WIRED HUMAN

MAY 2023

ROUNDTABLE FOR CHILD ONLINE SAFETY

VOL.2

"Childhood is Not for Sale."

Advancing the internet for children
to feel safe, healthy, and whole.

WHITE PAPERS THAT ELEVATE THE VOICES OF YOUTH

Prepared by: Lisa and Jason Frost
Wired Human 501 c3, www.wiredhuman.org
Our mission: "We protect kids from online harm and exploitation."

OUTLINE

01 What are the Challenges? The Voices of Youth

02 My Hope: A Song that Cries for Change

03 Why we need to pass KOSA and EARN IT

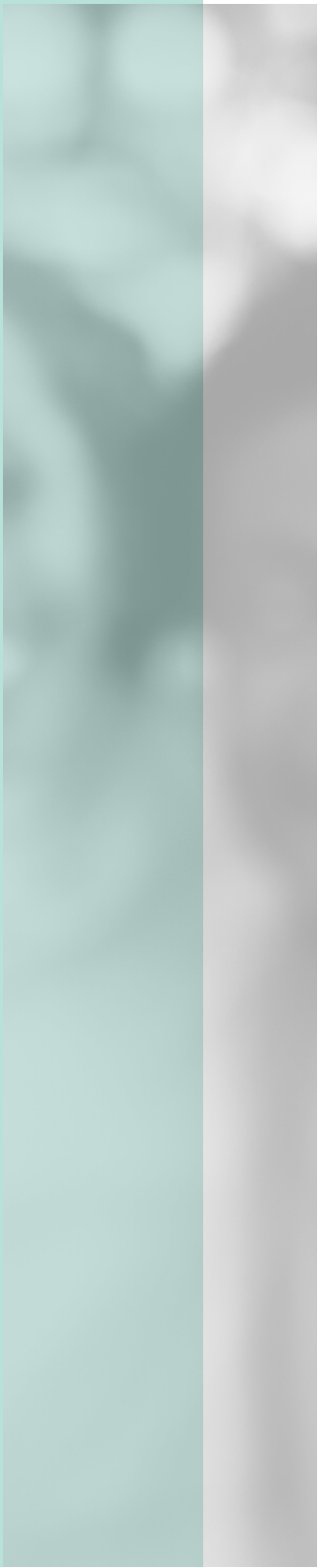
04 A Path to Online Safety:

- STOP harmful algorithmic funneling
- START age verification
- SOLITIFY transparency

WHERE DO WE GO:

As one 18-year old concluded: *"We need change at the rate we are going. Our world is divided right now. So we need to bring the world together if we want to see a future for our children."*

This report outlines three core standards to ensure child online safety.



INTRODUCTION

In February and May 2023, Wired Human gathered youth, top-level government and legislative officials, academics, tech industry leaders, and child online safety advocates at the "DC Roundtable for Child Online Safety" to find a path to better protect kids from online harm and exploitation.

This White Paper outlines **three online safety standards** developed by youth and top-level child online safety experts from across the nation and Canada.

1. Age Verification:
2. Accountability for Algorithmic Funneling
3. Transparency

The "Childhood is Not for Sale" industry standards reflect non-negotiable standards for tech platforms to protect underage users from harm.

Moving forward, The "DC Roundtable for Child Online Safety" will gather youth and top-level field leaders to highlight these standards before Congress.

At our next Roundtable in October 2023, we will focus on youth sharing with Congress about online harms. We are also developing a "**Congressional Briefing"** taking place early in 2024.

We believe this will be the "Child Safety Congress." It is time that We, the People, reclaim our power to 'choose' how to grow and learn in a tech omni present world.

Jason and Lisa Frost, Wired Human

01

WHAT ARE THE CHALLENGES? THE VOICES OF YOUTH

YOUTH ACTIVIST, 26:
DC ROUNDTABLE

#1 CHALLENGE: SUICIDAL IDEATION

"My brother, the one person I had in my life who knew me my entire life through foster care, he took his life because of negative impact of social media."

- **Negative impacts of social media, such as anxiety, depression, and low self-esteem, are all amplified and detrimental to those already struggling in their home environment.**
- **According to Surgeon General [Vivek Murthy], social media harms mental health. 13 is too young of an age to have social media.**

"Much of the evidence we do have indicates that there is enough reason to be deeply concerned about the risk of harm social media poses. For example, adolescents who spend 3+ hours per day on social media face double the risk of developing symptoms of depression and anxiety."

-Vivek Murthy

YOUTH ACTIVIST, 26:
DC ROUNDTABLE

#2 CHALLENGE: SEX TRAFFICKING

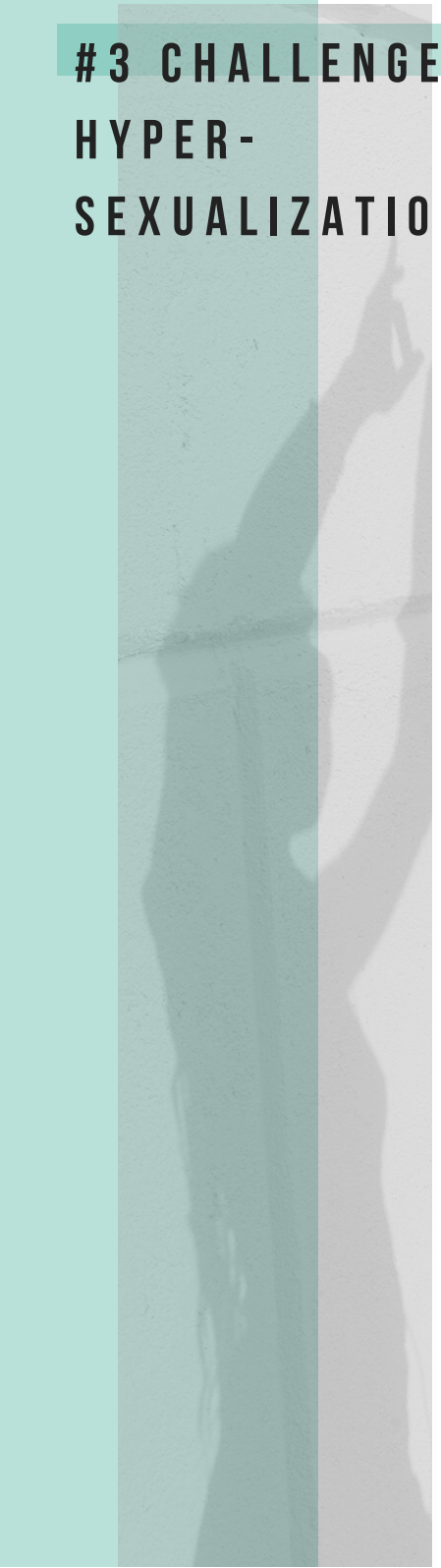
> *My friend who decided to travel the world would sell himself by advertising himself on social media to pay for his bills. This is what we refer to as "[abuse] survivor sex"* through social media; as young men in foster care, we don't always know what a healthy relationship is; at a young age, we turn to social media and figure out how to act and turn to pornography to learn what "love" is. [Coming out of foster care], we didn't understand how to experience healthy relationships.*

- Children and youth who do not experience healthy relationships seek love through other avenues, especially through social media.
- Youth are easily susceptible to being groomed online if they have no one close to turn to.

* ***Survivor sex*** *refers to exploitive sexual patterns that were learned through being abused as a child.*

YOUTH ACTIVIST, 18:
DC ROUNDTABLE

#3 CHALLENGE: HYPER-SEXUALIZATION



> *If I post a curse word, my Instagram will be disabled. If I post a video of me shaking my butt, it won't be. Everything is about sex and exploitation when it comes to youth.*

- **Hyper-sexualization of children has become the norm. Children of color are particularly vulnerable to falling victims to sex trafficking online.**

- **In a two-year review of all suspected human trafficking incidents in the U.S., 94% of sex trafficking victims were female, 40% were Black, and 24% were Latinx.** *Bureau of Justice Statistics, Characteristics of Suspected Human Trafficking Incidents, 2008-2010 (April 2011), p.6; The National Center for Victims of Crime, NCVRW Resource Guide (2013), p.24.*

- **Algorithms groom kids so predators don't have to.**

YOUTH ACTIVIST, 18:
DC ROUNDTABLE

#4 CHALLENGE: PREDATORS HAVE FREE RANGE ON PLATFORMS KIDS USE

"I was on a streaming app starting at age 12. Accounts were getting banned for individuals under 18. However, I made the app enough money by posting inappropriate content of myself, and the company allowed my account to stay active."

- **Predators online have never had so much access to children.**
- **Predators exploit the vulnerability of children and take advantage of the weaknesses built into the platforms kids use.**
- **The cycle of commodifying sexual pleasure and kids is ever-growing without kids being able to make it STOP.**

YOUTH ACTIVIST, 18:
DC ROUNDTABLE

#5 CHALLENGE: EXTREME CONTENT

"The number one thing on social media [is] clout. People do anything for fame."

- **Minors are exposed to and rewarded for extreme and degrading content.**
- **Influencers utilize clickbait content that features victims getting humiliated, shamed, or assaulted (punched in the face) to get picked up by algorithms. It is all about attention seeking.**
- **Posting anything extreme, whether illegal or not, gives you fame in return (clout).**

YOUTH ACTIVIST, 18:

"Tricks [pimps] sell people through social media and can make accounts after accounts. You see that there's people re-creating accounts over and over again. These kids [victims of sexual exploitation] look young and even are young."

#6 CHALLENGE: SEXPLOITATION & TRAFFICKING

- **Social media normalizes and pushes exploitation through its algorithmic structure.**
- **Grooming is so widespread that one young activist states, "It happened to everyone I knew."**
- **The sex trade is moving online through platforms like OnlyFans, Twitter and Instagram. Social media platforms are facilitators of the commercial sex trade.**

YOUTH ACTIVIST, 26

#7 CHALLENGE: PORN & GROOMING

"Since a young age, we turned to social media how to act. We turned to pornography to learn what relationships look like. Why change this behavior, because 'isn't this love?'"

- **Commodifying children's bodies is so normalized online that producing child porn (child sexual abuse material) is common practice leaving law enforcement completely overwhelmed by the shear magnitude of illegal content.**
- **In 2022, NCMEC's CyberTipline received more than 32 million reports of suspected child sexual exploitation.**

YOUTH ACTIVIST, 26

#8 CHALLENGE: ALGORITHIC DESIGN

"Because we've viewed pornography from a young age, experienced sexual assaults, and longing for love and belonging. We are susceptible to the algorithms presented to us. We are easy prey."

- **Algorithms amplify the platforms of public figures such as Andrew Tate, who promote the idea that women and girls are property and objects for sexual pleasure.**
- **The algorithm will always prioritize hyper-sexualized [or extreme] content.**

#9 CHALLENGE: GROOMING

YOUTH ACTIVIST, 18:

"I had 7 different direct messages asking me if I want a 'sugar daddy' just in the 4 hours we have been in the room while discussing child online safety."

- **The risks for youth online do not stop at eating disorders, over-exercising, and lifelong psychological issues. Innocence is exchanged for cash, and social media companies are "turning a blind eye" to this travesty.**

- **Profits are continually placed above children's safety and well-being. See: Tina Frundt's interview with the Guardian**

02

THE VOICES OF YOUTH
A SONG: MY HOPE

LYRICS: MY HOPE

song is written by 18-year-old Kendra Lukens for the DC Roundtable, performed on piano

Waking up everyday
Grabbing my phone and scrolling
First thing in the morning
Come what may

It sets you up for failure
Reading all the sad things
Sets your mind up for disaster

My hope is that social media
Will lift us up
Such a beautiful creation
Why can't we use for the better
My hope is that we can unite

I don't wanna open my phone
And the first thing I see
Is the bad things
Let's lift each other up

My hope is that we can make changes
Protect the youth for they are the future
Our future is bright
If we do what's right

My hope is for better days
Come what may
We can make some changes
And make the world a better place

My hope is that we can grow
And unite this divided world
But we gotta work together
And that's just my hope for the future

03

LEGISLATIVE EFFORTS
KOSA & EARN IT

SOLUTIONS:

LEGISLATIVE EFFORTS

PRESENTED BY COLLIN ANDERSON, CHIEF POLICY ADVISOR SEN. RICHARD BLUMENTHAL (D-CT)

- **Kids Online Safety Act** and the **Earn It Act** are two bills that address the harm against children online, reintroduced in May 2023 and passed out of the committee unanimously.

Earn It Act

- Removes blanket immunity for tech platforms when they are responsible for distributing child sexual abuse material targeted by social media such as Facebook, etc.

KOSA Bill

- KOSA creates a duty of care for platforms that facilitate and fuel eating disorders, suicidal ideations and behaviors, sexual exploitation, physical violence and bullying, and other harms. Tech companies that fail to address these dangers could be legally liable. KOSA requires covered platforms to provide tools and safeguards to parents and kids and a reporting mechanism.

- KOSA seeks to establish transparency standards by requiring covered platforms to hire independent auditors who will report to the public with scientific data identifying risks and harms to underage users.

SOLUTIONS:

LEGISLATIVE EFFORTS

PRESENTED BY COLLIN ANDERSON, CHIEF POLICY ADVISOR SEN. RICHARD BLUMENTHAL (D-CT)

- **What can we do to gain more support?** Call your Senators and Representatives to co-sponsor these bills. Usually, when there are more co-sponsors, there is more attention to give floor time to the bills we are working pass.

- Advocacy on the hill works.

- Additional advice and proactive steps beyond calling Senators and Representatives are to talk to colleagues and other organizations to build a broad network.

- 'When twelve parents came to Capitol Hill to share their tragic stories of losing their children to social media-related trauma created significant forward momentum for these bills. Furthermore, having children and youth come to the hill to share their stories leaves a powerful impact on the legislative process of getting KOSA and Earn-It passed.'

04

CHILD ONLINE SAFETY STANDARDS

AGE VERIFICATION

#1 CHILD ONLINE SAFETY STANDARD

BASED ON THE FEBRUARY 6TH ROUNDTABLE DISCUSSIONS, ENCOMPASSING WHITE PAPERS AND THE YOUTH ADVOCATES, AND EXPERT FEEDBACK, WE IDENTIFIED AGE VERIFICATION AS ONE OF THE CORE ONLINE CHILD SAFETY STANDARDS TO BE DEVELOPED IN OUR GROUP DISCUSSIONS.

AGE VERIFICATION

ONLINE CHILD SAFETY STANDARD

- ***Problem:*** *Tech companies do not only need to prove that a user is over 18 but also identify users who are trying to imitate underage children. Children need to be verified. Otherwise, age verification creates a back door for the "fox to enter the henhouse."*

- ***Goal:*** *Create an age verification standard that bridges the problem (adults impersonating children to groom and exploit online).*

AGE VERIFICATION

WHY DO WE NEED AGE VERIFICATION?

- Age verification protects kids and prevents predators from pretending to be kids.
- Age verification keeps predators from accessing kids on social media.
- Age verification proves that real people set up accounts.
- Age verification addresses bi-partisan interests: age verification mitigates lawsuits, disinformation, manipulation, and false identity and proves users are human.
- Age verification is even more crucial as AI poses a considerable danger, for example, teaching predators to learn how to better emulate and communicate with thirteen-year-olds.
- Putting policies such as age verification in place is essential to protect minors because it sets a precedent. For example, Canada has stiff penalties for providing pornography to children but lacks an enforcement mechanism.
- Youth voices (18 years old): "Tricks [pimps] sell people through social media and can make account after account. You see that there's people re-creating accounts over and over again. These kids [victims] look young and even are young."
  -

AGE VERIFICATION

- *"I had 7 different texts on my phone asking me if I want a 'sugar daddy,' just in the 4 hours we have been in this room while talking about online safety."*

- *"I was on a streaming app starting at age 12. Accounts were getting banned for individuals under 18. However, I made enough money for the app by posting inappropriate content of myself, and the company allowed my account to stay active. The company would keep your account active if you made enough money on the app by doing inappropriate things."*

- In many ways, age verification has been implemented already: We apply it to drinking and driving or tobacco sales, where it protects sellers and reduces liability.

- To date, Big Tech has no incentive to comply with age verification, which is why legislation like the "EARN IT Act" is essential. We have tools available now to remove child sexual abuse material, but no deterrent for tech companies to take responsibility.

- We know that the lack of age verification regulations has led to unprecedented access to digital content and products, creating a mental health crisis among youth. Still, the average American does not view this as an issue.

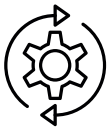
- Public awareness of the depth and darkness associated with technology and social media exposure is critical. The dangers lurking in online spaces, such as video chat games, are vastly unknown.

- Implementing age verification in the name of health or kids is plausible.

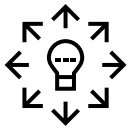
AGE VERIFICATION

WHAT DOES EFFECTIVE AGE VERIFICATION LOOK LIKE?

Effective age verification needs to (be):



Automated

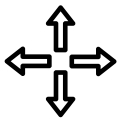


Scalable

Protect children from groomers, self-harm and suicide

Promote authentic relationships

Promote an increase in the happiness index (how can our kids be happy again?)



Find what is already there and build/expand on it.

AGE VERIFICATION

IN WHAT WAYS DOES AGE VERIFICATION NEED TO BE REGULATED, ADJUSTED, OR IMPLEMENTED TO PROTECT MINORS ONLINE EFFECTIVELY?

- Age verification must be “reliable and delete personal information. Such information should not be used for anything else besides verifying a minor’s age.”
- Age verification must support underserved communities, which are more vulnerable to trafficking (impoverished, foster youth, etc.), as they are commonly targeted online.
- People don’t care about the product. They care about the experience. Technology already exists. How can we utilize it?
- Age verification has to be auditable, potentially through a third-party government agency.
- Example: The UK has a third party that provides age verification, which is audited by an agency and then audited by the government.
- Age verification should go hand in hand with having filters on by default- The first company that did this showed a 75% increase in sales. Ideally, it won’t cut into sales.

AGE VERIFICATION

HOW CAN TECHNICAL MEASURES VERIFY A MINOR'S AGE WITHOUT COMPROMISING DATA AND PRIVACY?

- The distance between your eyes and mouth or ears and mouth determines whether you are an adolescent.
- Computer analytics can predict ages under 25 within a few months.
- Google states they can estimate within two months how old you are.
- Google monitors your content and presents ads based on your unique characteristics like age and interests.
- Many new websites require you to have an account, a unique username, and a date of birth.
- Microsoft (and three other companies) has a program for age verification using video stream information that is only stored long enough to verify identity and provide information if adults pose as teenagers to the proper authorities. Utilizing AI to confirm identity every time minors get on social media platforms is possible. For example, allowing the video camera to turn on while a user performs specific randomized actions (blink three times, look left/right four times, etc.)

AGE VERIFICATION

HOW CAN TECHNICAL MEASURES VERIFY A MINOR'S AGE WITHOUT COMPROMISING DATA AND PRIVACY?

- You can only access the web or specific apps if you confirm your identity.
- AI programs already exist but might have to be implemented by a third party.
- It is possible to use ID.me- which is used in the military. "If you get verified through ID.me, you get VIP access to certain content."
- KOSA- NIST (National Institution of Standards and Technology establishes a framework for cybersecurity) wants you to come up with age verification practices and come back in a year- not an enforcement.
- *Example:* There are over ten companies that provide age verification in Canada. You need a login key emailed to you, which changes about every six months.
- Could we create an age verification incentive allowing social media to make more money off children? Requiring a premium set of services that parents can pay for would enable tech companies to reinvest a certain percentage to improve security for free accounts.

AGE VERIFICATION

HOW CAN TECHNICAL MEASURES VERIFY A MINOR'S AGE WITHOUT COMPROMISING DATA AND PRIVACY?

- How can we leverage AI to prevent predators from talking to children?
- In cyber class, to catch predators, especially on the dark web, you can monitor their data and put together a picture of who they are. Thirteen-year-olds aren't accessing certain services/websites/etc.
- Get enough information on predators, then compile, analyze, and present that data to bring it to the market.
- Predators are using social media. They dream of having a computer program to groom their victims (research on keywords, music, shows, references, current slang, etc.)

AGE VERIFICATION

DISTINCTION: HOW DO AGE VERIFICATION IMPLEMENTATION TECHNIQUES HAVE TO BE ADAPTED TO CERTAIN PLATFORMS (SOCIAL MEDIA, PORN, GAMING)?

- When it comes to social media, it might be a way to require parents to sign off on their children's social media accounts. This proposal remains challenging:
- What about abusive parents or adults who might want to give access to children they plan to groom?
- How do you prove guardianship? How will they know who is actually their parents?
- If they have parental controls, can that be abused? What are some solutions for that? There are potential adverse outcomes — for example, custody battles. One parent wants to give social media access; the other doesn't. Facebook won't know that one said yes, the other said no, or if I go to my friend's parents, how will they know?
- There's peer pressure- not just from youth to youth, but youth to parents.
- No parents want their kids not to be included/uninvited.
- We've allowed technology to babysit our kids.

AGE VERIFICATION

DISTINCTION: HOW DO AGE VERIFICATION IMPLEMENTATION TECHNIQUES HAVE TO BE ADAPTED TO CERTAIN PLATFORMS (SOCIAL MEDIA, PORN, GAMING)?

- Social media wants youth to join as quickly as possible; however, advertisements should only be granted to minors' accounts once they are of age. It is an investment to secure child or youth users while avoiding monetization until 18 years or older.

- Most social media platforms are for young people 13 and older. Why does the law not require age verification for 13-year-olds?

FURTHER DISCUSSION

- We need to learn from others- this is a global issue- reach out to other organizations, countries, states, etc. and replicate/analyze/pull from their work.

- Look at the motivations of key stakeholders, industries, companies, etc., and find the win-win with what's possible with technology.

- We should consider a verification process for all consumers to prevent crimes, false identities, and AI abuse from happening.

TRANSPARENCY

CHILD ONLINE SAFETY STANDARD

BASED ON THE FEBRUARY 6TH ROUNDTABLE DISCUSSIONS, ENCOMPASSING WHITE PAPERS AND THE YOUTH ADVOCATES, AND EXPERT FEEDBACK, TRANSPARENCY WAS IDENTIFIED AS ONE OF THE CORE ONLINE CHILD SAFETY STANDARDS TO BE DEVELOPED IN OUR GROUP DISCUSSIONS.

TRANSPARENCY

ONLINE CHILD SAFETY STANDARD

- Just like the auto industry is required to release safety reports and five-star crash test ratings, so should tech companies be accountable for being transparent about how they interact with minors' data, the risks their products and services pose to children, and the steps they are taking to address those risks.

- **Problem:** Tech companies are largely shielded from publicly disclosing how they interact with a child's data and how they prioritize a minor's safety when processing that data. I.e., algorithms that use user engagement data to maximize attention retention with harmful content.

- **Goal:** Transparency reports (focused on the collection, interpretation, and use/purpose of that data), risk assessments, and child safety priorities must be made publicly accessible for meaningful accountability.

TRANSPARENCY

WHY DO WE NEED TRANSPARENCY?

- Transparency drives accountability and ensures users that companies are working in their best interest.
- Transparency allows companies to learn from each other.
- Companies must have consistent data to report on; however, it should be aggregated and anonymized.
- Users deserve to understand how companies are profiting from their data. They ought to know what a tech company's primary mission is. We know that Big Tech's business model comes down to advertising dollars, but it must be publicly transparent. The more data companies collect, the more they know who and how to target. If we are the product, we need to understand why/how we are the product and how children are victimized in the process.
- Companies can “slice and dice” data however they want.
- Roundtable Member: “My relationship with my phone allows me to have a stronger relationship with tech companies than with my husband.”

TRANSPARENCY

- Transparency prevents users from experiencing gaslighting on what's happening.
- Maximum profit rather than our needs drive tech companies.
- **Tech companies are part of a [trillion]-dollar industry that directly facilitates child trafficking and sexual exploitation.**
- **AI has already been launched without proper safety measures in place.** Privacy and transparency must be considered in the design phase of all AI development.
- Roundtable member: "I believe our decline in civilization is due to extreme anonymity in our interactions. Holding people accountable for their actions and words will restore our community."

TRANSPARENCY

HOW CAN WE REQUIRE TECH COMPANIES TO PUBLICLY DISCLOSE HOW CHILD PROTECTIONS ARE BUILT INTO DEVELOPING THE PLATFORMS THAT MINORS INTERACT WITH?

- Voluntary principles do not work.
  Example: Tech companies, comprised of different platforms (including cloud-based companies, gaming, social media, etc.), formed the Tech Coalition to address the online exploitation of children.

- Together, the Tech Coalition built TRUST, a Voluntary Framework for Industry Transparency, intending to report their efforts to combat online child sexual exploitation and abuse (CSEA).

TRUST consists of 5 frameworks:

1. Reporting should support trust and accountability so companies continually improve practices and policies.
2. Reporting shall reflect the unique nature of each company's services.
3. Reporting should depend on platform size – as companies grow, they should increase transparency measures.
4. Reporting should be regular, whether annually or quarterly, and should provide comparative information so we can track trends.
5. Reporting should not compromise safety or privacy (and it shouldn't be tied to specific individuals)

- These principles remain vague; there seems to be little follow-through on such principles to ensure online child safety regarding trafficking and abuse online.

TRANSPARENCY

- Instead of transparency measures remaining voluntary, every member of the Tech Coalition should commit to transparency and be held accountable for it.

- The framework for the Tech Coalition should be: asking each other to report for policies on child abuse sex materials.

- **Guiding Questions:**

    - *What is your process for implementing tools to curb abuse online?*

    - *What is the outcome of such tools?*

- Consumers need to know how these protections would play out.

- We [as consumers and child online safety advocates] want transparency, but why would tech companies want to comply? What would their incentives be? **There must be legislation for accountability.** Legislation should be implemented on the national level but can start at the state level. Big tech companies are solely concerned about lawsuits and losing money.

- **We** [as consumers and child online safety advocates] **need a federal regulatory commission to assess tech companies.**

TRANSPARENCY

- To date, legislators are putting “solutions” [legislative proposals] on paper.
- These efforts give us the platform to help drive the next steps.
- We [as consumers and child online safety advocates] want to know basic tools, how they are developed, and how they work.
- We [as consumers and child online safety advocates] ask companies to conduct child rights risk assessments and release the results.
- Companies have portals where you can complain about inappropriate content and violations. Having transparency on how many complaints they’re receiving, especially on children, and knowing how these complaints were handled as to what effect would help assist victimized kids.
- Roundtable member: “We have had many instances in our school districts where children have been harassed. We encourage children to defend themselves, but we also want adults to do what they should be empowered to do. We can act accordingly if we know how certain complaints play out.”
- The EARN It Act will lead to a baseline of accountability and should be expanded.

TRANSPARENCY

- We [as consumers and child online safety advocates] need criminal accountability across companies.

- We [as consumers and child online safety advocates] need private rights to action (would allow us to eliminate the immunity).

- We [as consumers and child online safety advocates] should be able to bring civil, criminal, and federal lawsuits for the crimes on these platforms.

WHAT ARE WAYS TO PUBLICLY DISCLOSE HOW MUCH MONEY A PLATFORM INVESTS INTO MITIGATING HARM TO MINORS, CURBING THE GROOMING OF MINORS, ETC.?

- Companies need independent auditors. An auditor can offer genuine insight as to whether companies are being transparent.

- There are many rules and laws, but they're not enforced. We need an enforcement mechanism.

- If there is no independent auditing, nothing regulates big tech companies. In the past, representatives from tech companies have not told the truth, even in front of Congress.

TRANSPARENCY

HOW CAN WE TAKE ACTIVE STEPS TO ADVANCE TRANSPARENCY INITIATIVES TO SUPPORT THIS STANDARD?

- We need baseline data to know where to target resources for improvement.

- We need an assessment of predators on tech platforms: Are child predators on specific social media platforms? What are companies doing about it? Are companies reporting threats to law enforcement? We need to know how companies will measure these efforts to ensure child safety online.

- One of the biggest roadblocks is that no brand or leadership wants to be associated with this problem, but child exploitation and abuse are a problem in the digital world.

- For example, Apple developed a prevention tool for anyone under a certain age (parents can opt into the tool through a family plan) If children use the phone to send explicit images, a text would be sent to them, cautioning their decision (which would blur the explicit image.)

- If Apple's algorithms detect that a predator is requesting explicit or personal info from a child, the predator receives a text message cautioning their illegal decision.

- Scanning iOS devices and iCloud photos for child abuse imagery.

TRANSPARENCY

- The first two tools were passed (they've been released for about a year); The third received a big uproar. After much deliberation, Apple decided it would not release the third tool. Apple instead pledged to invest more resources into the first two tools. Apple claimed they didn't know whether the first two tools were functional because they didn't have data.

- Questions Apple should be able to answer: *How many images are being blurred? How many kids are being sent these messages? How many reports are being sent to law enforcement?*

- There are caps on punitive and civil damages. Predators will still commit "bad acts" when they know it would only cost them $250.

- We need to look at model legislation that's been passed. We take this model legislation to the states, and Congress picks it up for further steps.

- There is a register for protecting children from sexual predators. Companies should be able to utilize these registers in tandem with firewalls.

- *Example:* In Sweden, all users are assigned a unique identifier that can be individually traced to identify predators.

TRANSPARENCY

- State laws are different: **How do we pursue the issues with registers nationally to identify and prosecute predators?** So far, we haven't been able to accomplish national registers due to privacy issues. This gap needs to be closed at the state level before we attempt efforts at the federal level.

- An enforcement mechanism is needed by having a federal commission or regulatory agency check on industry numbers to show compliance.

- **Federal, criminal, and civil lawsuits need to be brought, which will require the Earn It Act to pass. Further expansion of the Earn It Act will be needed.**

- There needs to be transparency on what enforcement is doing and not doing and if it is working.

- Find and identify the predators (look at Sweden's model); look at the history of criminal behavior.

- We need to learn from other countries' challenges in implementing age verification.

- We need to challenge anonymity online—half of the American population self-identifies with loneliness. We need a concerted effort to have a face-to-face interaction on a society level; reset the world we transitioned into for more in-person interaction.

ACCOUNTABILITY FOR ALGORITHMIC FUNNELING

CHILD ONLINE SAFETY STANDARD

BASED ON THE FEBRUARY 6TH ROUNDTABLE DISCUSSIONS, ENCOMPASSING WHITE PAPERS, THE YOUTH ADVOCATES, AND EXPERT FEEDBACK, TARGETING ALGORITHMIC FUNNELING WAS IDENTIFIED AS ONE OF THE CORE ONLINE CHILD SAFETY STANDARDS TO BE DEVELOPED IN OUR GROUP DISCUSSIONS.

ALGORITHMIC FUNNELING

ONLINE CHILD SAFETY STANDARD FORMAL DEFINITION: ALGORITHMIC RECOMMENDATION SYSTEM

- **Problem:** Algorithmic AI funnels a child into destructive and exploitive content. Algorithms monetize childhood by learning what content will produce maximum user engagement, even if the content is harmful to children.

- **Goal:** Based on the child's vulnerabilities, their online engagement should mirror a similar experience to what is expected in a library. Books should not fly off the shelves to capture a child's engagement; instead, the child should be empowered to seek out information based on their interests.

ALGORITHMIC FUNNELING

WHY DO ALGORITHMS NEED TO BE *REGULATED, ADJUSTED, OR STOPPED* TO PROTECT MINORS ONLINE EFFECTIVELY?

- Online, concepts such as sex, drugs, gambling are digitized, monetized and scaled to attract engagement and influences consumer behavior of every young person with a smartphone. It's "Las Vegas" by design.

- AI funnels a child into dangerous and exploitive content. Algorithms monetize childhood by learning what content will produce max user engagement even if the content is harmful to children, which can in turn lead to addictive behavior.

- Digital engagement is largely catered toward funneling content (most reels for example are 30 seconds).

- Algorithms cause us to live in a feedback loop. There is a positive feedback loop between what we're seeing online, which is impacting how we are living our lives in our communities.

- Youth Voices:

"Because we've viewed pornography from a young age, experienced sexual assaults, and longing for love and belonging. We are susceptible to the algorithms presented to us. We are easy prey."

ALGORITHMIC FUNNELING

WHY DO ALGORITHMS NEED TO BE *REGULATED, ADJUSTED, OR STOPPED* TO PROTECT MINORS ONLINE EFFECTIVELY?

- Various pieces of policy address definitions of data, modeling, and use cases, yet there is limited shared industry language that promotes a foundation of critical thinking about technology and its intersection with public policy.
- We have slapped a band-aid on the lack of social connection as a society. Algorithms are designed around humans' vulnerabilities for connection with other humans.
- The problems with algorithms are that humans are the product.
- Twenty-one million women and 10 million men are diagnosed with eating disorders annually. Exploitive content, such as anorexic content, are channeled towards teens.

ALGORITHMIC FUNNELING

KEY STEPS TOWARD MORE ETHICAL AND SAFE ALGORITHMIC MODELS

- We need a universal legislative definition of data. What kind of data are we asking the government to regulate?
- What kind of monetization model is built into the algorithm?
- What are the parameters of the path of least resistance to gaining influence over user behaviors?
- What vulnerabilities are we allowing tech companies to exploit (insecurities, loneliness, gaslighting)?
- How can we advance a legislative (discovery) study to form the legislative definitions for data and algorithms (what models are being used)? NHS funding for the study?
- Take a larger bill and add a government study to define a universal legislative definition of data as a component. Add algorithmic models and parameters for how algorithms interact with user data and for what purpose?

ALGORITHMIC FUNNELING

KEY STEPS TOWARD MORE ETHICAL AND SAFE ALGORITHMIC MODELS

- AI is making choices for users. We are asking for the power of choice!
- How are we managing youth cookies online (algorithms are using cookies to analyze and respond to user data)
- How do parents understand cookies? Which kinds of cookies are linked directly to a user's identity?
- Because cookies work hand-in-hand with algorithms, parents should be aware of the types of data and cookies that are collected on their children and what categories these cookies fall into.
- It comes down to the power of choice, and parents should be able to guide children in their choices effectively.
- There is so much unknown. We need to know how data (such as cookies) and algorithms interact with each other and how parents can control it with their kids.
- What is the impact? The measured effects should be over 12 months or longer. Before tech companies release a digital product, it must be determined whether any of its components or the product as a whole would amount to a definition of harm. Safeguards around "pumping out" new iterations and breaking them on kids are not safe practices.

ALGORITHMIC FUNNELING

KEY STEPS TOWARD MORE ETHICAL AND SAFE ALGORITHMIC MODELS

- We must establish a bipartisan legislative workgroup that aims to identify any additional information gaps in the above areas and deliver a comprehensive landscape analysis through a diverse stakeholder group of participants.

- The legislative workgroup will explore a shared language around a universal data definition and algorithmic models.

- We need a universally accepted legislative definition of data and what we mean by algorithmic recommendation systems. We need to do this in collaboration with tech companies. In future sessions, we need to define the design points of tech.

WHERE DO WE GO FROM HERE? NEXT STEPS

Moving forward, The "DC Roundtable for Child Online Safety" aims to host a Congressional briefing developed by a coalition of youth and child online safety experts. The first three online child safety standards will be essential when messaging how to keep children safe online.

Before developing any further online safety standards, we must move to action and help move what we consider the two most promising child online safety legislative proposals KOSA and EARN IT that address the standards below "over the finish line."

We plan to do this hand-in-hand with youth. We are currently building a coalition of youth and are convinced that their thoughts and experiences speak loudest. What if youth were no longer victims of a broken web, but empowered leaders ready to create a better digital future?

Age Verification

Tech companies do not only need to prove that a user is over 18 but also identify users who are trying to imitate underage children. Children need to be verified. Otherwise, age verification creates a back door for the "fox to enter the henhouse."

Transparency

Tech industries must become more transparent in their business practices to create accountability and allow child-centered organizations to offer input, critique, and support. We are asking tech companies to identify what priority particular child online safety tools hold within their business development. How much money is being allocated to safety-by-design (child-centered approaches to developing their products)?

Combat Algorithmic Funneling

Children must be protected from algorithmic AI that funnels a child into dangerous and exploitive content. Based on the vulnerabilities of the child, their engagement online should mirror a similar experience as what is expected in a library. Books should not fly off the shelves in an attempt to capture a child's engagement; instead, the child should be empowered to seek out information based on their own interests.