The European Commission's Digital Services Act Proposal:
Microsoft's Views on Digital Safety
(8 September 2020)

Microsoft welcomes the European Commission's efforts to strengthen digital safety through the proposed Digital Services Act (DSA). We agree that providers of digital services have an important role to play in helping people stay safe online—in particular, to design and operate their services responsibly, including by anticipating and reducing digital safety risks on their services. Promoting such behaviour requires a carefully calibrated regulatory framework, one that encourages positive and thoughtful action by providers but does not inadvertently incentivize censorship. As the DSA proposal moves forward, we respectfully urge the Commission to consider the following points.

Preserve and build upon the e-Commerce Directive framework. The EU's existing legal framework, based on the e-Commerce Directive (ECD), has been successful in promoting both online innovation and responsible behaviour by providers. For instance, the ECD's notice-and-takedown rules continue to work well in many scenarios, especially where the illegality of content is not apparent on its face (e.g., in claims of copyright infringement or defamation). That said, the variety and usage of online services has expanded dramatically since the ECD was adopted, and it is not clear that the concept of "storage" on which Article 14's notice-and-takedown framework rests is sufficiently nuanced to account for this diversity. As an example, while a cloud service provided to business customers, and a social media service offered to consumers, both involve the "storage" of user content, the digital safety risks they pose—and users' expectations about how providers will treat their content—vary substantially. Any new rules in this area should therefore preserve the general approach of the ECD, including its safe harbours and country-of-origin rules, but also incentivize online intermediaries to take actions appropriately tailored to their services to promote digital safety among individual users, families and online communities.

Promoting digital safety should not force providers to become censors. Obligations for service providers to promote digital safety should not force them to become content gatekeepers. The ability of users to create, share, and access content directly is what makes the internet so dynamic and such an important tool for promoting fundamental rights including freedom of expression. Although digital services should prioritize operating their services in ways that limit digital safety risks, making them responsible for what their users say, post, or link to would undermine how many services on the internet work and destroy the internet's essence and value. Digital safety rules should also avoid incentivizing providers to over-censor content in order to limit potential liability. This risk is particularly acute where the rules are vague, where providers must assess and remove content under tight time constraints, or where obligations vary between jurisdictions (since this may force providers to apply the most restrictive content removal rules globally).

There is no "one-size-fits-all" approach. No single technology approach or content moderation practice will be appropriate for every service or scenario. Instead, providers' obligations should be tailored to the nature of their services, the nature of the content, and the nature of the illegality. In particular:

- Nature of the service. Digital safety obligations should take into account the function of the service, the relationship between providers and end-users, the expectations of users, and the risk profile of the service itself. For example, online productivity tools tend to have lower risk of being used to spread illegal content virally than general-purpose social media services, while a corporate customer of an enterprise cloud service will have different expectations than a consumer who publishes content on a social messaging service that is accessible by the general public. It also makes sense to differentiate between services whose primary purpose is to make content widely available to the public, and those that are used primarily to store private content or facilitate private communications. Even for consumer-facing services, the fundamental rights impacts of requiring providers to remove content may vary significantly between services (e.g., search vs. a video-hosting service).

- Nature of the content. Content moderation rules should also be sensitive to the nature of the content. For instance, content removal or blocking mandates should apply only to content that applicable law defines as illegal. Rules to address harmful but legal content should focus instead on creating incentives for service providers to adopt systems and processes to minimize risks of harm to users, including by requiring providers to comply with their own contractual digital safety commitments.

- Nature of the illegality. Content moderation rules should also be tailored to the nature of the content's illegality. For instance, certain types of content are universally agreed to be unlawful (e.g., child sexual exploitation and abuse material), while other types of content might be illegal in one context and not another. Where lawfulness or harm turns on context, or the illegality of content is not apparent on its face, this may make certain content moderation obligations (e.g., automated filtering) less appropriate than others (e.g., notice and takedown).

Governments should provide maximum clarity. Where content moderation is involved, there is a fine line between protecting users from illegal content and censorship. Policymakers, regulators, and courts—not digital service providers—must decide where this line should be drawn. To ensure appropriate respect for fundamental rights, the law must be clear and precise, both in its scope and the obligations it imposes. For instance, vague definitions of illegal hate speech could place a burden on technology companies to attempt to ascertain the intent of the speaker. This can be virtually impossible when providers have little or no context, and at a time where the meaning of specific words can change rapidly. Also, because the act of complying with virtually any content moderation obligation will require providers to collect or process personal data, any rules in this area must clearly and explicitly reconcile providers' digital safety requirements with the privacy and other legal obligations applicable to their unique services.

Rules should reward good-faith efforts to remove illegal or harmful content. Even the clearest rules by law or a provider's terms of service will require judgment calls on whether to remove content. To avoid the risk that providers, in seeking to limit their liability, are either too aggressive or too conservative in removing content, any new rules should protect

providers against liability for actions they undertake in good faith to comply with the law or their own terms of service/community guidelines. This should include cases where a provider removes content based on a good-faith belief that it falls within a removal order, or where the provider does not remove content that it reasonably believes to be legal. Where a provider reasonably and in good faith does more than the law requires, it should not thereby be assumed to acquire "knowledge" of content that then subjects the provider to liability.