Because large online platforms provide the main channels to spread and amplify disinformation, they may reasonably be held responsible for equipping users with the necessary skills to engage with platforms, including, for example, by paying a percentage of advertising revenue into an education fund to be used to create and implement courses on media literacy.

Social media companies should provide **information regarding the source and truthfulness of content**, to prevent disinformation from spreading and finding an audience. Platforms should disclose where social media users/accounts are located and flag instances of misleading accounts and inauthentic behavior. Platforms should also engage in robust fact-checking, though research has shown that it is not a panacea.

Disinformation and misinformation communicated through social messaging apps will generally have a greater impact when shared among large groups. Laws can reduce this impact by **limiting the number of times a message can be forwarded or the number of people allowed into a chat**; by requiring transmission of a **warning with forwarded messages**; or by setting up **complaint or flagging mechanisms** when someone receives a message containing what appears to be disinformation or misinformation.

Contact Information

For further information or in case of questions, please contact Zachery Lampell, ICNL Senior Legal Advisor – Freedom of Expression, at zlampell@icnl.org, or Nikhil Dutta, ICNL Global Programs Legal Advisor, at ndutta@icnl.org.