THE FREEDOM OF EXPRESSION LEGAL NETWORK

Ms Nonkqubela Jordan-Dyani
Director General,
Department of Communications and Communications
Email: fwpsa2025@dcdt.gov.za

26 September 2025

Dear Ms Jordan-Dyani

FREEDOM OF EXPRESSION LEGAL NETWORK: SUBMISSION ON THE DRAFT WHITE PAPER 2025

1. INTRODUCTION

1.1 On 11 July 2025, the Department of Communications and Digital Technologies (Department) issued the Draft White Paper on Audio and Audiovisual Media Services and Online Safety: in Notice 3369, Government Gazette No. 52972 (Draft White Paper) and invited the public to made submissions thereon. The deadline for such submissions was extended to 26 September 2025 by Notice 6487, Government Gazette No. 53118 dated 5 August 2025.

1.2 The Freedom of Expression Legal Network (FELN) is an association of lawyers and media experts which has been formed to promote and protect the right to freedom of expression enshrined in section 16(1) of the Constitution of the Republic of South Africa, 1996 (the Constitution) and to engage in public processes such as these to secure the right of the public and of the media to the free flow of ideas and information. Several other organisations, namely; the Campaign for Free Expression, the Press Council of South Africa (the Press Council) and the South African National Editors' Forum (SANEF) have endorsed the submissions prepare by FELN.

1.3 FELN thanks the Department for the opportunity to make these written submissions on the Draft White Paper and requests the opportunity to make oral submissions at the public hearings which will doubtless take place in due course.

2. NATURE OF FELN'S SUBMISSIONS

2.1 FELN's expertise spans content governance across both professional media and the wider online environment, advising on the regulatory frameworks and institutions best placed to uphold freedom of expression, pluralism and human-rights standards, and to promote high-quality journalism alongside other credible online content essential to a flourishing, diverse democracy.

2.2 FELN's submissions have a single broad focus, namely, the online content regulation proposals contained in the Draft White Paper.

2.3 The dangers of state-driven control of expression—anchored in brute power rather than universally recognised, harm-based limits—are visible in the United States, where the Trump administration has targeted the media and citizens' information rights.

2.4 On 20 September 2025, US Defence Secretary Pete Hegseth announced rules under which the Pentagon would revoke press credentials unless journalists pledged not to obtain or publish any unauthorised information, even if unclassified. In parallel, the Federal Communications Commission has threatened regulatory action against broadcasters carrying critical late-night political satire (e.g., *Jimmy Kimmel Live!*), leveraging licensing powers in ways that risk chilling lawful speech and editorial judgment.

2.5 That a country often hailed as having the world's strongest constitutional press protections can contemplate such measures underscores the need for constant vigilance to safeguard freedom of expression and the free flow of information for present and future generations.

2.6 At the same time, information access is shifting rapidly. The Reuters Institute's *Digital News Report 2025* shows sharp growth in reliance on social media as a primary news source across Africa, parts of Asia, the United States and South America (notably Brazil). The real-world harms of non-news online content are also clearer—from the first wrongful-death suit against OpenAI after a teen was allegedly encouraged to self-harm by ChatGPT, to the circulation of child-sexual-abuse material (CSAM) involving South African learners on WhatsApp, which Meta removed only on pain of a prospective contempt of court order.

2.7 Calls to regulate harmful online content are therefore intensifying—but so too are the risks of overreach and censorship. The task is to craft safeguards that address demonstrable harms without stifling lawful speech.

2.8 It is this tightrope that the Department is attempting to walk in its fairly spare (at this stage) policy proposals involving online regulation which are found in the following clauses of the Draft White Paper:

2.8.1 Clause 5.3 "Regulatory Mechanisms" which proposes "an ombudsman for the regulation of online media services" which is said to "align with the models of self-regulation"[1].

[1] At clause 5.3.2.

2.8.2 Clause 5.5.3. “Platform Definition and Obligations” which proposes additional obligations be imposed on Video Sharing Platform Services (VSPs) and Very Large Online Platform Services (VLOPs) including requiring that these apply terms and conditions to users that:

2.8.2.1 include content prohibitions on:

2.8.2.1.1 incitement to violence;

2.8.2.1.2 incitement to hatred;

2.8.2.1.3 public provocation to commit terrorist offences;

2.8.2.1.4 content that may impair the physical, mental or moral development of minors;

2.8.2.1.5 advertising in content aimed at children;

2.8.2.2 establishing and operating mechanisms for users of VSPs to report or flag any of the above content and which explain to users actions taken in response to reporting and flagging;

2.8.2.3 establishing and operating systems allowing user rating of content on such platforms;

2.8.2.4 establishing and operating age verification systems of VSPs and parental control systems for content which may prepare the physical, mental and moral development of minors; and

2.8.2.5 providing for effective media literacy measures and tools raising awareness thereof.

2.8.3 Clause 6.4.3 which proposes that existing regulatory bodies, including self- and co-regulatory bodies, “will be invited to submit proposals to support the creation of an ombud function specifically to regulate the online environment within their scope” in the First Stage of policy development.

2.9 In responding to the Draft White Paper’s policy proposals on online content regulation, FELN submissions concentrate on the following key issues:

2.9.1 the internationally-accepted standards that justify content regulation, that is, what content justifies restrictions on freedom of expression;

2.9.2 the internationally-accepted standards for bodies or institutions that engage in content regulation, that is, which institutions are appropriate to regulate online content;

2.9.3 from there, to propose a constitutionally-compliant model for online content regulation for the country using, where possible, existing laws and institutions to avoid burdening the state with the task of establishing and funding a plethora of institutions with overlapping mandates leading to forum shopping by online content providers and general confusion among the public as to which institution is best placed to deal with a complaint or concern regarding online content particularly on social media platforms.

3. INTERNATIONALLY-ACCEPTED GROUNDS FOR RESTRICTING CONTENT

3.1 There is obviously no closed list of enumerated grounds for restricting content, whether online or otherwise.

3.2 However, there are grounds for restricting traditional media content[2] which have found acceptance in numerous international instruments, statements and declarations and we set out fourteen of these below:

3.2.1 **the right to prohibit broadcasting content unless authorised in terms of a licence[3]**. This is an important restriction to point out because the rationale for requiring the licensing of broadcasters and the acceptance of the imposition of detailed content restrictions on broadcasters is the scarcity rationale, that is, the fact that broadcasters use scarce and finite radio frequency spectrum resources to communicate with the public. There is no scarcity rationale for traditional print media nor, it is important to point out, for online media or for non-media content distributed online, that is, for online media, that is media distributed via the public internet;

3.2.2 **protecting reputations[4].** In balancing the right to freedom of expression vs the right to reputation it is clear that the public interest in disclosure is put ahead of reputations, particularly of public figures, and that criminal defamation, and particularly the imposition of custodial sentences therefor, is not appropriate[5] as has been ruled by the African Court on Human and Peoples' Rights;

[2] See generally Chapter 3, Limpitlaw J, *Media Law Handbook for Southern Africa*, Volume 1 Konrad Ardenauer Stiftung (2021).
[3] Article 10(1) of the European Convention on Human Rights.
[4] Protected under numerous international documents including: Principles 3.3, 21.1., 22.3, 22.4 of the African Principles on Freedom of Expression and Access to Information Declaration; the Dakar Declaration, Article 10(2) of the European convention on Human Rights, Article 19(3)(a) of the International Covenant on Civil and Political Rights, Resolution 169 of the African Commission on Human and Peoples' Rights, Unesco's Media Development Indicators.
[5] Konate v Burkina Faso https://africanlii.org/akn/aa-au/judgment/afchpr/2014/42/eng@2014-12-05

3.2.3 **protecting the rights of others generally[6].** It is important to recognise that often the rights of others are protected under specific grounds, such as the right to reputation but this does not include the right not to be offended, shocked or disturbed by expression;

3.2.4 **protecting privacy[7].** It is important to note that it is recognised that the right to privacy can be overridden in the public interest and that public officials have less compelling reason for claiming the right to privacy;

3.2.5 **regulating obscenity and protecting children and morals[8].** Most countries have laws regulating obscene content or materials aimed at children although many countries are moving away from regulating content on the grounds of "morality" given the subjective nature thereof. Further many countries impose time/manner/place restrictions such as packaging requirements, age restrictions, watershed periods and the like in respect of obscene content rather than prohibiting the publication thereof;

3.2.6 **propaganda for war[9].** Not only is this an internationally recognised ground for regulating content, but the Department will be aware that this form of expression is not protected under section 16(1) of the Constitution in terms of section 16(2)(a) of the Constitution.

3.2.7 **Hate speech[10]** Not only is this an internationally recognised ground for regulating content, but the Department will be aware that this form of expression is also not protected under section 16(1) of the Constitution in terms of section 16(2)(c) of the Constitution. The contours of hate speech have been the subject of a great deal of litigation in our courts and in the leading case of *Qwelane v South African Human Rights Commission and Another*[11] the Constitutional Court held that term "harmful" in relevant

[6] Protected under numerous international documents including: Principle 23.3 of the African Principles on Freedom of Expression and Access to Information Declaration, Article 10(2) of the European Convention on Human Rights, Article 19(3)(a) of the International Covenant on Civil and Political Rights, and Article 58 of the World Summit on the Information Society's Geneva Principles.

[7] Protected under numerous international documents including: Principle 22.3 of the African Principles on Freedom of Expression and Access to Information Declaration, the Unesco's Media Development Indicators and Article 58 of the WSIS Geneva Principles.

[8] Protected under numerous international documents including: Principle 3.3 of the African Principles on Freedom of Expression and Access to Information Declaration, Article 10(2) of the European convention on Human Rights, Article 19(3)(b) of the International Covenant on Civil and Political Rights, Article 29(3)(a) of the Malobo Convention, ie African Union Convention on Cybersecurity and Personal Data Protection, the Unesco's Media Development Indicators and Article 58 of the World Summit on the Information Society's Geneva Principles.

[9] Article 20(1) of the International Covenant on Civil and Political Rights.

[10] Protected under numerous international documents including: Principles 3.3 and 22.4 of the African Principles on Freedom of Expression and Access to Information Declaration, Principle 12 of the Camden Principles on Freedom of Expression and Equality developed by Article XIX, Article 10(2) of the European Convention on Human Rights, Article 19(3)(b) of the International Covenant on Civil and Political Rights, Article 29(3)(e), (g) and (h) of the Malobo Convention, ie African Union Convention on Cybersecurity and Personal Data Protection, the Unesco Media Development Indicators and Article 59 of the World Summit on the Information Society's Geneva Principles.

[11] 2021 (6) SA 579 (CC).

legislation imposing restrictions on hate speech was constitutional but the term "hurtful" was impermissibly vague in that context. Further, it broadened its interpretation of the constitutional parameters of hate speech to include hate speech on the grounds of sexual orientation;

3.2.8 **Protection of national security or territorial integrity[12].** While protecting national security or territorial integrity are legitimate grounds for regulating and even prohibiting expression, this cannot inhibit public debate on matters of public concern and cannot be used to, for example, protect a government from embarrassing scrutiny or concealing information about the functioning of its public institutions.

3.2.9 **War or state of emergency[13].** It is recognised that being in a state of war or emergency are legitimate grounds for regulating and even prohibiting expression. However this can be done only for the period of time strictly necessary in the circumstances.

3.2.10 **Protection of public order or safety[14].** For these grounds to be legitimate bases for regulation or prohibition of expression there has to be a real risk to public order or safety and a close causal link between the risk of such harm and expression.

3.2.11 **Protection of public health[15].** Note that there were instances of governments using prohibitions on misinformation during the Covid 19 Pandemic to stifle legitimate criticism of official pandemic responses[16].

3.2.12 **Maintaining the authority and impartiality of the judiciary[17].** Maintained generally through contempt of court laws.

---

[12] Protected under numerous international documents including: Principle 23.1 of the African Principles on Freedom of Expression and Access to Information Declaration, Principles 1(c) and (d) and read with Principles 2(a) and (b) and Principle 23 of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information developed by Article XIX, Article 20(2) of the International Covenant on Civil and Political Rights, and the Unesco Media Development Indicators.

[13] Protected under numerous international documents including: Article 15(1) of the European Convention on Human Rights, Principles 3 and 23 of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information developed by Article XIX, and the Unesco Media Development Indicators.

[14] Protected under numerous international documents including: Principles 3.3 and 9.3.b of the African Principles on Freedom of Expression and Access to Information Declaration, Article 10(2) of the European Convention on Human Rights, and Article 19(3)(b) of the International Covenant on Civil and Political Rights.

[15] Protected under numerous international documents including: Principles 3.3 and 9.3.b of the African Principles on Freedom of Expression and Access to Information Declaration, Article 10(2) of the European Convention on Human Rights, and Article 19(3)(b) of the International Covenant on Civil and Political Rights.

[16] https://www.cima.ned.org/publication/chilling-legislation/

[17] Protected under Article 10(2) of the European Convention on Human Rights and Unesco's Media Development Indicators.

3.2.13 **For the prevention of crime[18].**

3.2.14 **To prevent the disclosure of information received in confidence[19].** This provision operates to protect the government's ability to secure the free flow of confidential information to itself and to protect the media's ability to guarantee confidentiality to sources of information. Some countries protect the former and not the latter.

3.3 It is noteworthy that "untruth" is not an internationally-accepted ground for content regulation or prohibition outside of the narrowly tailored ground of defamation to which "truth in the public interest" is often a defence. However, although the term is not used in the Draft White Paper there has been a lot of public discussion about "information integrity" and the societal harms that can arise from so-called "fake news" and mis-and dis-information online. In the Draft White Paper, the Department talks about the creation of an ombudsman for the regulation of "online media services". But these are not clearly defined, and it is not clear if these would include social-media platforms such as Tik Tok, X, Facebook, Instagram, WhatsApp and the like. We urge and assume that the proposed ombud will be invested with jurisdiction in respect of social media platforms. To this end, we refer the Department to the 2017 *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda*[20] (the Disinformation Declaration) developed by the United Nations' Special Rapporteur on Freedom of Opinion and Expression, the Organisation for Security and Cooperation in Europe's Representative on Freedom of the Media, the Organisation of American States' Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights' Special Rapporteur on Freedom of Expression and Access to Information. In this regard:

3.3.1 The Disinformation Declaration sets out principles regarding the roles and responsibilities of platforms hosting social media or other third-party content:

3.3.1.1 In principle 1.d it is stated that "*Intermediaries should never be liable for any third-party content… unless they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it and they have the technical capacity to do that*."

[18] Protected under Article 10(2) of the European Convention on Human Rights.

[19] Protected under Article 10(2) of the European Convention on Human Rights.

[20] https://www.osce.org/fom/302796

3.3.1.2 In principle 4.e it is stated that "*Intermediaries should support the research and development of appropriate technological solutions to disinformation and propaganda which users may apply on a voluntary basis. [Intermediaries] should cooperate with initiatives that offer fact-taking services to users…"*

3.3.2 The Disinformation Declaration sets out principles regarding Standards on Disinformation. In principle 2.a it is stated that "*General prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression… and should be abolished.*"

3.3.3 The preamble to the Disinformation Declaration makes clear the concern for "*measures taken by intermediaries to limit access to or the dissemination of digital content, including through automated processes, such as algorithms or digital recognition-based content removal systems, which are not transparent in nature, which fail to respect minimum due process standards and/or which unduly restrict access to or the dissemination of content.*"

4. INTERNATIONALLY-ACCEPTED STANDARDS FOR CONTENT REGULATION BODIES

4.1 As the Department will be aware, civil society organizations have previously raised concerns in their submissions on the First (2020) and Second (2023) Draft White Papers issued by the Department that these documents do not clearly affirm, and at points appear to blur, fundamental principles about who should regulate content and how to safeguard the free flow of information and ideas in the public interest..

4.2 For online platforms, the appropriate model is statutory co-regulation: platforms develop and implement human rights and best practice-aligned codes, but those codes are approved, supervised and enforceable by an independent authority, with transparency, user redress and sanctions for non-compliance. Clause 5.3 of the Draft White Paper should be revised to state explicitly that the proposed online content regulator will operate on a co-regulatory basis.

4.3 Where the state plays a role in media content regulation—most notably in broadcasting—regulatory independence is essential. In South Africa, ICASA already performs a co-regulatory function by ensuring broadcaster compliance with an industry code under section 54 of the Electronic Communications Act, 2005 (ECA).

4.4 There is obviously no closed list of enumerated characteristics of independent broadcasting regulators.

4.5 However, there are characteristics of independence[21] which have found acceptance in numerous international instruments, statements and declarations[22] and we set these out below:

4.5.1 Broadcasting must be regulated (including the granting and enforcement of licences) by independent public authorities;

4.5.2 The independence of the broadcasting regulator must be guaranteed in national legislation and, ideally, in the constitution – as is done in the ICASA Act, 2000 (the ICASA Act) and section 192 of the Constitution;

4.5.3 An independent public broadcasting authority is one whose members are:

4.5.3.1 are appointed through an open, participatory, multi-party process;;

4.5.3.2 are accountable to the public through Parliament;

4.5.3.3 act in the public interest;

4.5.3.4 are insulated from political or commercial interference;

4.5.3.5 are not influenced by funding processes;

4.5.3.6 collectively have relevant expertise and reflect societal diversity; and

4.5.3.7 whose independence is affirmatively protected by government.

4.5.4 South Africa has the good fortune to have such a body in ICASA which is the regulator for the communications sector as a whole and not just of broadcasting.

4.5.5 Few other communications entities enjoy comparable constitutional protection. The Films and Publications Board (FPB), for example, functions as part of the executive and lacks many of the independence attributes listed above.

4.5.6 As the Department may be aware, a number of civil society bodies have long been concerned at the self-characterisation of the FPB as the "Content Regulatory Authority of South Africa"[23]. FELN shares these concerns and asks the Department to clarify this

[21] See generally Chapter 2, Limpitlaw J, *Media Law Handbook for Southern Africa*, Volume 1 Konrad Ardenauer Stiftung (2021).

[22] Article 2 of Part 1 of the African Charter on Broadcasting, Principle 14.3 and Principles 17.1, 17.2, 17.3, and 17.5 of the African Principles of Freedom of Expression and Access to Information Declaration, the Dakar Declaration, Principles 11, 12, 13.2, and 17.2 of the Access to the Airwaves Principles developed by Article XIX.

[23] The FPB's logo is available here https://fpb.org.za/

definitively. Under the Films and Publications Act, 1996 (FPA), the FPB's principal mandate is classification of films and games and, on request, publications, and enforcement against distributors, excluding films aired by licensed broadcasters and publications issuing from subscriber members of the Press Council.

4.5.7 Because spectrum scarcity does not apply online, licensing speakers is neither necessary nor constitutional. At the same time, platform scale and cross-border operation make purely voluntary arrangements ineffective. A co-regulatory system, comprising industry codes backed by an independent, expert, rights-based overseer, is therefore the appropriate default for online content. That overseer must meet section 192-level independence to ensure public confidence and to avoid "back-door" state censorship.

4.5.8 Accordingly, the proposed online content ombud should be established within ICASA (or its Complaints and Compliance Committee (CCC)), to secure constitutional protections and guarantee perceived and actual independence.

5. A CONSTITUTIONALLY COMPLIANT MODEL FOR ONLINE CONTENT REGULATION

5.1. FELN proposes that ICASA, by virtue of its constitutional independence and sector-wide mandate, serve as the general online-content regulator and first-instance forum for complaints, including matters that touch on the mandates below. Given the time-sensitive nature of online disputes, ICASA should develop dedicated expertise and issue initial determinations (including interim, proportionate remedies) under clear service-level timelines, with referral and appeal pathways to the relevant specialist bodies.

5.1.1 Hate speech and racist expression (PEPUDA).
Initial determination by ICASA; appeal and any follow-up investigations to the South African Human Rights Commission (SAHRC) and/or Equality Courts, as appropriate.

5.1.2 Privacy and data protection (POPIA/PAIA).
Initial determination by ICASA; appeal/investigation to the Information Regulator.

5.1.3 Child sexual abuse material (CSAM) and prohibited content (FPA).
Initial determination by ICASA (including urgent steps to preserve evidence and limit further distribution); appeal/investigation to the Films and Publications Board (FPB) and, where applicable, law-enforcement.

5.1.4 Elections and political conduct (Electoral Act/Code).
Initial determination by ICASA; appeal/investigation to the Independent Electoral Commission (IEC).

5.1.5 Criminal offences.
Where conduct appears criminal, ICASA to refer to South African Police Service for investigation and the National Prosecuting Authority for prosecution, while coordinating any platform-level interim measures.

5.1.6 Coordination, safeguards and effect.
ICASA should operate under MOUs with the SAHRC, Information Regulator, FPB and IEC to prevent duplication and forum shopping, define data-sharing, and set escalation timelines. Initial determinations should focus on proportionate, speech-preserving measures (e.g., labels, reductions in reach, takedown only for manifest illegality), be reasoned and publishable, and be subject to *de novo* review by the specialist body on appeal, without prejudice to parties' rights to approach a court.

5.2 ICASA is well-versed in operating as a co-regulator as it has played that role with regard to broadcasting content, in line with the constitution and international good practice for decades.

5.3 ICASA's has worked with the Advertising Regulatory Board (ARB) and with the Broadcasting Complaints Commission of South Africa (BCCSA) in a co-regulatory capacity for many years. It is ideally placed to provide oversight on development of platform content co-regulation and enforcement.

5.4 FELN recommends that Parliament expand ICASA's mandate and powers under the ICASA Act and the ECA, and amend ECTA (2002) to confer on ICASA general online-content regulatory authority on a co-regulatory basis. ICASA should be empowered to approve, supervise and enforce industry codes and to issue binding rules where codes are absent or ineffective, including authority:

5.4.1 To develop (and approve) an Online Content Code in the public interest, applicable to online platforms and providers, which must at minimum provide for:

5.4.1.1 **Harm-based prohibitions.**
Prohibitions limited to internationally accepted grounds and South African law (e.g., CSAM, incitement to violence, clear and direct threats, unlawful discrimination/hate speech as defined in statute, serious privacy violations, unlawful commercial conduct).

5.4.1.2 **Child-safety by design (age-appropriate).**

(a) Parental controls that are easy to find and use;

(b) Privacy-preserving age assurance for content/features not appropriate for minors (including AI chatbots and live features);

(c) Default high-safety settings for minors (reduced autoplay/notifications, stricter contact rules);

(d) Age-appropriate design requirements (clear nudge/choice architecture; no dark patterns);

(e) Digital-literacy tools and safety resources on-platform.

5.4.1.3 **Notice-and-action and evidence preservation.**

Simple user flagging; trusted-flagger channels for priority harms; rapid evidence preservation (hashes, URLs, logs) and time-bound responses for manifest illegality, with due regard to user rights.

5.4.1.4 **Transparency and user control over ranking.**

(a) Plain-language disclosure of main parameters of algorithms that increase or reduce the prominence of content;

(b) A non-profiling feed option (e.g., chronological/recent) for all users;

(c) Publication of moderation policies and enforcement statistics (human and automated);

(d) A public ads repository (sponsor, targeting, spend, reach), with stricter disclosure for political ads.

5.4.1.5 **Due process for users.**

Notice with reasons for content/account actions; human review on request; accessible internal appeal; timelines for decisions; and escalation to the online-content ombud at ICASA.

5.4.1.6 **Systemic-risk management (large services).**

Annual and pre-deployment risk assessments (elections/civic discourse, minors, public health), proportionate mitigations (design changes, recommender/ad adjustments, rate-limits), and publication of non-confidential summaries.

5.4.1.7 **Independent audits and compliance.**

Yearly independent audits of risk assessments, mitigations and transparency; an internal compliance function with direct access to senior leadership.

5.4.1.8 **Automation, bots and coordinated inauthentic behaviour (CIB).**

Mandatory bot/automation disclosure; prohibition of undisclosed automated

influence; policies to detect/deter CIB (including cross-platform signal-sharing under privacy safeguards); rate-limits/friction on mass actions.

5.4.1.9 **Synthetic and AI-generated content.**
Clear labelling of materially manipulated or AI-generated media; support for provenance/watermarking standards; AI chatbots must self-identify and follow child-safety rules by default.

5.4.1.10 **Elections and emergencies (time-limited measures).**
During election periods and declared emergencies, reasonable must-findability measures for public-interest information defined by neutral criteria; cooperation with the IEC and other competent bodies.

5.4.1.11 **Researcher access and data for accountability.**
Privacy-safe access for vetted researchers to study systemic risks and platform performance; publication of aggregate datasets where feasible.

5.4.1.12 **Complaints handling and service levels.**
Platform-operated, transparent complaints mechanisms with published timelines (acknowledgement, initial decision, appeal); accessibility in major SA languages and for persons with disabilities.

5.4.1.13 **Scaled obligations; SMEs protected.**
Obligations scale by reach and risk (heavier for very large services); templates and lighter regimes for SMEs and non-profits.

5.4.1.14 **Coordination and referrals.**
Clear MOUs and referral rules with the SAHRC (PEPUDA), Information Regulator (POPIA/PAIA), FPB (FPA/CSAM), IEC (Electoral Act), SAPS/NPA (criminal offences), to avoid duplication and forum shopping.

5.4.1.15 **Enforcement and safeguards.**
Proportionate administrative measures and penalties for systemic non-compliance, with judicial review preserved; explicit fidelity to sections 16 and 36 of the Constitution to ensure rights-consistent application.

5.4.2 To make public-interest regulations governing online-content service providers/platforms (after consultation), including the authority to:

5.4.2.1 **Define scope and scaling.**

Classify regulated services and set thresholds (e.g., *large online platforms/gatekeepers*) so obligations scale by reach and risk.

5.4.2.2 **Fairness in ranking, search and recommender systems.**

(a) Prohibit unfair discrimination and self-preferencing in ranking or recommendation of content, services or commerce;

(b) Require periodic fairness testing and independent audits of ranking systems;

(c) Mandate a non-profiling feed option and clear user controls;

(d) Publish methodological summaries of fairness tests and significant design changes;

(e) Provide administrative penalties for systemic non-compliance.

5.4.2.3 **Local content development.**

Impose proportionate financial or carriage obligations (e.g., a local content development levy or defined prominence windows) to support South African audio/audio-visual creation, with transparent governance of any fund.

5.4.2.4 **Advertising standards and transparency.**

(a) Require membership of and compliance with the Advertising Regulatory Board Code where advertising is carried;

(b) Create an online ads repository (sponsor, targeting, spend, reach), with stricter disclosure for political ads;

(c) Ban targeted advertising to minors and high-risk profiling practices.

5.4.2.5 **Automation, bots and coordinated inauthentic behaviour (CIB).**

(a) Require conspicuous disclosure of automated/bot accounts and automated messages;

(b) Prohibit undisclosed automated influence and CIB;

(c) Mandate rate-limits/friction on mass actions and maintain CIB detection policies;

(d) Permit privacy-safe signal-sharing among accredited platforms and with ICASA.

5.4.2.6 **Code approval and exemptions (co-regulatory model).**

Approve an industry Online Content Code (or sectoral codes) where equivalent to ICASA's Code; empower ICASA to exempt compliant providers from overlapping provisions **c**onditioned on sustained compliance and audit and to exempt subscribers to existing industry codes such as the Press Code for print and Online Media.

5.4.2.7 **Notice-and-action; put-up/take-down orders.**
(a) Establish a structured notice-and-action framework with service-level timelines and evidence preservation;
(b) After hearing the complainant and platform, empower ICASA to issue put-up or take-down orders where a refusal is unlawful or unreasonable, with reasons and appeal rights.

5.4.2.8 **Platform liability for unreasonable refusals.**
Determine that a platform is liable for (i) user content it unreasonably refused to take down following an ICASA order, or (ii**)** harm caused by an unreasonable refusal to restore content after a put-up order—without prejudice to statutory safe-harbours for timely, good-faith compliance.

5.4.2.9 **Trusted flaggers and priority channels.**
Designate trusted flaggers (SAHRC, FPB, IEC, accredited hotlines/fact-checkers), set fast-lane timelines and accuracy standards, and publish aggregate performance metrics.

5.4.2.10 **Child-safety by design.**
Set minimum age-assurance standards (privacy-preserving), require high-safety defaults for minors (limited autoplay/notifications, stricter contact), and ban dark patterns that nudge children toward risky choices.

5.4.2.11 **Synthetic/AI-generated content.**
Require labelling of materially manipulated/AI-generated media; support content provenance/watermarking; ensure AI chatbots self-identify and comply with child-safety defaults.

5.4.2.12 **Elections and emergencies (time-limited measures).**
For defined periods, require reasonable must-findability of public-interest information (criteria-based, neutral) and cooperation with the IEC and competent authorities.

5.4.2.13 **Researcher access, audits and compliance.**
Mandate independent audits (annual for large services), an internal compliance functio**n** reporting to senior leadership, and privacy-safe data access for vetted researchers to study systemic risks.

5.4.2.14 **Cross-border enforceability and local contact.**
Require a local legal contact/representative for service of orders; specify

procedures to overcome “foreign peregrinus” obstacles (recognition/enforcement of ICASA orders).

5.4.2.15 **Referrals and coordination.**
Provide for referral of complaints to the SAHRC, FPB, Information Regulator**,** IEC (as appropriate), and set MOUs, data-sharing, and confidentiality rules to avoid duplication.

5.4.2.16 **Due process and review.**
Guarantee notice, reasons, and appeal to the online-content ombud/ICASA committee and judicial review in the High Court; publish anonymised decisions for precedent and learning.

6. CONCLUSIONS

6.1 South Africa has gone too long without a fit-for-purpose framework for online content regulation. The sector is unquestionably fast-changing but delay in regulation carries real costs for the South African public and our democracy. We urge decisive action – fast, but principled – so that regulation protects rights while tackling concrete harms.

6.2 Content regulation cannot be the province of the executive. International best practice requires an independent regulator. Bodies operating, in effect, as arms of the Department should not be tasked with general content regulation and we again express our concern that such a role is contemplated in respect of the FPB.

6.3 Multiple authorities already touch online content (SAHRC, FPB, IEC/Electoral Court, Information Regulator, SAPS/NPA). What is missing is a rights-based “front door” and coordinator.

6.4 ICASA, constitutionally independent and with its sector-wide remit, is best placed to be that front door. Empower ICASA, on a co-regulatory basis, to set/approve enforceable codes and issue regulations, with clear referral rules to the specialist bodies named above.

6.5 Amend the ICASA Act, ECA and ECTA to:

6.5.1 confer general online-content jurisdiction on ICASA;

6.5.2 establish an online content ombud within ICASA; and

6.5.3 enable regulations and an Online Content Code that are harm-based, scalable by risk/size, and auditable (notice-and-appeal, transparency, child-safety by design,

bot/automation disclosure, fairness in ranking, researcher access, privacy-safe signal-sharing, and service-level timelines).

6.6 Move quickly and conscientiously to safeguard rights by adopting technology-neutral principles that will also govern AI-mediated content: systemic-risk assessment and mitigation; provenance/labelling of synthetic media; user control (including a non-profiling feed); neutrality/non-discrimination in ranking; and robust due process. These principles endure even as tools change.

6.7 To avoid further drift, and in line with the Draft White Paper's proposed phased timetable, FELN urges its own phased approach:

6.7.1 **Phase 1 (0–6 months):** designate ICASA lead; create ombud; conclude MOUs with SAHRC/FPB/IEC/Information Regulator; set up trusted-flagger channels and emergency SLAs.

6.7.2 **Phase 2 (6–12 months):** promulgate Online Content Code and priority regulations (child-safety, fairness in ranking, transparency, notice-and-action).

6.7.3 **Phase 3 (12–24 months):** audits, researcher access, and a first public review to finetune obligations.

7. FELN trusts these proposals assist the Department to close the gap rapidly and constitutionally: a co-regulatory system led by an independent ICASA, working alongside specialist agencies, that protects the public interest and free expression.

8. We are available to brief the Department further and to assist with draft clauses, implementation timelines, and coordination protocols.

Yours Sincerely

Nicole Fritz and Justine Limpitlaw

On behalf of The Freedom of Expression Legal Network; The Campaign for Free Expression; the Press Council of South Africa and the South African National Editors' Forum

082 452 3909/ 082 902 24 94

nicole@freeexpression.org.za/ **justine@limpitlaw.co.za**