Response to ***Online Safety Act 2021***

Jean Linis-Dinco, PhD

The eSafety Commissioner has substantial power to determine whether content is illegal or harmful, raising valid concerns about potential abuse of power and a lack of accountability, particularly in relation to human rights. This concentration of authority is particularly troubling given the historical misuse of similar regulations against marginalized groups, such as sex workers. The absence of specific provisions protecting sex workers in the Online Safety Act 2021 is a significant oversight. Sex workers have frequently been targeted by laws designed to regulate online content, often facing undue censorship and punitive measures that further marginalize them. For example, in the United States, FOSTA-SESTA has led to the shutdown of many online platforms that sex workers used to screen clients and operate safely. This has forced many sex workers to return to street-based work, increasing their exposure to violence and reducing their ability to control their working conditions. The Act should should have a procedural fairness (Section 100, Division 3, Blocking Notices) when issuing blocking requests with appeals process clearly outlined.

In Part 9, Division 8, Section 152 under the exemptions from service provider determinations, it says that the Minister may, by legislative instrument, exempt service provider from service provider determinations. This provision gives substantial discretionary power to the Minister, raising concerns about transparency, accountability, and potential conflicts of interest. The Act should require the Minister and the eSafety Commissioner to publicly announce all exemptions granted under Section 152, in compliance with Australia's Freedom of Information laws. This should include the names of the service providers, the nature of the exemptions, and the reasons for granting them. As part of the Act, there should be a dedicated platform or section on the eSafety Commissioner’s website where all exemption details are published and accessible to the public. This platform should be regularly updated and searchable.

In Section 45, Division 2 (Basic Online Safety Expectations), the Act allows for a broad interpretation of what constitutes compliance. This gives companies leeway to argue that their measures are sufficient even if they fall short of the intended standards. Key terms like "reasonable steps" and "significant harm" (Section 45, Division 2) should be precisely defined so that companies will not try to interpret these requirements in a way that minimises their obligations.

The provision allowing the eSafety Commissioner to engage consultants (Section 187) presents several potential issues. First, consultants often work for multiple clients, including social networking sites and service providers that are subject to regulation under this Act. This dual role can lead to significant conflicts of interest, where consultants might prioritise the interests of their corporate clients over their regulatory duties. This could undermine the Commissioner’s ability to enforce the Act impartially and effectively. The current provision lacks explicit safeguards to prevent consultants from using their insider knowledge and influence to benefit their other clients. There is no mention of conflict of interest policies, mandatory disclosures, or recusal requirements in situations where a consultant’s impartiality might be compromised. Without such mechanisms, the potential for regulatory capture and biased decision-making increases. While the Commissioner has the discretion to determine the terms and conditions of engagement, this discretion must be exercised transparently and with robust checks in place. The absence of clear guidelines on how consultants should be engaged and monitored can lead to inconsistent practices and potential abuses.

There should be an expansion of protection under the Online Safety Act to explicitly cover sextortion, doxxing, revenge porn, and the downstream distribution of intimate content from online dating apps. It would be helpful for all these terminologies to be defined early on to prevent misuse and legal loopholes that perpetrators can use. These malicious activities represent significant threats to personal safety and privacy, often resulting in severe emotional and psychological harm. Additionally, the Act should address the rising concerns of deepfake technology, where synthetic media is used to manipulate images and videos for nefarious purposes, and cyberstalking, where persistent and unwanted digital attention leads to distress and fear. Protections for sex workers should also be strengthened, as they are particularly vulnerable to online abuse, doxxing, and the non-consensual sharing of intimate images, which can result in both personal and professional repercussions.