ANNEXURE

AMCHAM SUBMISSION ON THE DRAFT AMENDMENT TO THE INTERMEDIARY GUIDELINES

- Intermediaries as entities that provide services in the form of online content to end users host a lot of security and privacy issues. The draft amendment of these rules which was issued by Ministry of Electronics and Information technology (MeitY) may result in eroding the safe harbour protection available to intermediaries. Intermediaries in the form of Internet Services providers (ISPs), Search engines, Web Hosts and Website Providers are some players that come under the gamut of affected players. While the end user is free to post or generate content which may be illegal or may infringe someone else's copyright or obscene content, the liability of this content may come to the intermediaries who host or transmit this content.

- The new intermediary guidelines mandate these intermediaries to put forward a set of rules to the user. The set of terms of such regulations have a broad list of categories of content which should not be posted by the user. In these days of fake news and misconstrued arguments, it is important to bring Safe harbour guidelines and not burden the intermediaries.

- ISPs/TSPs should be exempt from the definition of Intermediaries under the act. As they are mere carriers or providing access to internet or connect destinations. No content is generated by the TSPs/ISPs who are already bound by the terms and conditions of their respective license agreements in this regard. Providing same time frame for all categories of intermediaries is unjustified given the varying nature of intermediaries – some of these platform providers have no control on the traffic even if its encrypted.

- While lawfully, free expression online is a human right, the right includes freedom to hold opinions without interference and to seek, receive and impart information which gives more choice, power and opportunity. Online platforms' ability to innovate and operate responsibly.

- The vague legal standards and uncertainty may hamper investments and innovation in the country as it brings uncertainty in the business environment and increases compliance cost for big and small players alike. This also creates barriers to competition and brings an uneven playing field.

- Carefully designed legal frameworks regarding liability for illegal third-party content makes innovation and responsible operation possible for online platforms. These laws make sure that as long as an online platform meets certain conditions, it is not liable for the third-party information, data or communications link which is generated by its users.

- With more than 80% of internet traffic encrypted, the ISPs as a carrier and owner of bandwidth cannot deliver a technological solution to detect, trace or report offenses related to the security of the state. We would further recommend that they advocate against the replacement of "terms and conditions" with "privacy policies." Privacy policies are generally intended to provide users notice about data collection and use practices. User agreements or other terms and

conditions are more appropriate vehicles for providing users notices about what they may or not be able to post on a given platform. Given the trend to have reader friendly privacy policies, this rule that mandates content unrelated to privacy would introduce confusion and complexity.

- The proposal also introduces the need of 'Traceability' which violates the provision of end-to-end encryption through some service providers and while the state would want to trace the source of messages which are inducing violence or fake news, it endangers the promise of end-to-end encryption by larger platforms. The free flow of information is essential to creativity and innovation and leads to economic growth for companies and countries alike.

- There is a need for clear rules for today which promise flexibility for tomorrow. When platforms follow their removal obligations under the law, they should be certain that they will not be held liable for the third party hosted content. It must also be noted that because technological change can render language obsolete, safe harbours should not be limited to enumerate lists of services or technologies or conditions, but should be allowed to operate on certain broad universally accepted principles.

- While it is important for platform to take down content through a notice-and-take down approach, it is important that there should not be rigid timelines for content removal which imposed short turnaround times. This inhibits companies from carefully considering the merits of each supposed infraction.

- The lack of procedural safeguards brings uncertainty on the circumstances under which intrusive and potentially privacy endangering requests can be made, and who can make such requests. Adding to the concern, extremely strict and short-term limits for direct compliance leads intermediaries with no time to address unlawful requests. Recent amendments in the Aadhaar Act also rule out that unfettered access to citizen data would not be permitted and it is important for the country to not undergo such legal changes that prove to be unstable.

- In the regulation to require intermediaries to implement proactive measures, it has become difficult for intermediaries to work sustainably. If failing to filter a particular piece of content which could endanger a service and its legal whether through fines or engineering changes, then platforms can't take a fair approach to content removals and will have to take a 'better safe than sorry approach' which in this case mean 'take down first, ask questions later'.

- Self-regulation in terms of conducting due diligence and removing the content will also have concerns. ISPs under their telecom license issued under the Indian Telegraph Act, 1885 need to ensure privacy of its customer with no deep packet inspection. Given such mandates it is not possible to expect ISPs to check their customer traffic in the name of conducting due diligence. This is also at variance with section 79 of the IT Act 2000 which extends safe harbor. Even with DPI ISPs will not be able to look within IP packets payloads due to encryption of social media transmission. Therefore, even if this amendment/rule overrides previous privacy acts, ISP may not be able to implement it.

- 'One Size Fits all' standard or principle of review and reviewing content is not appropriate. Online content sharing platforms that actually host the content must be distinguished from other

services that may not have direct access to content, electronics communication services, and enterprise B2B services. Here, instead of the enterprise cloud provider, the business entity providing the end service to its users or customers is in a more appropriate position to handle removal and user information requests along with conducting proactive monitoring.

- Removal of Provision: The lack of clarity, technical infeasibility (especially for smaller players), potential for breach of privacy via surveillance and subjectivity in enforcement are all reasons why this provision should be removed. Alternatively, the provision should provide clarity on terms such as 'enable tracing', define criteria of what would be 'sufficient' when it comes to user information that can be collected by providers and limit the scope of requests that can be made under the rule to prevent 'one to many' matching of content, etc.

- Graded Content Takedown Time Limits: In situations of an emergency, where the content relates to public wrongs and meets the criteria / grounds laid down in Sec 69A of the IT Act, it may be tenable to impose a certain median time lines, but for content that relates to private disputes/wrongs and has a free speech element such as defamation, it would be unreasonable to impose such a strict timeline for intermediaries to act. Some ISPs are not capable of complying due to predominant use of encryption is social media transmission and should be granted exception.

- The extended retention period introduces significant burden on intermediaries from increased costs to storing, protecting, and administering the retained data.

- Stop the Clock Provisions: In all instances, the provision should also contain "Stop the Clock" provisions by listing out a set of criteria (such as seeking clarifications, technical infeasibility, etc.) under which the time limit would cease to apply to allow for due process and fair play in enforcing such requests.