August 21, 2023

Dear Lord Bethell,

Thank you for your willingness to engage. I'm going to provide my perspective here, given that voters and the public are clearly interested in this topic. Please know that I am sincere, that I have worked on these issues for nearly two decades, and that I am no champion of Big Tech, as my background makes very clear. Indeed, I am opposed to Clause 122 (formerly 111), and similar measures, in large part because I see them as extending the pernicious surveillance power of large tech firms under the guise of providing "accountability."

You assert that Parliament would not have passed these measures if it was concerned that the measures were undermining the UK's safety and security. I believe you are right. The issue is that the Online Safety Bill has been in process for a number of years, is now very bloated, and contains a multitude of provisions, some good and some bad. Clause 122–the part that Signal and the vast majority of the technical expert community is alarmed by–was only added to the Bill in September 2022, during a very chaotic and unstable time in the UK government.

While other parts of the Bill may have been reviewed in depth, this dangerous Clause has not received significant scrutiny in Parliament. This is something that Lord Stevenson raised during report stage on July 19, 2023, emphasizing that the question of the extent of external supervision under Clause 122 remains "open," and urging that the Clause be put to further Parliamentary scrutiny in order to be "workable." Indeed, as the dangers of this Clause have become evident, some who were previously supporters of the Bill, like former Conservative Minister Lord Syed Kamall, have withdrawn their support. Reflecting on these harms, Kamall stated in an op-ed that, "an unintended consequence of the bill may make apps more vulnerable to attack or interception by bad actors."

What's confusing, especially given this lack of scrutiny, is the unwillingness of Clause 122's supporters to accept the longstanding consensus of the technical expert community. This community is not composed of large companies, or US-based Big Tech. It's made up of people who work with networked computational systems closely, and who thus understand that these systems are not magic–that they operate according to particular logics and rules that cannot be changed simply by wishing or mandating that things be different. They also know, many from direct personal experience, that attempting to undermine these logics can wreak havoc with these systems–causing problems that affect the core digital infrastructures that the UK, and the world, increasingly depend on.

This is what the 70+ UK-based cybersecurity academics and over 400 global cybersecurity researchers were generously outlining in their respective open letters, addressing the implications of Clause 122 and measures like it. It's also what a group of leading researchers on topics of privacy, security, and technical infrastructure laid out in a well-cited 2021 paper, which systematically dismantles the notion that the mass surveillance implied in Clause 122 can be conducted safely, securely, or effectively. And it is what the government's hand-picked reviewers at the REPHRAIN research center stated in their assessment of potential "accredited technologies" is poised to be mandated under the powers granted by Clause 122.

I am still unsure why these and other careful and painstaking interventions go unnoted by supporters of the Clause. You mention that this is a "very nuanced policy area" and as a rule I agree. But the term 'nuance' does not function as a magic wand, dissolving inconvenient barriers between legislative desire and technical impossibility. Indeed, attending to nuance implies spending time with the details, listening to experts, and recognizing when something that feels like an easy technological solution is in fact a dead end.

To summarize the points made by these experts, whose work I truly hope you will visit in full: **it is not possible to create a technological system that can both scan everyone's messages for impermissible expression, and preserve the right to privacy.** This is the stubborn truth. And nothing about this truth negates the grave seriousness of child abuse and exploitation, or makes redress impossible. As Cambridge's Dr. Ross Anderson makes clear in a recent paper, it does mean that turning to evidence-based approaches in order to protect children is required–approaches that look more like funding social services, providing early intervention support, and ensuring that powerful people in positions of authority over children are not believed over the testimony of the vulnerable. These are measures that could use much more support from UK politicians, given that investment in early intervention support in the UK has been cut by 50% in the last decade, even as demand is at an all-time high. Indeed, the government determined to fund only 7% of the £200 million recommended by the UK's own Independent Review of Children's Social Care.

I truly hope that this message finds you well, and that I have been able in some small way to help clarify the stakes of this issue, and decouple it from the patina of Big Tech alarmism that seems to have stained it in your eyes. The stakes here are high, and I know that myself and the broader technical expert community are eager to engage in good faith.

Warmly,

Meredith Whittaker
President, Signal