SECTION BY SECTION

Changes to subsection (c)

DOJ proposes to revise (c)(1) to include a new subparagraph (B) to make clear that decisions to remove or restrict access to material are governed solely by (c)(2).

DOJ proposes to revise (c)(1) to include a new subparagraph (C) which would clarify that any content-moderation decision made by a provider in good faith and consistent with its terms of service does not, on its own, render a platform a speaker or publisher for all other third-party content on its service. This subsection would make clear that *Stratton Oakmont v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. 1995) continues to be explicitly overruled and avoids the "Moderator's Dilemma" in which a platform faces increased liability for good faith moderation of offensive content.

DOJ proposes to revise subsection (c)(2) to replace the vague term "otherwise objectionable" with four additional categories of harmful content, including promoting terrorism, promoting violent extremism, promoting self-harm, and unlawful. The proposal would also limit the immunity in subsection (c)(2) to content-moderation decisions made in good faith and based on an objectively reasonable belief that the materials falls within the enumerated categories.

New subsection (d)

DOJ proposes to add a new subsection (d) and to redesignate current subsection (d) as subsection (e). The new subsection (d) would create certain exclusions from immunity.

New subsection (d) would, under certain conditions, remove the immunity from liability that an interactive computer service provider would otherwise possess under subsection (c).

Specifically, subsection (d)(1) would remove the immunity, for purposes of prosecutions and civil actions not already removed by current subsection (e)(1), to be redesignated as subsection (f)(1), from an interactive computer service provider that acted purposefully with the conscious object to promote, solicit, or facilitate material or activity by another information content provider that the service provider knew, or had reason to believe, would violate federal criminal law.

New subsection (d)(2) would remove the immunity from an interactive computer service provider under (c)(1), for purposes of a prosecution or civil action related to a specific instance of material or activity that, if knowingly disseminated or engaged in, would violate federal criminal law, if the provider had actual notice of the material's or activity's presence on the service and its unlawfulness, yet failed to remove or restrict access to the material, report to law enforcement where required by law, or preserve related evidence.

New subsection (d)(3) would remove the immunity protections of subsections (c)(1) and (c)(2) for any interactive computer service provider that receives a final court judgment indicating that illegal content or activity is on its platform but fails to remove that illegal content within a

reasonable time. It would also provide immunity for platforms that take down content consistent with this provision.

New subsection (d)(4) would require interactive computer service providers to offer easily accessible and apparent mechanisms for users to notify providers of unlawful content as described in subsection (d)(2) and (3), and would bar (c)(1) immunity if an interactive computer service provider is not able to receive actual notice of federal criminal material and comply with the requirements of (d)(2)(C).

Current subsection (d) is re-designated as subsection (e).

Changes to current subsection (e), now re-designated subsection (f)

Subsection (e) in the current statute is now re-designated subsection (f).

DOJ proposes a number of additions to the exclusions from Section 230 immunity.

The changes to current subsection (e)(1) would ensure that Section 230 immunity could not be used as a defense against the federal government in civil enforcement actions. The changes would clarify that all enforcement actions brought by the Federal Government are not subject to claims of Section 230 immunity, including civil enforcement actions.

New paragraphs (6), (7), and (8) would preclude the immunity protections of subsections (c)(1) and (2) from being invoked in any civil action involving 18 U.S.C. §§ 2333, 2255, or 2261A(2), which relate to terrorism, child sex abuse, and cyber-stalking, respectively.

New paragraph (9) would make clear that Section 230 cannot be used to immunize actions that would violate the federal antitrust laws.

New definitions in current subsection (f) (to be redesignated as subsection (g))

Subsection (f), which defines various terms as used in Section 230, would be redesignated as subsection (g).

Within that new subsection (g), the Department proposes additional clarifying language to the definition of "**information content provider**" in paragraph (3) to provide examples of actions that would render a platform "responsible in whole or in part" for creation or development of content and therefore unable to rely on Section 230 immunity.

Within that new subsection (g), new paragraph (5) would define **"good faith"** under subsection (c)(2). It would provide that, to restrict access to particular content in "good faith," a provider must meet four criteria. First, it must have publicly available terms of service or use that state plainly, and with particularity, the criteria the service will employ in its content moderation

practices (A). Second, any restrictions on access must be consistent with those terms of service or use and with any official representations or disclosures regarding the service provider's content-moderation policies (B). Third, a provider must not base its decisions on pretextual or deceptive grounds or treat content inconsistently with similarly situated material that it intentionally declines to restrict (C). And fourth, the provider must supply the provider of the content with a notice explaining the basis for the restriction on access and a meaningful opportunity to respond, unless such notice would interfere with law enforcement, would risk notifying a terrorist or criminal, or would risk imminent harm to others (D).