The Vermont Kids Code: Debunking Big Tech Myths

Overview:
Major Tech companies like Amazon, Google, and Meta publicly claim a commitment to child safety while covertly retaining their priority of putting profit before kids. This is done through funding proxy groups like NetChoice and Tech Net to thwart meaningful legislation like the Kids Code – an Age Appropriate Design Code model – that would implement real protection for children online. Employing scare tactics and double talk, they hide behind sympathetic figures to avoid accountability. All the while, Tech giants can make empty statements and promises of safety while continuing to extract and sell the personal data of children through the explicit engineering of addictive features. It's crucial to expose these manipulative rhetorical practices and highlight the root problem - tech companies prioritize profit-driven motives over the safety impacts of their products.

The following document outlines the "myths" most frequently used by Big Tech in order to scare legislators and the public from moving forward with the Vermont Kids Code. The main myths used throughout the country are:

1. This legislation is going to break the internet. The bill requirements are unclear, we can't comply.
2. Child safety online should be the parents' responsibility.
3. This legislation violates the First Amendment, just look at the California lawsuit.
4. This legislation is going to be worse for privacy.
5. This legislation is going to be worse for marginalized kids.
6. This legislation is going to harm innovation and business.

MYTH: Big Tech Says, "This is going to break the internet, the bill requirements are unclear, we simply can't comply."
TRUTH: Don't believe these company's scare tactics - this type of tech reform is currently law in the UK and Ireland and the internet has not broken.

- Children, and adults, continue to be able to access the websites of their choosing, search for specific content, use social media platforms, and generally continue about their business online in those countries that have already regulated tech in this way.
- In fact, no business operating in the United Kingdom, including the NetChoice members, challenged the Children's Code in court or otherwise asserted an inability to comply. Rather, several large companies have lauded the Children's Code and its implementing guidance:
    - In October 2021, the head of TikTok's Public Policy for the Americas testified before the US Senate that TikTok "ha[s]voluntarily implemented much of the Age-Appropriate Design Code here in the United States" and that TikTok "strongly and enthusiastically support[s] that kind of child safety law."

    - The Director of Government Affairs and Public Policy at Google UK advised Parliament in May 2022 that the Children's Code "has helped us determine new ways to keep users safe." And Google's President of Global Affairs stated in a public post that "good legislative models - like those based on age appropriate design principles - can help hold companies responsible for promoting safety and privacy, while enabling access to richer experiences for children and teens."
- And there has been a wave of changes in response to those laws that have actually made the internet a better, safer, more developmentally appropriate place for all of us. For example:
    - Instagram now automatically sets the accounts of users under the age of 16 to private during the initial account set up, and adults can no longer direct message young people who do not follow them.
    - TikTok automatically applies a 60-minute screen time limit to all accounts belonging to people under 18.
    - Pinterest no longer shows children in the UK ads and their data is not shared or used outside of the service.
    - Among Us now grants users the opportunity to manage data collection at sign-up and in-game, including the option to turn off a personalized game experience and opt out of all data collection.
- It is critical to underscore that none of these changes require content to be removed or prohibit children from searching out specific information.

MYTH: This violates parental rights and parents want to take responsibility themselves.
TRUTH: A recent poll reports that 87% of the electorate believes that it is important for the government to take action to combat the harms being caused by social media platforms. Parents need and want safer tech products to protect kids; this is not a replacement for parental oversight but a digital seatbelt supporting responsible parenting in the digital age.

- Few families have "the talk" around internet use because most parents didn't have social media growing up and don't understand how virtual platforms can affect kids' state of mind, self-esteem, and well-being.
- The fault cannot and should not be laid at the feet of parents or youth. It's the tech companies that intentionally build platforms to nudge kids into risky behaviors, recommend harmful material, and encourage compulsive behavior who are at fault.
- Even when companies claim to provide parents with controls, there is little consultation with parents about their actual needs. This mismatch in what is provided and what is useful or wanted by parents in actuality goes unaddressed in the company's deluge of public statements.
- Technology is growing at an unbelievably rapid pace that makes it difficult to adapt to the latest update and know the implications of that update on children. The onus should not have to be on us – companies simply have to design their platforms to be safe from the start. It's the tech companies who should be held accountable and mandated to make their platforms safer for young people.

MYTH: This bill violates the First Amendment as shown in the CA AADC Lawsuit.

TRUTH: The Vermont Kids Code upholds free speech by focusing on platform designs and algorithms - not content removal - to mitigate harms, steering clear of regulating speech.

- The California Lawsuit exemplifies Big Tech turning to the Courts when they aren't successful at preventing legislation from passing.
    - Specifically, the challenge to the CA AADC was brought by NetChoice, whose members include Big Tech companies Google, Facebook, TikTok, Amazon, and others. It aims to block regulation of their platforms to maximize profits and allow them to continue to design their products with addicting, harmful, and data-hoarding features.
- The suit hides behind the First Amendment and Sec. 230 - trying to conflate regulating data privacy and design with speech and content moderation, intentionally sowing confusion among the public. The Vermont Kids Code regulates data management practices and product design, it is **not** content-based regulation. Since the model code doesn't target any content or require tech companies to moderate content differently, it's not regulating protected speech under the First Amendment.
- Acknowledging the constitutionality of data privacy laws, the Vermont Kids Code strives to make the Internet safer for children by overseeing how companies collect, manage, and use children's data, without encroaching on protected speech. If the First Amendment prevents data privacy regulation, then we will never be able to make the Internet a safer place for children.
- The District Court's sweepingly broad decision, currently under appeal, dangerously empowers tech companies to unilaterally shape the online experience for kids, undermining democratic processes and stifling legislative avenues for input. Given the growing body of evidence of these harms, and the growing state litigation efforts to combat them, we know these companies are never going to prioritize our kids' safety - unless regulation requires them to do so.

MYTH: This bill is going to be worse for privacy, it will require mandatory facial recognition, ID checks, or other age verification. It is more privacy-invasive.

TRUTH: This bill does not mandate any form of age or identity verification; companies already make age approximations of users based on the data they collect.

- The Kids Code went into effect in the United Kingdom in September 2021 and not a single user has been forced to submit an ID or be subject to facial recognition due to this bill.
- This is a classic Big Tech reaction: Any time new legislation or regulations to protect children online are proposed, the companies affected use fear tactics to claim they will need to use privacy-invasive age verification to comply. They do not want to comply with any data collection limitations, as this would significantly hurt their revenue.
- Platforms like TikTok and Meta already assign age-ranges to users based on the data they collect. We know this because despite Meta's terms of service barring under 13-year-olds from having an account on their platforms and in violation of COPPA, recently unsealed evidence revealed internal communication bragging about reaching 11 and 12-year-olds. The data from

the internal report came from Meta's age estimation algorithms confirming that millions of accounts belong to kids under 13.

- The AADC does not require age verification, and certainly does not require identity verification, as some critics have argued. The Vermont Kids Code has no provision for age estimation provision and continues to prohibit the collection of additional personal data for age assurance purposes.
- Proposed laws like the American Data Privacy Protection Act – which has broad support – rightly say that it is entirely possible to treat minors and adults differently online without collecting additional data or implementing age verification. Language included in the bill has been tailored to mitigate these concerns.

MYTH: This bill is going to be harmful for LGBTIQ+ and minority children.
TRUTH: This bill allows children of all identities to safely access age-appropriate information and essential resources.

- The internet is an essential place for LGBTQ+ youth to access the information and resources they need to explore their identity and build community. That is incredibly important to protect.
- By minimizing data collection, the Vermont Kids Code would stop platforms from tracking, profiling, targeting, and/or discriminating against LGBTQ+ youth online. Stronger default privacy settings and better data protection foster online environments where it's safer for everybody to grow, explore, and express themselves.
- As 5Rights notes, "LGBTQ children can be more susceptible to the risks of the digital world, however, as offline vulnerabilities manifest themselves online too. LGBTQ children are more likely to be cyber-bullied compared to non-LGBTQ children both offline (59% v. 38%) and online (42% v. 15%). One in three (32%) young LGBTQ people have said that they had been sexually harassed online, four times as many as non-LGBTQ young people (8%)."
- Furthermore, The Vermont Kids Code includes explicit anti-discrimination language that expressly prohibits tech companies from making any design choice that discriminates against a child based on race, religion, national origin, disability, sex and/or sexual orientation.

MYTH: This bill is going to harm innovation and business.
TRUTH: Smart regulation spurs innovation by incentivizing companies to proactively address risks and develop safer, more ethical products from the outset.

- The Vermont Kids Code is business-friendly. Rather than prescribing how a company makes changes, designs products, or bans features, it asks companies to assess risk and make changes to mitigate those risks, creating a new business landscape model that values safety from the outset. It is structured with a primary focus on harm prevention, prioritizing measures that aim to prevent harm rather than merely punishing companies. Its cost-effective nature stems from smart design principles that lead to significant savings.
- By calling for safety by design and privacy by default, the Vermont Kids Code serves as a path to accountability for tech companies. It simply requires tech to take a good, honest look at their products and then mitigate harms and the exploitation of our kids stemming from data management practices. Platforms that successfully undergo an impact assessment through the AADC framework are entitled to a 90-day right to cure, underscoring the clear benefits offered by this system.