Facebook submission to UN Special Rapporteur on Freedom of Opinion and Expression for Report on Disinformation.

Facebook welcomes the opportunity to provide input to the Report on Disinformation issued by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. We support the aim of the report to clarify how human rights law applies to disinformation.

Freedom of expression is a foundational human right that includes and allows for the free flow of information. We're reminded how vital this is, in particular, as the world grapples with COVID-19, and accurate and authoritative information is more important than ever. Human rights defenders know this and fight for these freedoms every day. Facebook gives people voice and helps build community: these rights are core to our mission.

1. a) What do you believe are the key challenges raised by disinformation?

Disinformation and misinformation present real challenges for human rights and political systems- indeed they are currently regarded as one of the greatest threats to democracy by experts internationally.

At the same time, overbroad, disproportionate and inappropriate responses to these phenomena create even greater threats to human rights.

As we have seen in several countries around the world, disinformation can and does undermine the right to free and fair elections (Article 25, ICCPR).

It can also undermine the right to health (Article 12 of the ICESR) through encouraging the use of harmful or ineffective treatments and discouraging vaccination efforts, as has been seen in many countries in the context of COVID-19. We note access to health-related education and information is indeed part of the right to health. (CESCR General Comment No. 14, The Right to the Highest Attainable Standard of Health, para 12 (b)).

However, efforts by governments to contain or repress disinformation and misinformation can - intentionally or otherwise - restrict freedom of expression. Governments need to be clear that restrictions on the flow of information generated by individuals, media outlets, and social media companies can only be done within the constraints of legality, necessity, proportionality in order to protect harms to other rights, national security, ordre publique or public health as defined in the ICCPR, related authoritative guidance, or (in states of emergency) the Siracusa Principles.

There is an inherently fraught definitional challenge when it comes to "disinformation".

First, there is much conflation and confusion between concepts such as disinformation, misinformation, foreign interference, and influence/information operations. And there is an important difference between false information shared unintentionally—what is generally understood to be “misinformation”—versus false information shared intentionally to deceive,which is commonly referred to as “disinformation”. At Facebook, we have adopted the following definitions:

- **Misinformation:** refers to misleading content (false news, manipulated content, etc)
- **Disinformation:** provably false information used by someone who knows it is false
- **Influence operation:** coordinated effort to manipulate or corrupt public debate for a strategic goal

Second, governments, policymakers, civil society, academics, and people in general do not agree on what misinformation is - what one person considers to be false information, for example, may simply be another’s opinion.

Third, these challenges are compounded by the difficulty of determining who decides if something is untruthful; who or what is the source of truth; and what the penalties for untruthful content should be. Any measures attempting to address these questions risks capricious or disproportionate restrictions on freedom of expression and the right to information.

Some governments are looking at mis/disinformation as a category of harm. In the UK, for example, addressing mis/disinformation as harmful content *“will ensure the focus is on protecting users from harm, not judging what is true or not.”*[1] However, deciding on the definition of harm can still be highly contextual, difficult to define, often culturally subjective, and legally ambiguous.

Therefore, any regulation for harmful content should indeed recognise the need to balance the removal of harmful content with the protection of freedom of expression and other fundamental rights. For these reasons, many governments have explicitly opted not to engage in the arena of regulating misinformation, even though some government or state entities intentionally engage in the spreading of untruthful information.

In order to find solutions, more clear and nuanced terminologies are needed to differentiate between the different components of the problem and to better align democratic concerns with security concerns. Methodologies of how misinformation or disinformation is addressed by various entities in different operational environments needs to be understood in more granularity.

As disinformation applies and is used in a multitude of different operational environments, and across multiple platforms and media surfaces, no one-size-fits-all methodology to combat it can be implemented.

---

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

Indeed, as the Carnegie Endowment for International Peace noted[2] in its assessment of the EU Code of Practice on Disinformation:

> *"The EU should first revise the terminology used to support disinformation policy and analysis to make it easier to distinguish between different aspects of the problem. Disinformation is currently used as a catchall term that does not help the EU institutions define different areas of problematic behavior. It muddles the actions of individuals inadvertently sharing incorrect information [i.e. misinformation] with the hybrid influence campaigns of hostile states."*

At Facebook, we try to make a clear distinction between the different terms. When we look at misinformation and disinformation, we differentiate between the two based on actor, behavior and content.

When we look at disinformation, we focus on solutions to curb inauthentic **behaviors**. With misinformation, we focus on solutions to reduce the spread of false and misleading **content** on our platforms.

To identify posts as misinformation, it is necessary to analyze the content.

Conversely, actors engaged in disinformation need not necessarily use misinformation. (For clarity, it is important to note that, at Facebook, we use the term "influence operations (IO)" - instead of "disinformation" to describe coordinated efforts that aim to manipulate or corrupt public debate for a strategic goal.)

Most of the content shared by IO campaigns are not provably false, and would in fact be acceptable political discourse if it was shared by authentic actors. The real issue is that the actors behind these campaigns are using deceptive behaviors to conceal the identity of the individuals or organisation behind a campaign; make the organisation or its activity appear more popular or trustworthy than it is; or evade enforcement efforts.

Two key markers for influence operations are inauthenticity and coordination. To combat this threat, we have developed an inauthentic behaviour policy that targets coordinated efforts to manipulate public debate for a strategic goal, where fake accounts are central to the operation, and allows us to take down networks of accounts, pages and groups based on behavioral signals.

There are two tiers of these activities that we work to stop:

1. Coordinated inauthentic behavior in the context of domestic, non-government campaigns (CIB); and
2. Coordinated inauthentic behavior on behalf of a foreign or government actor (FGI).

While there may be some overlap (actors engaged in IO may also utilise misinformation), disinformation and misinformation are not the same. This is the view of numerous experts in

[2] https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82286

this space, such as Camille Francois at Harvard University,[3] and respected news coalition First Draft.[4]

The distinctions between disinformation and misinformation are important, because the policy concerns underlying each differ: thus, appropriate responses from platforms like Facebook will also be different. For example, we believe the appropriate role we should play in relation to disinformation is different in relation to misinformation.

As policymakers decide on the appropriate measures to tackle disinformation, it is important that the terms and definitions are clear and precise. Precision is essential to help educate the broader community, ensure effective and rights-consistent regulation; and also to ensure enforcement and accountable metrics (such as transparency reporting metrics) are fit-for-purpose.

1. b) What measures would you recommend to address them?

Ensuring the quality and safety of our communities, by addressing bad actors, inauthentic behaviors, and problematic content, is a top priority for Facebook. Dealing with the broad range of integrity-related issues online is a complex problem. The public debate often treats integrity issues (in this case, disinformation) as a single problem, but the truth is that concerns over mis- and disinformation involve a variety of different problems rolled together. When we blur issues together as one problem set, it becomes very hard to develop a strategy to solve any one part.

The following outlines how we break down and approach different integrity issues.

Enforcement Based on Actor, Behavior, Content (ABC)

At Facebook, we enforce against a broad range of violating activity across three specific areas:

1) Actor-based enforcement, which involves the removal of accounts or organizations because of the totality of their activity on the platform;

2) Behavior-based enforcement, which is predicated on specific violating behaviors exhibited by violating actors; and

3) Content-based enforcement, which predicates enforcement on specific violations of our content policies

In accordance with other cross-sector approaches used across the influence operations environment, we intentionally break this problem out along three dimensions - actors, behaviors, and content.

---

[3] C Francois, *Actors, Behavior, Content: A Disinformation ABC*, 20 September 2019, https://science.house.gov/imo/media/doc/Francois%20Addendum%20to%20Testimony%20-%20ABC_Framework_2019_Sept_2019.pdf

[4] H Derakhshan & C Wardle, 'Information Disorder: Definitions', *Understanding and Addressing the Disinformation Ecosystem*, December 2017, https://firstdraftnews.org/wp-content/uploads/2018/03/The-Disinformation-Ecosystem-20180207-v4.pdf?x42643

For example, any potential violation could be conducted by a problematic actor (for example, a foreign government); using problematic behavior (for example, networks of fake accounts); or could distribute problematic content (e.g., misinfo or hate speech).

We have specific policies that work along each dimension, and tailor our response to the nature of the violation. This gives us a range of tools to respond with. By combining all three dimensions, we have a network of enforcement operations. It's important to remember that there's no silver bullet, and all of them have to work together.

Combatting Coordinated Inauthentic Behaviour and Influence Operations

In the social media landscape and beyond, influence operations (IO) rely on inauthenticity and coordination. Users misrepresent themselves, through fake profiles or non-transparent behaviors, often building complex networks, for the purpose of manipulating or corrupting public debate. IO manifest in different ways on different platforms and in different fora. They may have political, financial or personal incentives, or indeed a mixture.

Government efforts to address this issue through legislation and regulatory efforts have been fragmented despite the global nature of the problem. creating a

The IO legislative principles summarized below consolidate approaches that we have seen work worldwide, in multiple governance structures, to foster cross-sector and collaborative ways to mitigate this threat within a consistent and cohesive global regulatory framework.

We believe that approaching legislation or regulation in the IO space should be pursued, but accompanied by a regulatory package fixing overarching principles applicable to all information society services and establishing more detailed rules for dealing with disinformation under such general principles.

It should strike a balance between effectively combating IO threats, while also protecting speech and the privacy of users. These would include:

- **Transparency in Ads.** Require much greater transparency for contributions or expenditures for political advertising;
- **Reporting on Inauthentic Behavior.** Work with industry and civil society experts to provide minimum disclosure frameworks, collaborative development of transparency best practices, and the sharing of lessons learned, so there are parameters on what to report publicly on the impact of inauthentic behavior across social media and elsewhere to help governments, researchers and the public assess current risk.
- **Broad Applicability.** Be crafted to cover IO broadly, as opposed to specific tactics of IO (e.g., the use of fake accounts), because IO manifests differently on different platforms and in traditional media, and narrow definitions will likely leave loopholes that attackers can exploit;
- **Increased Information Sharing.** Enable greater information sharing of IO threat signals among industry and between industry, civil society, and government, while protecting the privacy of innocent users who may be swept up in these campaigns;

- **Deterring Violators.** Impose economic, diplomatic, and/or criminal penalties on the threat actors behind serious IO campaigns, understanding that different penalties and mitigations apply in foreign and domestic contexts;
- **Supporting Technical Research.** Support private and public innovation and collaboration on technical detection of adversarial threats such as manipulated media and deep-fakes; and
- **Supporting Media and Digital Literacy.** Support media and digital literacy to educate users and promote and strengthen societal resilience.

Three-Part Strategy to Tackle Misinformation: Remove, Reduce, Inform

Our efforts to combat IO campaigns is complemented by a three-prong strategy to reduce the spread of false news and misinformation. Our approach to misinformation is guided by the principle that we should provide people with accurate and informative content, while balancing free expression. Our users want to see high quality content on our platform, and so do we. We apply a three-part strategy - remove, reduce, and inform - to combat misinformation.

This involves removing content that violates our policies, reducing the spread of problematic content that does not violate our policies but still undermines the authenticity of the platform, and informing people with additional information so they can choose what to click, read or share.

- **Remove:** We remove content that violates our Community Standards, including fake accounts and accounts engaged in inauthentic behavior, misinformation that may contribute to the risk of imminent violence or physical harm (such as harmful health misinformation), voter fraud or interference, hate speech, bullying and harassment. We also remove ads that violate our Advertising Policies, including ads with debunked claims by third-party fact-checkers or, in certain circumstances, by authoritative bodies, as well as our Community Standards.
- **Reduce:** Problematic content that does not violate our Community Standards is demoted in the News Feed. Such content undermines the authenticity and integrity of our platform: for example, clickbait and content debunked by our network of independent third-party fact-checking partners, are both demoted in the News Feed. These actions significantly reduce the number of people on Facebook and Instagram who see such content.
- **Inform:** We help prevent the spread of misinformation by providing additional context and connecting people with accurate information so people can make informed decisions. This strategy is often implemented through design and user experience features, which can be narrowly framed and extensively tested.
    - For example, content that has been rated false or partly false by our fact-checkers is prominently labeled so people can better decide for themselves what to read, trust, and share; and we added a context button in Newsfeed in 2018 to provide users with important credibility information,

- We have begun to label media outlets that are wholly or partly under the editorial control of their government,[5] and also label ads that they purchase. We also blocked ads targeting the US from state-controlled media to provide an extra layer of protection against various types of foreign influence in the public debate ahead of the US 2020 election.We have also introduced important but rights-respecting user cues to encourage users to actively consider before sharing certain kinds of content. For example, in June 2020 we introduced a new notification screen that lets people know when news articles they are about to share are more than 90 days old.

You can find recent real world summaries of how we apply these and other integrity measures across Africa,[6] Myanmar,[7] and the United States.[8]

Connecting People to Accurate and Authoritative Information

We continue to find new ways to connect people with accurate, reliable and authoritative information. This is a core component of our strategy to combat misinformation because we want to be able to provide our users with the means to decide what to read, trust and share.

Informing people with accurate and authoritative information, as well as more context, is an approach that can be more impactful than the alternative of just removing content. If we simply removed all posts flagged by fact-checkers as false, for example, the content would still be available elsewhere on the internet, other social media platforms, or even around the dinner table. By leaving this content up and surfacing research from fact-checkers or pointing people to authoritative information, we're providing people with important information and context.

Our strategy around authoritative information is centered on launching products (such as our COVID-19 Information Center and Climate Science Information Center) when communities are facing certain threats (such as the COVID-19 health crisis); where the risk for widespread misinformation and user confusion about that threat is high; and there are widely agreed-upon authoritative sources and information that can be referenced. We want to change people's behavior, attitudes or knowledge about those threats by making authoritative information more visible and accessible. In doing so, we seek to reduce the spread of misinformation and reduce the efficacy of malicious networks that might try to take advantage of uncertainty and manipulate public discourse.

As noted by an international group of human rights experts (in relation to COVID-19):

> *"it is essential that governments and internet companies address disinformation in the first instance by themselves providing reliable information… Resorting to other measures, such as content take-downs and censorship, may result in limiting access to important information for public health and should only be undertaken where they meet the standards of necessity and proportionality."*[9]

[5] https://about.fb.com/news/2020/06/labeling-state-controlled-media/
[6] https://about.fb.com/news/2020/10/supporting-elections-across-africa/
[7] https://about.fb.com/news/2021/02/an-update-on-myanmar/ and https://about.fb.com/news/2020/08/preparing-for-myanmars-2020-election/
[8] For example: https://about.fb.com/news/2020/10/preparing-for-election-day/ and https://about.fb.com/wp-content/uploads/2020/12/Elections-Fact-Sheet.pdf
[9] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25729

From Digital Literacy to Digital Citizenship

Media and digital literacy initiatives to raise awareness and help people be more critical about the information they see is an important part of our strategy to combat misinformation. Given the multitude of online threats that a person may encounter, media and digital literacy initiatives should do more than raise awareness. Instead, they should aim to promote skills and competencies that are needed to safely and intelligently navigate the digital landscape. A holistic approach is necessary - one that also aims to enable people to participate in digital society safely, respectfully, responsibly and ethically.

Facebook has implemented a variety of digital literacy programs at scale, many focused on new-to-internet populations.[10] Fostering digital citizenship is a whole-of-society responsibility and cannot be achieved by any one stakeholder. It requires a multi-disciplinary strategy involving the full range of stakeholders, from government to industry to civil society, educators and citizens themselves. Governments can play a role in this space by facilitating collaboration between relevant stakeholders, investing resources, and establishing cooperation frameworks.

Tackling Disinformation on WhatsApp

Private messaging services differ in key ways from public social media platforms, and disinformation challenge plays out differently on these services. The approach to tackling disinformation on these services should be flexible and reflect the differences, as well as those between different messaging services.

While efforts to address the challenge will be most effective if they are tailored to each service, we believe they should fall into three broad categories:

- Tackling abuse at the account level based on behavioural and other signals that is not not based on content;
- Developing integrity features in the product; and
- Connecting people with authoritative sources of information and advice.

WhatsApp, for example, is designed to help people communicate directly with their friends and loved ones. Approximately 90 percent of the messages sent on WhatsApp are one-to-one, the maximum group size is 256 and the majority of group chats include fewer than ten people. There are no algorithms to promote content, and users do not build audiences or discover new people as they would on social media. Preventing unsolicited communication is built into the design of the service. A user must have someone's phone number to contact them on WhatsApp, and when a WhatsApp user receives a message from an unknown number, we immediately ask them if they want to allow messages from, block or report the sender of the message.

Further, WhatsApp is designed to limit spam and virality through product features like forward limits and through measures to detect and ban accounts engaging in bulk messaging or automated behavior. WhatsApp messages and calls are protected by end-to-end encryption, which means no one except the sender and recipient can see the content, not even us. End-to-end encryption is essential to protect people's private

[10] See, for example, https://wethinkdigital.fb.com/ and She Means Business.

conversations and keep them safe from criminals and hackers.

In light of WhatsApp's nature and purpose, its approach to tackling disinformation focuses on three key areas: tackling abuse at the account level based on behaviour-based signals and other available information not message content; introducing features in the product to limit virality and empower users; and connecting people with authoritative sources of information, education and tips. We believe this three-pronged approach is the most effective way to help address the disinformation challenge while protecting people's ability to communicate freely, privately and securely on messaging services.

We respectfully emphasize the importance of user experience and design features in limiting the spread of disinformation and misinformation. Such features can be more effective than content policies. In 2020, Messenger introduced limits to ensure messages could only be forwarded to five people or groups at a time (details here, with video). Similarly, in April 2020 WhatsApp enacted limited forwarding of frequently forwarded messages to one chat at a time, resulting in a global 70% reduction in the number of highly forwarded messages.[11]

2. a) What legislative, administrative, policy, regulatory or other measures have Governments taken to counter disinformation online and offline?

It is important to note that there is no silver bullet for combatting disinformation or misinformation. A whole-of-society, multi-prong approach, with collaboration among the full range of stakeholders (including the user community, and national advertising and PR industries) are needed to respond to different aspects of the problem.

Legislative or regulatory responses to curb misinformation or disinformation should be balanced with protecting fundamental rights like freedom of expression.

To contribute to policy discussions, we published a whitepaper last year - "Charting a Way Forward: Online Content Regulation" - setting out some principles to consider for online content regulation, which include:

- **Freedom of expression**. Regulation should recognize the need to balance content restrictions with the protection of freedom of expression and other fundamental human rights.
- **Global and cross-border nature of the internet.** Regulation should recognize the global scale of the internet and the value of cross-border communications.
- **Flexibility.** Regulation should be based on understanding of capabilities and limitations of content moderation technology and allow internet companies the flexibility to innovate.

[11] Manish Singh, WhatsApp New Limit Cuts Virality of Highly Forwarded Messages by 70, Techcrunch, April 27, 2020.

- **Proportionality and necessity.** Regulation should take into account severity and prevalence of harmful content, its status in law, and efforts already underway to address the content.
- **Incentives for accountability.** Regulation should ensure accountability in content moderation systems and procedures by creating incentives for companies to responsibly balance values like safety, privacy, and freedom of expression.

We also published a set of Recommended Principles for Regulation or Legislation to Combat Influence Operations, which has been outlined in Section 1.b) above.

2. b) What has been the impact of such measures on i) disinformation; ii) freedom of opinion and expression; and iii) other human rights?

Regulatory measures, if designed well, can contribute to the internet's continued success by articulating clear ways for government, companies, and civil society to share responsibilities and work together. However, we have seen many examples of governments developing approaches to disinformation that - deliberately or otherwise - repress rights to freedom of expression and access to information, amongst others. Designed poorly, these efforts risk unintended consequences that might make people less safe online, stifle expression and slow innovation. Such measures are often poorly thought through, not rights respecting, and grossly disproportionate. Many fail basic rights protections, such as executive orders requiring platforms to remove certain misinfo without judicial review, often used in arbitrary ways.

See section 1. b) above where we speak to the measures that we, at Facebook, have taken.

2. c) What measures have been taken to address any negative impact on human rights?

As described in this submission, the process of identifying, removing and restricting access to harmful disinformation is complex and challenging for a company with billions of daily users.

FB uses its global stakeholder engagement mechanisms, its policy development processes, and explicit consultation of global human rights standards to guide related policy and product development. We note we also developed an extensive network of local and global partners who can also help us identify and remove untruthful or unverifiable information that may lead to real world physical harm. We welcome the opportunity to answer any questions, and seek to ensure we do all we can to prevent or mitigate the damage caused by disinformation while respecting human rights principles.

We seek to do all that we can to address disinformation without prejudice to the freedom of expression of our users.

3. a) What policies, procedures or other measures have digital tech companies introduced to address the problem of disinformation?

See section 1. b) above where we speak to the measures that we, at Facebook, have taken to address the problem of disinformation.

3. b) To what extent do you find these measures to be fair, transparent and effective in protecting human rights, particularly freedom of opinion and expression?

At Facebook, our commitment to freedom of opinion and expression is paramount, but we recognise that the internet creates new and increased opportunities for abuse. The COVID-19 pandemic has exacerbated and highlighted the enormous challenges faced by social media companies in navigating the protection of free speech and the prevention of harmful disinformation. Yet, we have

3. c) What procedures exist to address grievances and provide remedies for users, monitor the action of the companies, and how effective are they?

At Facebook, we give people the option to appeal our decisions, except in cases with extreme safety concerns. We restore content we incorrectly removed or when circumstances change, both when it is appealed and when we identify issues ourselves.

We believe that transparency brings greater accountability. We publish regular reports to give our community visibility into how we enforce policies, respond to data requests and protect intellectual property, while monitoring dynamics that limit access to Facebook products.

Our quarterly Community Standards Enforcement Report provides metrics on the amount of content we actioned that people appealed; the amount of content restored after an appeal; and the amount of content restored without an appeal (that we self-corrected).

In late 2019 we created an independent operational grievance mechanism, the Oversight Board. The Board began taking cases in late 2020. The Board was created to provide additional remedy to users, and to =help Facebook answer some of the most difficult questions around freedom of expression online: what to take down, what to leave up, and why. In its first decisions, it has already demonstrated its independence in overruling the company on four of our first five decisions.

4) Please share information on measures that you believe have been especially effective to protect the right to freedom of opinion and expression while addressing disinformation on social media platforms.

See section 1. b) above where we speak to the measures that we, at Facebook, believe have been effective to protect the right to freedom of opinion and expression while addressing disinformation on social media platforms. We particularly draw your attention to our behavioral policies, our labelling efforts, and our product interventions. We also draw your attention to our recent integrity efforts in Myanmar (from August 2020-February 2021) which may provide useful, up-to-date, practical examples of our work.[12]

5) Please share information on measures to address disinformation that you believe have aggravated or led to human rights violations, in particular the right to freedom of opinion and expression.

A number of governments around the world have used the spread of disinformation or “fake news” as a pretext to restrict dissent and critical speech through repressive legislation or through takedown or correction requests that violate their commitments to respect the freedom of opinion and expression of their citizens. This trend has accelerated under the pretext of the COVID-19 pandemic as has been well-documented including here

Facebook has previously expressed concern, to give but one example, about the Singapore’s Protection from Online Falsehoods and Manipulation (POFMA) law and objected to judicial orders to block access to a news site. “We've repeatedly highlighted this law's potential for overreach and we're deeply concerned about the precedent this sets for the stifling of freedom of expression in Singapore."[13]

Facebook has also expressed concerns about the efforts to rail in free speech under the guise of addressing misinformation in Vietnam and Cambodia. Cambodia is a very good example of a country where restrictions on the media have left social media as the only possible source of free expression and dissent within the country leading the government to seek to take action against websites and social media platforms using “fake news” as a pretext to censor dissent.

[12] https://about.fb.com/news/2020/08/preparing-for-myanmars-2020-election/; https://about.fb.com/news/2020/09/additional-steps-to-protect-myanmars-2020-election/ and https://about.fb.com/news/2021/02/an-update-on-myanmar/

[13] https://www.bbc.com/news/world-asia-51556620

6) Please share any suggestions or recommendations you may have for the Special Rapporteur on how to protect and promote the right to freedom of opinion and expression while addressing disinformation.

Detailed recommendations can be found in section 1.b) and 2.a) above.

The enormous and growing scale of internet use worldwide, the rapid development and adoption of new technologies and increased political polarization in many countries around the world create enormous complexity for the management of this issue.

We commend the Special rapporteur for her engagement with this issue and pledge our full support for her mandate. We note that there is little human rights guidance on disinformation, and we would genuinely welcome the mandate's guidance in this regard.