Age Appropriate Design Codes – Well Meaning, but Do They Make for Good Law?

March 20, 2022

As we've discussed here, there's bipartisan momentum in Congress to enact stronger privacy protections for kids and teens – and specifically, tools that would enable minors and their parents to limit algorithms and online content that fuel self-harm and addictive behaviors. These efforts, reflected in several federal bills (see here and here) and now in a California bill too, build on months of testimony by a social media insider and are modeled in large part on the UK's Age Appropriate Design Code.

In his State of the Union address, the President added to this momentum, calling on Congress to enact stronger protection for kids – a move that was heralded in the media as a potential "game changer" for privacy that could "help clear the logjam on Capitol Hill." (Relatedly, report language accompanying the recently signed budget bill directs the FTC to prioritize kids' privacy in its enforcement efforts.)

It's certainly understandable why U.S. policymakers would want to protect the privacy and safety of minors. It's also notable that that they are focusing on an area where bipartisan action might be possible and emphasizing the *safety* aspects of these bills (as if the word "privacy" would jinx the effort while "safety" might garner more support). But, looking past the good intentions to protect kids, some of the concepts and language in these bills pose real challenges as to clarity and enforceability.

Focusing on just a few:

- **Best interests of the minor.** The bills generally require companies to design and operate online services used by minors with the minors' best interests as a primary consideration.
    - This language raises real questions about implementation and enforceability. While the bills sometimes include factors to consider (e.g., the types of harms to avoid), or authorize rulemakings or taskforces to flesh out the standards, this language is rife with subjectivity and will be difficult to interpret and apply.
    - For example, if a company demonstrates that it made a good faith effort to develop policies to address this issue, will that be sufficient? Will companies be able to develop a uniform set of criteria that apply to all minors when these types of judgments are normally left to parents? Will rulemakings or taskforces really be able to flesh out the standards in a way that the bill-drafters apparently concluded they couldn't?

- **Avoiding "dark patterns" or "nudge" techniques.** The bills generally state that companies should avoid design interfaces or techniques that cause excessive use of an online service, or that encourage minors to provide more data, forego privacy protections, or engage in harmful behaviors.
    - Some aspects of these standards will be easier to apply than others. For example, it seems clear that companies shouldn't expressly offer incentives to minors to provide more personal data or change settings. Nor should they feature bold, enticing "yes" options for data collection and sharing, in contrast to tiny or hidden "no" choices. And, of course, it shouldn't be more difficult to cancel a service than it is to sign up.
    - But so much of this lies in a grey area. Is it a "dark pattern" to allow minors to win and advance in a game which, as parents well know, keeps kids playing? What about gaming interfaces with vivid graphic pictures and details – a dominant feature of the most popular video games? Will they go the way of Joe Camel (the ubiquitous, cartoon character in tobacco ads that ended amidst controversy and litigation in the late 90s)? Is a portal used by children inherently problematic because it encourages minors to return again and again to access varied and changing content? And, of particular relevance to the concerns that are driving these efforts, will companies be expected to block content on bulimia, suicide, cutting, or sexual activity if that's precisely the information young teens are searching for?
- **Likely to be accessed by a minor.** Many of the bills' provisions – including the best interest and dark patterns requirements, as well as provisions requiring parental controls and strong default settings – are tied to whether an online service is "likely to be accessed by a minor."
    - This standard is very confusing and will be extremely difficult to apply. In contrast to COPPA – which covers online services "directed to children" or circumstances where an online service has actual knowledge a user is a child – this standard will require companies to anticipate access by minors even if the company hasn't designed its service for minors, and even if it has no specific knowledge that minors are using it.
    - Although COPPA has been criticized as too narrow, this new standard could be entirely unworkable. While some companies know full well that minors are using their services, others don't. Will this approach inevitably lead to universal identification and age-gating of all users of all online services? Given the ease with which minors can outwit age-gates, will that even be sufficient, or will companies need to set up more comprehensive data collection and monitoring systems? And would these outcomes really advance user privacy?

Certainly, the concerns driving these efforts – the harmful effects of social media on minors – are serious ones. They also unite members from different political parties, which is always a welcome development. However, as policymakers and stakeholders study these bills, they will likely (or hopefully) realize just how difficult implementation would be, sending them back to the drawing board for another try. Or maybe they will ultimately conclude that comprehensive privacy legislation is still the better approach.