[redacted]

[redacted]

I am a recently retired computer systems engineer with 25 years experience in computer operating systems, programming, email and other Internet services, networking, network protocols and security.

This is a very short and informal submission as the fundamental problem with the Electronic Services standard precludes its successful implementation. I can't comment about the Designated Internet Services draft as I don't have direct, in-depth experience with the large corporations providing these, although my comments will no doubt also apply there.

The issue centers on part 2 section 7: Technical Feasibility. This section in both draft standards in fact has no language related to technology nor encryption (the passage only redefines the word to mean financial or commercial), yet this incorrect definition is relied upon to provide guidance for technical actions required by the standard. This smacks of the Turnbull approach: "The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia." It is magical thinking to assert, as this standard passively does by purposely ignoring the scientific foundations of computing, cybersecurity and mathematics, that encrypted communications can be harmlessly observed without destroying encryption. End-to-end encryption ipso facto precludes observation by third parties. To hold otherwise is similar to issuing a safety mandate requiring that boiling water not exceed 60°C - the mandate can be made but it is fallacious and cannot be achieved.

In the Guardian news website, the Commissioner is quoted as saying: "[the discussion paper] clearly states that the standards do not require service providers to design systematic vulnerabilities or weaknesses into encrypted services." That is true, there are no technical requirements in the standards whatsoever. In the discussion paper under the approach to minimum compliance measures section, it states that the approach ensures: "obligations are meaningful as well as technically feasible". So what would these purported "non-systematic vulnerabilities" or "non-weakened encrypted services" be that allow secure decryption by the vendor for observation? Please, publish some examples. These needn't be part of the standards; they would show that such an meaningful approach would be 'technically feasible' in the correct, actual sense of the phrase.

It is a persistent fallacy amongst politicians and policy makers to gloss over technology and expect their impossible aims to be achieved by "nerding harder". Computer scientists, mathematicians and engineers have published extensive and unrefuted critiques where similar standards and laws have been proposed and unfortunately enacted, here in Australia and in the UK, for example, see: https://blog.whatsapp.com/an-open-letter . Prove us wrong with some published examples of workable solutions, please. Unless experts and vendors at large can see and test such proofs, these standards are just another ineffectual measure by government / administration that actively reduces user safety.

Phil Crooker

[redacted]