16 June 2026

Association for Competitive Technology

Comision de Regulacion de Comunicaciones (CRC)
Coordinacion de Prospectiva Estrategica e Innovacion
Calle 59A BIS No. 5-53, Edificio Link Siete Sesenta, Piso 9
Bogota, D.C., Colombia
Codigo Postal 110231

RE: Comments of the Association for Competitive Technology (ACT) on the Study "Monetization in the Content Industry, Traffic and Unsolicited Content" (Study Code 11000-41-3-1) and the accompanying Technical Consultation on Methodologies for Measuring Unsolicited Traffic in Digital Services and Platforms

I. Introduction and Statement of Interest

The Association for Competitive Technology (ACT) appreciates the opportunity to provide input to the Comision de Regulacion de Comunicaciones (CRC) on its study "Monetization in the Content Industry, Traffic and Unsolicited Content" and the accompanying technical consultation on methodologies for measuring unsolicited traffic.[1]

ACT is the leading global association for small businesses and startups that develop the technology that is transforming the world. Our members are entrepreneurs, independent software developers, and small firms across the global application ecosystem who build internet-enabled products and services for consumers and businesses in every sector, including health, education, communications, and commerce. Many of our members build and distribute the kinds of applications the Study examines, and many serve or aspire to serve Colombian consumers and businesses.

[1] Comision de Regulacion de Comunicaciones, Estudio "Monetizacion en la Industria de Contenidos, Trafico y Contenido No Solicitado" (Resumen para consulta, Codigo 11000-41-3-1, May 2026), and accompanying "Consulta tecnica sobre metodologias para la medicion de trafico no solicitado en servicios y plataformas digitales." Available at https://www.crcom.gov.co/es/noticias/proyectos-regulatorios/crc-abre-consulta-publica-sobre-trafico-no-solicitado-en-redes.

1401 K Street, NW, Suite 501
Washington, D.C. 20005

+1 (202) 331 - 2130 www.ACTonline.org /US-ACT @ACTonline

These comments build on ACT's 31 January 2025 submission to CRC on the "over-the-top" (OTT) 2024 study,[2] of which this Study is the express continuation. ACT supports a rigorous, evidence-based approach to understanding traffic dynamics, and we welcome CRC's stated intent neither to regulate content nor to impose direct obligations on application and service providers, together with its recognition that it lacks legal competence to do so.[3]

II. General Position on the Study and on Network Usage Fees

ACT shares CRC's interest in a competitive and well-functioning digital ecosystem for Colombian consumers and businesses, and in network investment that keeps pace with demand. However, ACT remains concerned with the premise that appears to motivate this CRC Study. ACT fundamentally objects to network usage fees, "fair share" contributions, and sender-pays mechanisms imposed on application and service providers because they rest on the mistaken view that such providers impose uncompensated costs on networks.

In reality, application providers and network operators are complementary. The applications that ACT's small business members build generate the consumer demand for data and bandwidth that drives operators' revenue and justifies their investment in networks. These proposals also ignore that small developers already pay for the delivery of their own services, such as purchasing connectivity, cloud hosting, and content-delivery capacity from third parties, so the cost of carrying their traffic is already borne and is not externalized onto networks. Neither CRC nor any regulator in any other country has demonstrated a market failure that a network fee would cure, and ACT opposes such fees as a matter of principle, not merely of degree.

We are therefore concerned that this Study, although framed as a neutral measurement exercise, risks being used to manufacture an empirical predicate for precisely those fees by recharacterizing ordinary and beneficial application traffic as "unsolicited" and then attributing a cost to it. ACT offers the specific responses below to assist CRC in understanding why the proposed measurement is conceptually unsound and technically infeasible. They are not an endorsement of any methodology, any measurement program, or any path toward network fees or new obligations on application and service providers.

III. Specific Input of ACT on the CRC Study

Initially, we offer three threshold observations to CRC:

- First, the central category of the Study, "unsolicited" or "unintentional" traffic, is imprecise as defined and, if carried into policy, prejudicial. Defining it as traffic transmitted "without a deliberate and unequivocal action of the user" sweeps in a large amount of ordinary application activity that delivers value the user has in fact chosen. The absence of a foreground tap is not the same thing as an absence of consent, demand, or benefit.

[2] Comments of the Association for Competitive Technology (ACT) to CRC Regarding "Study on the role of 'Over the Top' OTT services in Colombia – 2024" (31 January 2025). Available at https://actonline.org/2025/02/10/always-be-filing-act-the-app-association-filing-activity-january-2025/.
[3] Resumen para consulta at Section 2.1, noting that the current legal framework does not grant CRC competence to intervene in the content offered by OTTs, nor competence to require detailed information directly from them, and that the study does not seek to regulate content or impose direct obligations on OTTs.

- Second, a measurement exercise should not become the empirical predicate for network usage fees, "fair share" contributions, or other transfers of value from application providers to network operators. ACT opposes such mechanisms for the reasons set out in our OTT comments, and a study framed as measurement should not be used to manufacture a foundation for them.
- Third, the measurement of these phenomena must not weaken encryption or rely on deep packet inspection. The privacy and security of Colombian users, and the integrity of digital trade, depend on strong encryption remaining intact.

IV. The Definition of "Unsolicited" Traffic Requires Precision (Responsive to Questions 4 through 7.)

ACT discourages CRC from utilizing a "traffic without direct user interaction" test, which would ignore that modern applications routinely transfer data without a discrete tap for each byte precisely in order to serve the user well. Treating that traffic as "unsolicited" mischaracterizes how applications work.

Practically, CRC should distinguish at least four categories before attempting any measurement:

- **Functional, automatic traffic that delivers user-requested value.** This includes content the user is actively consuming, prefetching that makes the next screen load instantly, content delivery network handshakes, message and email synchronization, and security and software updates, as well as the analytics and operational telemetry that developers rely on to detect outages and fraudulent activity and to keep their applications running reliably. Although not directly connected to a tap, the user solicited this traffic by choosing to install and use the application and by reasonably expecting it to function.
- **Configurable traffic operating under the user's own settings and permissions.** Autoplay, background refresh, and notifications are features the user can enable or disable in operating-system or application settings, and that operate according to the configuration the user selected and the permissions the user granted.
- **Advertising traffic supporting an understood value exchange.** Ad-supported applications provide a service to the user at no monetary cost in exchange for advertising. This is a transparent and widely understood model, not "unsolicited" traffic in any meaningful sense, and it is the model on which a large share of small developers depend to reach users.
- **Genuinely unrequested or manipulative traffic.** A narrow residual category of traffic that delivers no value the user sought and that the user did not authorize.

The vast majority of the mechanisms the Study lists fall into the first three categories. If CRC proceeds with its study, a realistic starting definition would be traffic that is not necessary for the service the user has chosen and not authorized by the user's settings or permissions (and ACT therefore believes the answer to Question 7 is no). Indeed, not all traffic that occurs without direct interaction is unsolicited, so CRC should separate its categories by functional necessity, user configuration and permission, and disclosure, not the mere presence or absence of a tap.

V. User Intent Is Not Observable from the Network, and Network-Based Measurement Has Severe Limits (Responsive to Questions 6, 8 through 11, and 15.)

Although a network operator can observe traffic volume, timing, protocol, and at times a destination IP address or domain, an operator cannot observe user intent. Whether a given byte was "solicited" is a question about the user's expectations and the application's function, and that information is simply not present in network metadata. In fact, as users may have different goals and life experiences when visiting an application, functionally equivalent network data could have different user intents.

Several well-documented and necessary features of the modern internet make network-side attribution of traffic to "solicited" versus "unsolicited" categories unreliable. These include the general use of encryption (HTTPS, QUIC, and TLS 1.3, with Encrypted Client Hello further removing visibility of the Server Name Indication), the use of content delivery networks and shared domains, the multiplexing of connections, and dynamic addressing. The Study itself acknowledges these constraints. As a result, in answer to Question 10, the viability of distinguishing intentional from unintentional traffic using network metadata alone is low, and for several typologies it is not possible. Any classification built on network metadata alone would carry high false-positive and false-negative rates, which Question 11 itself asks respondents to address.

From a practical perspective, because network metadata cannot reliably separate solicited from unsolicited traffic, any aggregate figure produced that way would carry large and largely unquantifiable error. Such a figure should not be presented as a measurement of "unsolicited traffic," and it should not be used as a basis for policy or to justify value transfers between parties.

VI. Measurement Must Not Weaken Encryption or Rely on Deep Packet Inspection (Responsive to Question 16, and consistent with ACT's OTT comments.)

ACT strongly supports the continued use of strong encryption, which protects Colombian users from fraud, identity theft, and unlawful surveillance, and underpins the trust on which digital trade depends. Deep packet inspection or HTTPS interception undertaken in order to measure traffic would be disproportionate to a measurement objective, would introduce security vulnerabilities, and would raise serious privacy and lawful-interception concerns.[4]

In direct answer to Question 16, ACT believes that it is viable to study these phenomena without deep packet inspection, but only through device-side and experimental methods rather than network inspection. Such a study may be possible via controlled laboratory experiments such as a device-side study conducted on representative applications with informed consent, potentially user-consented measurement panels, or aggregated and anonymized analysis. However, network deep packet inspection should be excluded from the toolkit entirely.

[4] The Resumen para consulta itself notes the security challenges that the European Union Agency for Cybersecurity (ENISA) has documented in connection with the inspection of encrypted traffic and HTTPS interception.

VII. The Proposed Measurement Is Technically Infeasible (Responsive to Questions 12 through 14 and 18 through 22.)

As noted above, ACT does not endorse any methodology for measuring so-called unsolicited traffic because ACT objects to the premise of the exercise and to the use to which any resulting measurement would be put. Each of the methods CRC raises faces fundamental limitations that prevent it from reliably distinguishing solicited from unsolicited traffic, generalizing beyond a single tested application, or attributing a defensible cost to the traffic observed. Challenges include:

- **Advertising and trackers (Question 18).** No available method can establish from traffic volume whether the user sought or valued the underlying service. Laboratory capture and black-box measurement can at most approximate volumes for one tested application and version, which cannot support a generalizable measurement or any defensible cost attribution.
- **Background activity (Question 19).** No method can reliably separate functionally necessary synchronization, such as security updates and messaging, from discretionary activity without device-level context (e.g., user settings) that the network operator does not possess and cannot obtain at population scale.
- **Autoplay (Question 20).** Autoplay is user-configurable and is frequently switched off, so any measurement that does not record each user's setting state, which network and black-box methods cannot, will systematically misclassify it.
- **Prefetch and preload (Question 21).** Prefetch delivers latency reduction and offline availability that the user receives in return for the data used. Measuring its volume in isolation, without netting those benefits, measures nothing meaningful.
- **"Dark patterns" and user-experience design (Question 22).** "Dark pattern" is a contested, normative label, not a measurable network quantity. Infinite scroll, a default autoplay setting, and notifications are not manipulative as such, and are standard, beneficial, and user-controllable. No method can measure manipulation from traffic, and attempting to do so would simply relabel ordinary, beneficial design as harm.

Taken together, these limitations mean that the measurement CRC proposes cannot produce a reliable, generalizable, or policy-grade figure for unsolicited traffic. Laboratory conditions do not equal field conditions, black-box measurement cannot read user intent, panels carry selection bias, and results are specific to the application, version, and moment tested. A figure produced in spite of these limitations would be unfit to support any regulatory conclusion, and in particular unfit to justify network fees or new obligations on application and service providers.

VIII. Any Impact Assessment Must Be Even-Handed (Responsive to Question 17.)

The impacts CRC proposes to measure, which include unnecessary data consumption, cost to the user, network congestion, competitive advantage for platforms, and loss of user control, are inherently weighted toward harm. A credible study must weigh the benefits of these features against their costs. For example, prefetching reduces latency and enables offline use, background synchronization delivers timely email, messages, and security updates, and advertising-supported delivery gives small developers a way to offer their applications to users at no monetary cost.

The non-Colombian and dated figures the Study cites should not be transposed to Colombia without current, local, and methodologically robust evidence.[5] Any competition concern CRC would act on should rest on a strong, data-driven record, not on edge cases or hypotheticals. The Study's own observation that small participants bear these costs disproportionately, while large platforms absorb them, confirms that any remedy should not fall on ACT's small business members, who use standard, off-the-shelf delivery techniques, advertising networks, and platform defaults that they do not control.

IX. The Study Provides No Basis for Network Usage Fees or New Obligations on Application Providers

ACT opposes network usage fees on application and service providers as a matter of principle, irrespective of how any traffic might be measured. We reiterate that application and service providers and network operators perform different and complementary roles, and are not substitutable. A "fair share" or sender-pays mechanism would improperly conflate these two roles, would damage the digital ecosystem, and would fall hardest on the small developers least able to absorb new per-byte costs or to negotiate with network operators.

The imposition of network usage fees on application and service providers would fragment the digital economy and place Colombia at a significant disadvantage. Such fees would create a Colombia-specific cost and liability that does not exist in other markets, splintering a single, borderless internet into a patchwork of national toll regimes. Small developers reach customers worldwide precisely because the marginal cost of serving an additional market is low, and they would be among the first to deprioritize or withdraw from a market that singled them out for fees. The result would raise the cost and narrow the range of digital services available to Colombian consumers and businesses, deter inbound investment and local startup formation, and undercut Colombia's competitiveness and its standing in digital trade, including its interest in an open and interoperable global internet.

An OTT network fee would also run counter to the long-standing international norms reflected in joint statements by the United States, United Kingdom, Japan, South Korea, Australia, New Zealand, Singapore, Mexico, Argentina, Peru, Uruguay, and others committing to continue not imposing customs duties on electronic transmissions among themselves.[6] A fee would also run counter to the plurilateral WTO Agreement on Electronic Commerce (ECA), which contains a permanent commitment not to impose customs duties on electronic transmissions for participating members.[7]

[5] The figures cited in the Resumen para consulta (for example, estimates drawn from Silva et al. (2020) and Papadopoulos et al. (2018)) derive from specific, dated, and non-Colombian measurement contexts and should not be transposed to Colombia without current, local, and methodologically robust evidence.
[6] See https://www.wto.org/english/tratop_e/ecom_e/ecom_work_programme_e.htm.
[7] See https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm.

X. Conclusion

ACT appreciates the opportunity to provide its views and can offer any further information that would assist CRC. We urge CRC to define the phenomenon it is studying with precision, to preserve strong encryption and user privacy, to weigh the benefits of these features alongside their costs, and, above all, not to allow a measurement exercise to become the foundation for network fees. Such fees would fragment the digital economy and place Colombia, and the small developers who serve its consumers and businesses, at a disadvantage in digital trade.

Respectfully submitted,

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