Dear President von der Leyen,
Dear Executive Vice-President Virkkunen,

Subject: The right approach to protecting children from the negative effects of social media

I'm writing this letter as a member of parliament from Bulgaria, as a former minister for digital transformation, as a technical expert and as a father.

Protecting children online has become a priority for the European Commission and for many EU governments, and rightly so. The threats online, the negative psychological effects of addictive designs and the algorithms that prioritize virality over quality have significant negative effects on children.

The European Commission has started addressing the addictive design problem, analyzes algorithmic bias and has undertaken an age verification initiative, in addition to long-term measures against CSAM, online crimes against children, etc.

While we all see the good intentions behind these initiatives, they sometimes lack the technical depth and the ambition to achieve swift results. My focus in this letter will be age verification, as the measure that is the most polarizing and may have significant negative side effects if done wrong. And I'm concerned that the currently selected approach by the European Commission is the wrong one.

The idea sounds simple – "social networks are proven to be detrimental to children's mental health, and so they must not be allowed to use it. The way to do it is to add an age check before registration, so that only adults can use the service". While simple to formulate, it's much more difficult to implement, if not impossible.

There is an inherent paradox - if a solution is fully privacy-preserving, it's ineffective. If it's effective, it bears significant risks to privacy, as it will require every citizen to prove their identity online in order to use everyday services.

The European Commission has made a well-meaning attempt to design and implement a proper zero-knowledge proof of age. It's a great tool, with proper cryptography, complex-yet-elegant. It has "just" one problem – it doesn't account for the actual "threat actor" in this scenario – the user, who would try many things to circumvent the age limitation. As security consultant Paul Moore has brilliantly shown, you don't have to compromise the age verification app in order to circumvent the flow – by a simple relay attack, where you just present someone else's verified age credentials in order to use a service. The proof of concept was implemented as a chrome extension which relays age checks to 3rd party service, backed by an over-18 person's device, which sends the proof to the service. That way a single adult can verify the accounts of all minors, and because of the necessary privacy guarantees, the relying party (the social network) won't even know.

This is very likely to happen – “age verification as a service” providers will certainly pop-up to help minors get into social networks. What’s worse – some of these providers may collect children’s personal data, including phone number or social network account ID, in order to provide them with the much coveted proof of age. That data, purposefully or after an inevitable data breach, may be used by sex predators to target children. There are completely realistic nightmare scenarios, born from the good intention to limit the negative effects of social networks.

Even in a school context, a single over-18 (or over-16) student can lend their age verification app to help younger children register profiles. What are policy makers going to do then? Issue administrative fines for sharing age tokens/attestations? Criminalize it?

Any attempt to fix that technically, breaks the privacy guarantees; any attempt to fix it legally, is doomed to fail in enforcement.

My advice, in all my capacities listed in the beginning of this letter, is to abandon that approach and focus on a different approach - rely on parental control apps.

Parental control apps remain rudimentary, and perhaps there are reasons for this. They are not widely used and are often unintuitive and unreliable. However, they can be regulated and improved. They can also incorporate government-mandated lists of apps and domains restricted for children according to age. For example, a child protection agency could publish a list that parental control apps would be required to import automatically. Legislators could also require these apps to be pre-installed on every phone sold in their country. Parents would remain in control and could adjust the settings if they considered their children ready to use particular services responsibly.

Certain apps can be banned for under-14, others for under-16 and others – for under-18. Governments would have much better control over the exact services they deem risky for children, without the need for any changes on the service’s side. Or, if an app vendor wants to have it whitelisted, they may have to implement children-friendly versions.

Going further, this may eventually lead to platform-level parental control APIs, so that each app can read parental control settings, and on the other hand export parental control configuration options to be used in the parental control app.

What’s even better about this approach, is that VPNs can’t be used to circumvent it - it’s a device-level limitation, not service-level limitation, which needs to figure out the country of the user, which can only be done by their IP address.

And It’s completely privacy-preserving, as users don’t have to show or prove anything to anyone.

Of course, the harder part is making sure every child and parent has a parental control app installed. Information campaigns and teachers can help with that, and I'm sure it will achieve much better results than what we are seeing in Australia for example.

Even if the right age limitation measures are implemented, the efforts to limit the addictiveness and so-called "brainrot" on online platforms should continue.

We have proposed national legislation to implement the approach above. But in order to avoid fragmentation in the digital single market, and in order to have a working, cross-border model, where the experience of each country improves the model EU-wide, a solution should be discussed on a EU-level.

Yours sincerely,
Bozhidar Bozhanov,
Member of parliament of the Republic of Bulgaria