At about the same time on Sunday afternoon that former Labor prime minister Paul Keating was referring to him as a " fossil with a baseball cap ", Prime Minister Scott Morrison announced a re-election promise to crackdown on social media platforms and online predators, and " protect children, families and the community ".

Our government's determination to address online safety is to be commended, but the current proposals contain few details on policy and implementation.

In reality we're unlikely to see much improvement in online safety unless we tackle the real elephant in the room: big tech's business model.

Read more: ***How big tech designs its own rules of ethics to avoid scrutiny and accountability***

Four initiatives

The plan consists of four initiatives.

The first would see increased maximum penalties for existing crimes such as using the internet to menace, harass or cause offence. Penalties would also increase, and new offences created, for a range of child sex offences that rely on the internet.

The second initiative is designed to hold major social media platforms to account by enacting laws that require them to provide transparency reports relating to illegal, abusive and predatory content by their users – that is, trolling.

The third is to provide parents with tools to “make their own decisions about how their children use the internet”. It will become mandatory for online apps, games and services marketed to children to be pre-configured with the most restrictive privacy and safety defaults.

Complementary initiatives involve providing a filtered internet service that blocks sites considered unsafe by the eSafety Commissioner, and providing point of sale and point of account creation information to parents about online safety and parental controls.

The final initiative is to work with the G20 to “ensure that technology firms meet obligations regarding the prevention and protection, transparency and deterrence to stop terrorists weaponising the internet”.

Scandals and social harm

In the wake of a variety of scandals that have plagued “big tech” over the last few years – including the Facebook Cambrige Analytica controversy , and Robert Mueller’s investigation into Russian interference with the 2016 US Presidential elections – governments across the world have become increasingly concerned about the social harms produced by a largely unregulated technology sector.

The Coalition’s election announcement comes soon after the passage of amendments to the Criminal Code to address live streaming of “abhorrent violent material” by social media platforms in the wake of the Christchurch massacre. It should be seen as an advance in governmental resolve to address the excesses of big tech. This is a long overdue and welcome development.

Read more: ***Livestreaming terror is abhorrent – but is more rushed legislation the answer?***

Extra offences and tougher penalties, particularly for online-enabled sexual exploitation of children, play well in a febrile pre-election environment. The prospect of more punishment and denunciation seems like tough and determined action will be taken.

But the deterrent effect of criminalising activity and imposing harsher jail sentences is based on an assumption that people weigh up the costs and benefits of their actions whenever they make decisions – that they make rational criminal choices. This assumption is open to question where online harassment and child sex offending occurs.

Equally, there is little evidence that jail time for sex offenders serves rehabilitative objectives or that, long term, the community is safer. After all, when offenders have served their time they are released and return to the community.

Read more: ***Helping to rehabilitate sex offenders is controversial – but it can prevent more abuse***

It's easy – and cheap - to legislate for new offences and more incarceration. It's harder – and expensive – to ensure the community is safer in the long term. This involves addressing causes, not effects.

Only the 'major' platforms

The proposed greater transparency measures appear to apply only to “major” social media platforms. Presumably, this means digital platforms that have a corporate presence in Australia – like Google and Facebook – and who can be compelled to obey Australian laws.

But there are many other sites that Australians access which have no presence, other than a cyber presence, in Australia.

Has the Coalition taken account of the fact that those who choose to propagate “illegal, abusive and predatory” content may simply switch their activities to platforms like 4 Chan, 8 Chan or reddit to avoid transparency requirements, making it harder to regulate them? How will they be made transparent?

Another challenge is how to define “illegal, abusive and predatory content”. Presumably government will provide legislative guidance about this in its proposed Online Safety Act, but it will be interesting to see how Silicon Valley corporations steeped in US first amendment free speech doctrine interpret and implement this requirement.

Read more: ***We need to talk about the data we give freely of ourselves online and why it's useful***

Policing is the hard bit

One of big tech’s most consistent arguments to avoid regulation is that we should rely on technology to solve technology-caused harm
. The Coalition’s proposal to provide parents with controls to “make their own decisions about how their children use the internet” falls into this category.

But how are default privacy and safety settings to be policed? What will stop curious, technically-literate children simply changing the default settings behind their parents’ backs?

Likewise, the proposal to supply filtered internet services that block sites nominated by the e-Safety Commissioner seems like an invitation to find work-arounds to avoid censorship.

Read more: ***Sorry everyone: on the internet, you're always the product***

As commentators like Roger McNamee , Zeynep Tufekci and Tristan Harris have argued, the risks that big tech poses to society are caused by their “free” service business model.

The need to collect more and more personal data and keep their users’ attention focused on their services by feeding them more and more content that they “like” is baked into social media corporate DNA. Companies create “filter bubbles” and “preference bubbles” that ensure popular content is succeeded by more extreme and disturbing versions of the same.

Big tech’s business model is the root cause of the harms the Coalition’s online safety package is designed to address. Although any government action to address these harms is to be encouraged and supported, the package is likely to fall short of our expectations.

David Watts does not work for, consult, own shares in or receive funding from any company or organisation that would benefit from this article, and has disclosed no relevant affiliations beyond their academic appointment.

Authors: David Watts, Professor of Information Law and Policy, La Trobe University

Read more http://theconversation.com/coalition-plans-to-improve-online-safety-dont-address-the-root-cause-of-harms-the-big-tech-business-model-116592