

Autoridade Nacional de Proteção de Dados (ANPD)
Superintendência de Regulação
Coordenação-Geral de Normatização
Brasília, Distrito Federal, Brazil

RE: *Association for Competitive Technology (ACT) Comments on the Draft Guia Orientativo
“Providers of Information Technology Products or Services: Scope and General
Obligations under the ECA Digital” (Law No. 15.211/2025)*

On behalf of the Association for Competitive Technology (ACT), we respectfully submit these comments in response to the Tomada de Subsídios on the draft guidance addressing the scope and general obligations of providers of information technology products or services under the Estatuto Digital da Criança e do Adolescente (ECA Digital), Law No. 15.211/2025.

I. Introduction and Statement of Interest

ACT represents small business innovators and startups in the software development and technology space located in Brazil and around the world. Our members build the products and services that drive the digital economy by improving productivity, advancing education, and helping people lead healthier lives. The app economy supports significant economic activity and employment in Brazil and globally.¹ Small developers and startups account for a meaningful share of that activity, and a clear and proportionate regulatory environment is essential to preserving their ability to compete and innovate.

ACT and our members share the ANPD’s commitment to protecting children and adolescents online and to empowering families with meaningful tools to manage young people’s digital experiences. We take this responsibility seriously and support policies that genuinely improve online safety without unintentionally undermining privacy, innovation, or legal clarity. We welcome the ANPD’s decision to seek input through this Tomada de Subsídios and its stated

¹Association for Competitive Technology (ACT), “State of the App Economy,” actonline.org. ACT also publishes research on the cost of digital regulation for small developers, including market-specific analyses.

objective of providing greater predictability and legal certainty to regulated parties. Clear, well-scoped definitions are especially important for the micro, small, and medium-sized developers who lack the legal and compliance resources of large platforms.

II. General Views and Recommendations

ACT and our members approach online safety from a position of shared purpose with regulators around the world. We support measures that protect children and adolescents from genuine online harms and that give parents and guardians effective tools to guide their children's experiences. We have consistently maintained that the most durable protections come from a layered, shared-responsibility model, in which each participant in the digital ecosystem contributes according to its role and capacity, rather than one that concentrates the entire compliance burden on individual small developers that have neither the data nor the resources to carry it.

On age assurance in particular, ACT's view is that the level of assurance applied to a service should be proportionate to the risk the service actually presents to young users. Broad mandates that require every service, or every user of an application store, to undergo intrusive identity-based age verification tend to be counterproductive. They compel the large-scale collection and retention of sensitive personal data, including government identity documents, creating concentrated repositories that become attractive targets for malicious actors and that place the data of children and adults alike at risk. Independent security researchers have repeatedly cautioned that age-verification technologies remain immature and carry significant privacy and security risks, and that requiring reliable verification for every interaction would centralize sensitive data in the hands of a small number of large gatekeepers.

For these reasons, ACT favors approaches that are privacy-preserving, data-minimizing, and technology-neutral. Age assurance should rely on the least amount of personal data necessary, should not be tied to a single prescribed method, and should leave room for continued innovation in privacy-protective techniques. We also support empowering parents and guardians directly, through accessible and effective parental controls and device and account settings, rather than relying on a single age check at one gateway. Families consistently express a preference for protections that operate continuously as young people use a service, which a one-time verification event at the point of download or sign-up cannot provide.

Finally, ACT supports safety-by-design as a core strategy, including privacy defaults for younger users, sensible limits on the profiling of minors, robust parental controls, and clear transparency. Protections of this kind advance the goals of child-safety frameworks while preserving the openness, competition, and innovation that allow small developers to serve users of all ages.

III. Specific Recommendations on the Draft Guidance

a. Define “likely access” (acesso provável) with objective, predictable, and proportionate criteria.

The concept of “likely access” in Article 1, sole paragraph, is the single most consequential determinant of who must comply with the law. The draft guidance identifies three factors for assessing likely access, namely the attractiveness of the service to children and adolescents, the ease of access and use, and the possibility of exposure to risks to privacy, security, or biopsychosocial development. ACT encourages the ANPD to apply these factors so that the standard turns on a demonstrable likelihood of meaningful child access rather than the mere theoretical possibility that a minor could reach a service. Almost any general-purpose online service is theoretically accessible to a minor, and an overly broad reading would sweep in business-to-business tools, infrastructure and back-end services, and general-purpose products that are neither designed for nor meaningfully used by children. That result would dilute protective resources without advancing the safety of young users.

ACT respectfully requests that the ANPD clarify whether the relevant criteria are cumulative, alternative, or graduated, and that it adopt a graduated and proportionate reading. We encourage the ANPD to provide objective, illustrative examples of services that are and are not within scope, including clear negative examples, so that a small developer can self-assess its status with confidence. Predictable criteria reduce the incentive for defensive over-compliance, which is particularly costly for small developers and can lead to the unnecessary collection of personal data.

b. Provide precise definitions of the core service categories to avoid inadvertently capturing small-developer and general-purpose tools.

The draft guidance interprets several foundational terms, including “information technology product or service,” “social networks,” “internet application stores,” “operating systems,” and “services with editorial control.” ACT encourages the ANPD to define each term precisely and to accompany each with concrete examples and out-of-scope cases. Without clear boundaries, broadly worded categories risk capturing developers and intermediaries whose products bear little relationship to the risks the law targets. Clear delineation of these categories, and of how obligations are allocated across different actors in the digital chain, will reduce duplicative or conflicting compliance expectations and give small developers a workable understanding of their responsibilities.

c. Interpret the duty of prevention (dever de prevenção) as proportionate, risk-based, and outcome-oriented.

ACT supports the draft guidance's recognition that the duty of prevention under Article 5 is the central organizing principle of the ECA Digital. We encourage the ANPD to interpret this duty as a proportionate, risk-based, and outcome-oriented standard rather than a prescriptive, one-size-fits-all checklist. The law itself contemplates that obligations vary according to the characteristics and functionality of the service, the degree of control the provider exercises over content, the number of users, and the size of the economic agent. The guidance should give full effect to that calibration so that the expectations placed on a low-risk small developer are commensurate with the risk its service presents.

Consistent with this approach, ACT requests that the ANPD recognize a reasonable, good-faith standard of compliance and consider safe harbors or compliance assurances for providers that conduct and act upon good-faith risk assessments. Recognizing genuine, documented efforts to identify and mitigate risk will promote consistent application of the law, encourage proactive safety work, and reduce uncertainty, particularly for smaller providers.

d. Preserve a privacy-preserving, technology-neutral, and data-minimizing posture.

Although the mechanics of age assurance are the subject of a separate Tomada de Subsídios, the scope and general-obligations guidance will shape the data-collection behavior of regulated providers. ACT encourages the ANPD to ensure that the guidance does not, directly or indirectly, push providers toward collecting more personal data than necessary. Mandating that age information be collected and transmitted to all providers requires them to divert limited resources to building or expanding technical infrastructure, and the receipt and storage of such information creates new security risks and may trigger additional legal obligations even where a service is not designed for or marketed to children.²

ACT therefore encourages a flexible, technology-neutral approach that supports diverse, privacy-preserving methods rather than rigid identity-verification requirements that could compel sensitive data collection and burden small developers with costly compliance barriers. We also prioritize safety-by-design measures such as high privacy defaults, limits on profiling of minors,

²In March 2026, the cybersecurity outlet Cybernews reported that a global identity-verification provider left more than 203 million sensitive consumer records exposed, underscoring that requirements pushing services toward large-scale collection and storage of age or identity data create high-value targets for bad actors and place users, including minors, at risk.

robust parental controls, and clear user transparency, and we ask that these measures be embraced as central tools for achieving the law’s protective goals.

e. Adopt an iterative implementation approach with proportionate expectations for smaller developers.

Finally, ACT recommends an iterative implementation approach that includes reasonable timelines, proportionate expectations calibrated to provider size and risk, and ongoing engagement with the small-developer community. Given the technical and operational complexity of child-safety measures, continued dialogue will be essential to ensure the framework achieves its objectives without creating unnecessary fragmentation or barriers to innovation. Coordinating this guidance with the ANPD’s parallel work on age-assurance mechanisms, and with established international approaches, will further reduce uncertainty and duplicative compliance burdens for developers that operate across borders.

IV. Conclusion

ACT appreciates the opportunity to contribute to this Tomada de Subsídios and would welcome the opportunity to engage further with the ANPD as this guidance and the broader ECA Digital framework are finalized and refined.

Sincerely,

A handwritten signature in black ink, appearing to read 'B. Scarpelli', with a stylized, cursive script.

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Global Policy Counsel

Association for Competitive Technology
1401 K St NW (Ste 501)
Washington, DC 20005
United States