

1 Bradley S. Schrager, Esq. (SBN 10217)
Daniel Bravo, Esq. (SBN 13078)
2 BRAVO SCHRAGER LLP
6675 South Tenaya Way, Suite 200
3 Las Vegas, Nevada 89113
Tele.: (702) 996-1724
4 bradley@bravoschrager.com
daniel@bravoschrager.com

5 Dani Pinter
6 Senior Legal Counsel, NCOSE
1201 F. St. NW, Suite 200
7 Washington D.C. 20004
dpinter@ncoselaw.org

8 *Counsel for Amicus Curiae*

Marci A. Hamilton, Esq.
CEO & Founder, CHILD USA
3508 Market Street, Suite 202
Philadelphia, PA 19104
marcih@sas.upenn.edu

Jessica Schidlow, Esq.
Legal Director, CHILD USA
jschidlow@childusa.org

Carina Nixon, Esq.
Senior Staff Attorney, CHILD USA
cnixon@childusa.org

10 **IN THE EIGHTH JUDICIAL DISTRICT COURT**
11 **OF THE STATE OF NEVADA IN AND FOR CLARK COUNTY**

13 STATE OF NEVADA,

14 Plaintiff,

15 vs.

16 META PLATFORMS, INC. f/k/a
17 FACEBOOK, INC.,

18 Defendant.

Case No.: A-24-886110-B

Dept. No.: XVI

**MOTION FOR LEAVE OF CHILD
USA AND THE NATIONAL
CENTER ON SEXUAL
EXPLOITATION TO FILE BRIEF
OF AMICUS CURIAE IN SUPPORT
OF PLAINTIFF STATE OF
NEVADA’S REQUEST FOR
PRELIMINARY INJUNCTION**

21 CHILD USA and The National Center on Sexual Exploitation, by and through
22 their undersigned counsel, respectfully submits this Motion for Leave to Appear as
23 *Amicus Curiae* and File a Brief in Support of Plaintiff State of Nevada’s Motion for
24 Preliminary Injunction pursuant to Nev. R. App. P. 29 & 32.

25 **STATEMENT OF INTEREST OF AMICI**

26 CHILD USA is the leading national non-profit think tank fighting for the civil
27 rights of children. CHILD USA engages in in-depth legal analysis and cutting-edge
28 social science research to determine the most effective public policies to protect

1 children from sexual abuse and online exploitation and ensure access to justice for
2 victims.

3 The National Center on Sexual Exploitation (“NCOSE”) is a nonprofit
4 organization, founded in 1962, that combats sexual exploitation and abuse by
5 advocating in state and federal courts for survivors, engaging in corporate advocacy
6 to encourage companies to adopt responsible and safe practices, particularly
7 regarding children, and advocating for legislative change that protects survivors and
8 promotes human dignity.

9 As organizations dedicated to protecting individuals—especially children—from
10 sexual abuse and exploitation and eliminating barriers to justice for victims of the
11 same, amici have a strong interest in the outcome of this case.

12 Amici are experts on the proximate, immediate, and persistent harms to child-
13 victims whose imagery is trafficked online, the ways in which digital communication
14 platforms like those operated by Meta exacerbate this abuse and the attendant
15 harms, and on the measures Congress has taken to address the epidemic of child
16 sexual abuse and exploitation by holding entities like Meta accountable. Amici
17 therefore has a substantial interest in ensuring that courts uphold laws that further
18 the fundamental public interest in child protection.

19 **THE *AMICUS CURIAE* BRIEF WOULD AID THIS COURT IN**
20 **CONSIDERATION OF THE ISSUES ADDRESSED BY THE PARTIES**

21 Tech companies like Meta have propelled much of the harmful content on their
22 platforms to optimize user engagement and increase their bottom-lines, often with
23 little regard to the collateral consequences. To that end, Meta recently made end-to-
24 end encryption the default setting on its Messenger platforms despite overwhelming
25 evidence that such a design feature has and will continue to needlessly endanger
26 scores of children and preclude them from seeking justice when they are harmed on
27 its platforms. Contrary to Meta’s stated position, there is nothing in the text or
28 legislative history of the Communications Decency Act (“CDA”) that shields

1 companies like Meta from liability based on their own affirmative conduct—here the
2 implementation of a design feature that it knows enables child abuse and exploitation
3 and subverts law enforcement efforts to prevent the same. Amici are concerned that
4 Meta’s position, if accepted, would provide a shield to powerful technology companies
5 with broad reach, while leaving the vulnerable children powerless and unprotected
6 online.

7 Amici are uniquely positioned to provide this Court with the social science
8 research on the prevalence and effects of online child exploitation, highlighting our
9 understanding of the impact on victims of online exploitation and abuse should the
10 District Court find that Meta is insulated from liability under Section 230 of the CDA.
11 Additionally, amici can assist this Court by providing an extensive overview of the
12 legislative history behind the enactment of the CDA including Section 230 immunity,
13 as well as how courts have attempted to reconcile these two areas of the law.

14 ///

15 ///

16 ///

17 ///

18 ///

19 ///

20 ///

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

28 ///

1 **CONCLUSION**

2 For the foregoing reasons, amici respectfully requests that this Court enter an
3 Order granting this Motion for Leave to Appear as *Amicus Curiae* and accepting the
4 *Amicus* brief attached hereto, as Exhibit A, in consideration of Plaintiff's Motion for
5 Preliminary Injunction.

6 Respectfully submitted 14th day of March, 2024.

7 **BRAVO SCHRAGER LLP**

8
9 By: /s/ Daniel Bravo

10 Bradley S. Schrager, Esq. (SBN 10217)
11 Daniel Bravo, Esq. (SBN 13078)
12 6675 South Tenaya Way, Suite 200
13 Las Vegas, Nevada 89113
14 Tele.: (702) 996-1724
15 bradley@bravoschrager.com
16 daniel@bravoschrager.com

17 Marci A. Hamilton, Esq.
18 CEO & Founder, CHILD USA
19 3508 Market Street, Suite 202
20 Philadelphia, PA 19104
21 marcih@sas.upenn.edu

22 Jessica Schidlow, Esq.
23 Legal Director, CHILD USA
24 jschidlow@childusa.org

25 Carina Nixon, Esq.
26 Senior Staff Attorney, CHILD USA
27 cnixon@childusa.org

28 Dani Pinter
Senior Legal Counsel, NCOSE
1201 F. St. NW, Suite 200
Washington D.C. 20004
dpinter@ncoselaw.org

Counsel for Amicus Curiae

1 **CERTIFICATE OF SERVICE**

2 I hereby certify that on the 14th day of March, 2024, a true and correct copy of
3 **MOTION FOR LEAVE OF CHILD USA AND THE NATIONAL CENTER ON**
4 **SEXUAL EXPLOITATION TO FILE BRIEF OF *AMICUS CURIAE* IN**
5 **SUPPORT OF PLAINTIFF STATE OF NEVADA’S REQUEST FOR**
6 **PRELIMINARY INJUNCTION** was served by electronically filing with the Clerk
7 of the Court using the Odyssey feline system and serving all parties with an email-
8 address on record, pursuant to Administrative Order 14-2 and Rule 9 of the
9 N.E.F.C.R.

10
11 By: /s/ Dannielle Fresquez
12 Dannielle Fresquez, an Employee of
13 BRAVO SCHRAGER LLP
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

EXHIBIT A



EXHIBIT A

1 Bradley S. Schrager, Esq. (SBN 10217)
Daniel Bravo, Esq. (SBN 13078)
2 BRAVO SCHRAGER LLP
6675 South Tenaya Way, Suite 200
3 Las Vegas, Nevada 89113
Tele.: (702) 996-1724
4 bradley@bravoschrager.com
daniel@bravoschrager.com

5 Dani Pinter
6 Senior Legal Counsel, NCOSE
1201 F. St. NW, Suite 200
7 Washington D.C. 20004
dpinter@ncoselaw.org

8 *Counsel for Amicus Curiae*

Marci A. Hamilton, Esq.
CEO & Founder, CHILD USA
3508 Market Street, Suite 202
Philadelphia, PA 19104
marcih@sas.upenn.edu

Jessica Schidlow, Esq.
Legal Director, CHILD USA
jschidlow@childusa.org

Carina Nixon, Esq.
Senior Staff Attorney, CHILD USA
cnixon@childusa.org

9
10 **IN THE EIGHTH JUDICIAL DISTRICT COURT**
11 **OF THE STATE OF NEVADA IN AND FOR CLARK COUNTY**

12 STATE OF NEVADA,

13 Plaintiff,

14 vs.

15 META PLATFORMS, INC. f/k/a
16 FACEBOOK, INC.,

17 Defendant.

Case No.: A-24-886110-B

Dept. No.: XVI

**BRIEF OF AMICUS CURIAE OF
CHILD USA AND THE NATIONAL
CENTER ON SEXUAL
EXPLOITATION IN SUPPORT OF
PLAINTIFF STATE OF NEVADA'S
REQUEST FOR PRELIMINARY
INJUNCTION**

18
19
20
21 **STATEMENT OF INTEREST & AUTHORITY¹**

22 CHILD USA is the leading national non-profit think tank fighting for the civil
23 rights of children. CHILD USA engages in in-depth legal analysis and cutting-edge
24 social science research to determine the most effective public polices to protect
25 children from sexual abuse and online exploitation and to ensure access to justice for
26

27
28 ¹ No party's counsel authored the brief in whole or in part. No person other than these amici curiae, their members, or their counsel contributed money that was intended to fund preparing or submitting this brief.

1 victims. Distinct from an organization engaged in the direct delivery of services,
2 CHILD USA produces evidence-based solutions and information needed by
3 policymakers, organizations, courts, media, and the public to increase child protection
4 and the common good.

5 The National Center on Sexual Exploitation (“NCOSE”) is a nonprofit
6 organization, founded in 1962, that combats sexual exploitation and abuse by
7 advocating in state and federal courts for survivors, engaging in corporate advocacy
8 to encourage companies to adopt responsible and safe practices, particularly
9 regarding children, and advocating for legislative change that protects survivors and
10 promotes human dignity.

11 Amici offers the foregoing brief in support of Plaintiff State of Nevada’s Motion
12 for Preliminary Injunction pursuant to Nev. R. App. P. 29 & 32. As organizations
13 dedicated to increasing child protection and eliminating barriers to justice for victims
14 of sexual abuse and online exploitation, Amici have a significant interest in the
15 outcome of this case. Amici are experts on the proximate, immediate, and persistent
16 harms to child-victims whose imagery is hosted and trafficked online, the ways in
17 which digital communication platforms exacerbate this abuse and its attendant
18 harms, and on the measures Congress has taken to address the epidemic of child
19 sexual abuse and exploitation by holding technology companies accountable.

20 The failure of the technology industry and specifically Electronic Service
21 Providers (“ESPs”) like Meta to develop child-protective processes has made child
22 sexual exploitation and abuse a feature of today’s digital communication platforms.
23 This profit over protection approach has been tacitly endorsed by and through judicial
24 expansion of Section 230 immunity which too often protects technology companies
25 from liability for their own criminal and tortious conduct. This case presents an
26 opportunity for the Court to restore the balance of the law in favor of child protection
27 and to reaffirm the proper interpretation of Section 230 consistent with its original
28 public policy objectives.

ARGUMENT

Child sexual exploitation and the production and distribution of child sexual abuse material (“CSAM”) are rapidly growing problems in the United States. While perpetrators are responsible for the resulting harm to children, so too are the technology companies that have brazenly enabled these heinous crimes by placing their own profits above child safety. Meta’s recent decision to default to encryption on its communication platforms will inevitably and profoundly curtail—if not outright prevent—law enforcement efforts to protect children from online predators and bring these bad actors to justice when they cause harm. Rather than simply eliminate this dangerous feature for its youngest users, Meta seeks to invoke a Section 230 defense to avoid liability for its defective messaging design that has and will continue to needlessly harm scores of vulnerable children. Such blatant attempts to avoid accountability and circumvent the law must not be entertained.

I. The Context of Online Child Sexual Abuse and Exploitation Is A Compelling Humanitarian Crisis That Must Be Given Due Consideration When Assessing The Suitability of Injunctive Relief

The proliferation of child sexual abuse and exploitation online has created a public policy crisis for lawmakers halt and address. To that end, if Meta is forced to comply with the injunction sought by the State, countless children will be spared of the devastating, long-term harms attendant to victimization.

A. The Online Marketplace for CSAM Has Reached Epidemic Proportions

The expansion of the internet and widespread use of mobile digital technologies together have facilitated an explosive growth in the online marketplace for the production and trafficking of CSAM. At any given time, there are at least one million child sex offenders searching for CSAM online.² Indeed, online exploitation

² EUR. PARLIAMENTARY RSCH. SERV., CURBING THE SURGE IN ONLINE CHILD ABUSE: THE DUAL ROLE OF DIGITAL TECHNOLOGY IN FIGHTING AND FACILITATING ITS PROLIFERATION 2 (Nov. 2020), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659360/EPRS_BRI\(2020\)0100_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659360/EPRS_BRI(2020)0100_EN.pdf)

1 and abuse of children has increased by 422% over the last 15 years.³ Millions of
2 individual users consume more than 15 million child sexual abuse images in a market
3 currently valued between \$3 and \$20 billion dollars annually.⁴ Unfortunately, there
4 are no signs that the market is slowing down.

5 Before the digital age, CSAM could only be shared physically thus making it
6 risky to find, and costly to produce and duplicate. Today, the availability of encrypted
7 messaging platforms, peer to peer networks, and the like have made it easier and
8 cheaper for perpetrators to produce CSAM and to connect, collaborate, and exchange
9 such materials with individual users—and to do so with virtual anonymity.⁵
10 Tragically, the demand for CSAM has reached epidemic proportions in recent years.
11 The COVID-19 crisis created a “perfect storm” for CSAM to proliferate as children
12 spent more, often unsupervised, time online. In 2020, 65.4 million images and video
13 files of CSAM were reported to the National Center for Missing and Exploited
14 Children’s (“NCMEC”) CyberTipline, the highest number of reports ever received in
15 a single year.⁶ As of 2018, there was a backlog of millions of suspected CSAM images
16 and videos in need of review while police reported being overwhelmed by the increase
17 in overall cases *and* the increased volume and severity of CSAM in each case.⁷ Given

18
19 0)659360_EN.pdf.

20 ³ U.S. SENT’G COMM’N, FEDERAL SENTENCING OF CHILD PORNOGRAPHY:
21 PRODUCTION OFFENSES 3 (2021),
22 [https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-](https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2021/20211013_Production-CP.pdf)

23 ⁴ Michael H. Keller & Gabriel J.X. Dance, The Internet Is Overrun With Images
24 of Child Sexual Abuse. What Went Wrong?, NYTIMES.COM (Sep. 2019), available at
[https://www.nytimes.com/interactive/2019/09/28/us/child-sex-](https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html?msclkid=531b2a24a55511ec9733999ed45d40bd)

25 ⁵ Id.

26 ⁶ Overview. (2020). National Center for Missing and Exploited Children.
27 <https://www.missingkids.org/gethelpnow/cybertipline>.

28 ⁷ ECPAT International. (2018). Trends in online child sexual abuse material.
Bangkok: ECPAT International. 32.

1 the recent increases in online CSAM activity during the pandemic that backlog has
2 likely expanded.

3 **B. CSAM Victims Suffer Significant Short-and Long-Term**
4 **Harms**

5 The trauma stemming from child sexual abuse is complex and individualized,
6 and it impacts victims both in the short-term and throughout their lifetimes.⁸ Child
7 sexual abuse takes a significant toll on victims' overall health, increasing the risk not
8 only for depression, anxiety, substance abuse, post-traumatic stress disorder (PTSD),
9 and suicidal ideation, but also physical ailments such as high blood pressure and
10 chronic illness.⁹ The paradigm shift from tangible to digital CSAM has exacerbated
11 these effects.¹⁰ A victim's mere knowledge of the presence and distribution of their
12 abusive imagery causes intense feelings of shame, humiliation, and powerlessness.¹¹
13 As explained by NCMEC, "[o]nce these images are on the Internet, they are
14 irretrievable and can continue to circulate forever. The child is re-victimized as the
15 images are viewed again and again."¹² Sadly, these feelings usually persist and even
16 intensify over time over time.¹³ The problem has taken on a new dimension as CSAM

17
18 ⁸ See generally, BESSEL VAN DER KOLK, *THE BODY KEEPS THE SCORE: BRAIN, MIND, AND BODY IN THE HEALING OF TRAUMA* (Viking 2014).

19 ⁹ See CENTERS FOR DISEASE CONTROL AND PREVENTION, NATIONAL CENTER FOR
20 INJURY PREVENTION AND CONTROL, DIVISION OF VIOLENCE PREVENTION, PREVENTING
21 SEXUAL VIOLENCE (last reviewed by the CDC on Jan. 17, 2020), available at
22 https://www.cdc.gov/violenceprevention/sexualviolence/fastfact.html?CDC_AA_refVal=https%3A%2F%2Fwww.cdc.gov%2Fviolenceprevention%2Fsexualviolence%2Fconsequences.html.

23 ¹⁰ Von Weiler, J., Haardt-Becker, A., & Schulte, S. Care and treatment of child
24 victims of child pornographic exploitation (CPE) in Germany, 16 *J. OF SEXUAL*
AGGRESSION 211, 216 (2010).

25 ¹¹ Id.

26 ¹² NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN, CHILD PORNOGRAPHY
27 POSSESSORS ARRESTED IN INTERNET-RELATED CRIMES: FINDINGS FROM THE NATIONAL
JUVENILE ONLINE VICTIMIZATION STUDY, available at
http://us.missingkids.com/en_US/publications/NC144.pdf.

28 ¹³ U.S. DEP'T OF JUSTICE, THE NATIONAL STRATEGY FOR CHILD EXPLOITATION AND
PREVENTION AND INTERDICTION, 11 at D-12 (2010), available at

1 involves increasingly younger victims and is becoming more violent and graphic over
2 time.¹⁴

3 In addition to the permanence of the imagery, CSAM victims are also
4 traumatized by their reach. Many victims whose images have been distributed online
5 experience debilitating anxiety about who has seen the images (i.e., family members,
6 coworkers) and preoccupation with the context and motives of their viewing.¹⁵ The
7 most difficult part of their revictimization is victims' knowledge that their images
8 may be used to groom future victims as a way to normalize the abusive
9 behavior.¹⁶ Often, perpetrators strategically produce CSAM in which victims are
10 seen smiling leading victims to worry that others will assume their enjoyment or
11 implicate them in the abuse.¹⁷ In fact, it is common for victims to feel as they though
12 they were an active participant in their abuse, which in turn contributes to a range
13 of psychological difficulties.¹⁸ These worries are not entirely unjustified; indeed, the
14 possession and viewing of CSAM enlarges the market and results in further
15 exploitation and sexual abuse of children. See, e.g., United States v. Williams, 444
16 F.3d 1286, 1290 (11th Cir. 2006) ("Our concern is not confined to the immediate abuse
17 of the children depicted in these images but is also to enlargement of the market and

18
19 <http://www.justice.gov/psc/docs/natstrategyreport.pdf> (finding that almost ninety-
20 five percent of CSAM victims suffer lifelong psychological damage and may never
overcome the harm, even after lifelong therapy).

21 ¹⁴ Id.

22 ¹⁵ Leonard, M.M., 'I did what I was directed to do but he didn't touch me': The
23 impact of being a victim of internet offending, 16 J. OF SEXUAL AGGRESSION 249, 254
(2010).

24 ¹⁶ Id.

25 ¹⁷ PALMER, T. & STACEY, L., JUST ONE CLICK: SEXUAL ABUSE OF CHILDREN AND
26 YOUNG PEOPLE THROUGH THE INTERNET AND MOBILE PHONE TECHNOLOGY (Barkingside,
UK: Barnardo's, 2013) .

27 ¹⁸ Steel, J.,et. al., Psychological sequelae of childhood sexual abuse: Abuse-
28 related characteristics, coping strategies and attributional style, 28 CHILD ABUSE AND
NEGLECT 785 (2004).

1 the universe of this deviant conduct that, in turn, results in more exploitation and
2 abuse of children.”).

3 **II. Meta’s End-to-End Encryption System Subverts the Fundamental** 4 **Public Policy Objective of Protecting Children Online**

5 In recent years, social media platforms—including Meta—have implemented
6 end-to-end encryption (“E2EE”) programs. E2EE poses a serious threat to the safety
7 of children online and in the real world, providing abusers with a “black hole” where
8 they can “trade illicit images of children with impunity.”¹⁹

9 By utilizing E2EE in messaging apps, social media companies simultaneously
10 facilitate the production and spread of CSAM while undermining law enforcement’s
11 ability to prosecute CSAM offenses.²⁰ This creates a dangerous reality in which
12 children have little to no protection or recourse from horrific sexual exploitation and
13 victimization.²¹

14 Before the rise of E2EE, ESP’s aided law enforcement by using a tool called
15 PhotoDNA to detect CSAM on their digital communication platforms. PhotoDNA
16 relies on “perceptual hashing” to “automatically scan content,” which has proven to
17
18

19 ¹⁹ Laura Draper, Protecting Children in the Age of End-to-End Encryption, Joint
20 PIJIP/TLS Research Paper Series 80 (2022), available at
<https://digitalcommons.wcl.american.edu/research/80/>.

21 ²⁰ See Nicholas A. Weigel, Apple’s “Communication Safety” Feature for Child
22 Users: Implications for Law Enforcement’s Ability to Compel iMessage Decryption,
23 25 STANFORD TECH. L. REV. 210 (2022) (explaining that “[e]ncrypted communications
24 have long presented an obstacle to law enforcement’s ability to gather valuable
25 evidence in criminal investigations—often described as the ‘Going Dark’ problem.”);
F.B.I Director Christopher Wray, Finding a Way Forward on Lawful Access: Bringing
Child Predators Out of the Shadows, Remarks delivered at Dep’t of Just. Lawful
Access Summit (Oct. 4, 2019), available at
<https://www.fbi.gov/news/speeches/finding-a-way-forward-on-lawful-access>.

26 ²¹ See Hanv Farid, Facebook’s Encryption Makes it Harder to Detect Child
27 Abuse, WIRED (Oct. 25, 2019), [https://www.wired.com/story/facebooks-encryption-](https://www.wired.com/story/facebooks-encryption-makes-it-harder-to-detect-child-abuse/)
28 [makes-it-harder-to-detect-child-abuse/](https://www.wired.com/story/facebooks-encryption-makes-it-harder-to-detect-child-abuse/) (stating, “[b]roader adoption of end-to-end
encryption would . . . significantly [increase] the risk and harm to children around
the world.”).

1 be “extremely accurate, reliable, and fast.”²² In fact, the ten-fold increase of CSAM-
2 related reports to NCMEC between 2011 and 2021 is “likely due, in part, to ESPs
3 adopting highly efficient detection tools” such as perceptual hashing.²³ E2EE
4 eviscerates the effectiveness of these detection tools and will almost certainly result
5 in a precipitous drop-off of CSAM reports to NCMEC.²⁴ The European Union’s 2020
6 enactment of the ePrivacy Directive provides a particularly concerning example of
7 this phenomenon. The ePrivacy Directive “limited ESPs’ ability to use hash-scanning
8 technologies to detect CSAM,” resulting in a 51% decrease in CSAM reports in just
9 the first six weeks.²⁵ In using E2EE, ESPs sacrifice child safety by severely crippling
10 their own ability to detect CSAM and report it to law enforcement.²⁶ This, in turn,
11 incapacitates law enforcement’s efforts to rescue children from abuse and bring
12 offenders to justice. F.B.I Director Christopher Wray spoke in stark terms about this
13 harsh reality:

14 “A cyber tip came in . . . that a 9-year-old girl was being sexually abused. The
15 abuser was using a particular app to send out images of what he was doing to that
16 little girl while remaining anonymous. Our agents . . . contacted the app provider.
17 Using legal process, we . . . locate[d] the little girl in less than 24 hours. We obtained
18 multiple search warrants, rescued her, and arrested her abuser. In another case . . .
19 a different child predator used a different app to distribute sexually explicit images

20
21 ²² Draper, *supra* note 19.

22 ²³ *Id.*

23 ²⁴ *Id.* “In end-to-end encrypted environments, ESPs cannot detect and report
24 CSAM using perceptual hashing techniques. As more and more tech companies
implement end-to-end encryption, the volume of reports to NCMEC will likely drop
dramatically.”

25 ²⁵ *Id.*

26 ²⁶ *Id.* See Farid, *supra* note 21 (noting that “child sexual abuse material shared
27 via . . . services that use end-to-end encryption generally don’t get reported to NCMEC
28 or anyone else.”). Hanv Farid is a professor of electrical engineering and computer
science at UC Berkeley and was part of the team that developed PhotoDNA in
collaboration with Microsoft.

1 of two young girls—one 12 and one 13 years old. Responding to a tip, agents served
2 legal process on that app provider and located and rescued those two girls in less than
3 12 hours. Both of those cases could have ended very differently. Because without the
4 information from the tech companies . . . we wouldn't even have known about those
5 children. And we wouldn't have been able to rescue them With the spread of
6 user-controlled default encryption, providers frequently can't identify horrific images
7 within encrypted data. That means tips like the ones that allowed us to rescue the
8 three girls in those examples—those tips just don't get sent. The harm doesn't stop.
9 The victims—those little kids—are still out there enduring the abuse.²⁷

10 Director Wray went on to explain that E2EE means ESPs only have access to
11 “metadata—for example, the time a message was sent, and its recipient—but not the
12 content of any messages, including attached photos and videos.” This greatly reduces
13 the chance of successfully holding child abusers accountable for their crimes, as
14 metadata “will almost never meet” the “high standard” the government bears to
15 conduct a search, bring criminal charges, and convict offenders.²⁸ Director Wray
16 noted that “while an algorithm or AI might reveal suspicious customer usage, that
17 kind of information—standing alone—will rarely be adequate to make a case and
18 bring the perpetrators to justice.”²⁹

19 Technology companies like Meta possess the tools to greatly stymie the flow of
20 CSAM on their platforms. They have the technology to assist law enforcement in
21 rescuing children from abuse and preventing offenders from perpetrating additional
22 heinous acts in the future. Instead, by utilizing E2EE instead of these vital tools,
23

24 ²⁷ Wray, *supra* note 20.

25 ²⁸ Id. See Draper, *supra* note 19 (stating that “[o]nce an offender has uploaded
26 and shared the content, end-to-end encryption effectively creates a black box around
27 the affiliated activity, preventing ESPs from accessing the content and preventing
law enforcement from lawfully retrieving it from the provider with a search
warrant.”).

28 ²⁹ Wray, *supra* note 20.

1 technology companies are enabling predators to seek out young users with impunity
2 while blocking law enforcement from seeking justice when they are harmed. Unlike
3 the CSAM sent via encrypted messages, the severe psychological and physical
4 consequences children suffer due to sexual abuse and exploitation do not simply
5 disappear. As Director Wray poignantly noted,

6 These stories are hard to listen to—and they should be hard to listen to—
7 because no one should ever have to endure what these victims lived through. It’s hard
8 for us to contemplate what those images actually show. Horrific abuse. Scarring,
9 awful crimes against kids, even infants and toddlers. Photographed and videotaped,
10 so it can follow them for years to come.³⁰

11 Technology companies must not be permitted to turn a blind eye to the
12 suffering of our children. Indeed, Meta is well-aware of its products’ capabilities
13 manipulate human behavior both on and offline, and of the harms that have befallen
14 its users as a result. Yet Meta is still refusing to take any responsibility by, for
15 example, eliminating the default E2EE feature for minor users from its design. As is
16 true in the physical world, these companies have a duty to not design or implement
17 digital products that are known to cause significant harm to consumers. And just as
18 a consumer may seek redress for their harm by filing a tort claim against the
19 manufacturer in the physical world, so should the consumers of these digital products
20 and the public be able to hold these technology companies accountable when they
21 allow CSAM to proliferate on their platforms or inhibit the efforts of law enforcement
22 to address the same.

23 **III. This Court Should Interpret Section 230 Consistent With Its Child**
24 **Safety Purpose To Avoid Further Injustice**

25 With the dawn of cable television, digital communication, and the growing
26 advent of the internet, Congress took on the daunting task of modernizing the
27

28 ³⁰ Id.

1 regulatory framework of the national telecommunications law, the Communications
2 Act of 1934. Communications Act of 1934, c. 652, Title I, § 1, 48 Stat. 1064 (1934)
3 (codified as amended at 47 U.S.C. § 151 et seq.). Among the many issues that a
4 nascent internet implicated, Congress sought to tackle only one: the ease with which
5 children could access or be subjected to sexually explicit materials.

6 To that end, in 1996, Congress passed what would eventually become Section
7 230 as part of the Communications Decency Act (“CDA”) to protect children online—
8 both from exposure to sexually explicit material and from the harms attendant to the
9 production and distribution of CSAM. See, e.g., 141 Cong. Rec. H8470 (daily ed. Aug.
10 4, 1995) (statement of Rep. White); (statement of Rep. Goodlatte) (“Congress has a
11 responsibility to help encourage the private sector to protect our children from being
12 exposed to obscene and indecent material on the Internet”). More precisely, Section
13 230 was intended to eliminate barriers to the development and use of technologies
14 that would “empower[ing] parents to determine the content of communications their
15 children receive through interactive computer services” by providing a *limited defense*
16 from liability for providers for their “good faith” attempts at restricting user access to
17 obscene and indecent materials on their platforms. *Id.* ; see also 47 U.S.C. § 230(c).

18 Notwithstanding the history and plain language of Section 230, powerful
19 technology companies including Meta have relentlessly advocated for an expansive
20 interpretation of Section 230’s defense and labored to reframe the law’s purpose from
21 child protection online to one limited to the civil liberty interests of adults.³¹ But this
22 extreme position that would have courts confer upon technology companies near
23 absolute immunity from liability under Section 230 is impossible to reconcile with the
24 statute’s plain language and underlying child-protection objectives.

25 “Section 230(c)(1) of the Communications Decency Act protects some parties
26 operating online from specific claims that would lead to liability for conduct done

27
28 ³¹ Nicolas Conlon, Freedom to Filter Versus User Control: Limiting Scope of § 230(C)(2) Immunity, 2014 UNIV. ILL. J. L. TECH. & POL’Y. 105, 115 (2014).

1 offline. But it is not a license to do whatever one wants online.” Henderson v. Source
2 for Pub. Data, L.P., 53 F.4th 110, 117 (4th Cir. 2022). Protection under § 230(c)(1)
3 extends only to bar claims that seek to impose liability on the defendant as a
4 publisher of third-party content. Id. While an online platform may be primarily
5 designed for posting and exchanging content, that fact alone does not sweep all
6 decisions made by the platform within the scope of its publishing role. Indeed,
7 “Section 230(c)(1) limits liability *based on the function the defendant performs, not its*
8 *identity.*” Force v. Facebook, Inc., 934 F.3d 53, 81 (2nd Cir. 2019) (emphasis added).

9 To that point, the functional transformation from early internet into a virtual
10 world with all manner of products and services has changed the way online platforms
11 relate with third-party content, which means Section 230’s limits on immunity are
12 more important than ever for child protection. Modern technology companies like
13 Meta are vastly larger, wealthier, and more powerful than were the online service
14 providers of two decades ago.³² These companies can not only manipulate content and
15 exploit user behaviors to drive up profits, but they also affirmatively exercise that
16 ability as well. “Many . . . successful internet companies . . . design their applications
17 to collect, analyze, sort, reconfigure, and repurpose user data for their own
18 commercial reasons, unrelated to the original interest in publishing material or
19 connecting users. These developments belie any suggestion that online
20 intermediaries are merely conduits of user information anymore.”³³

21 When companies design, develop, and implement their own digital tools, they
22 owe a specific duty to refrain from designing a product that poses an unreasonable
23 risk of injury or harm to consumers that is distinct from their duties as publishers of
24

25 ³² See Shira Ovide, Big Tech Has Outgrown This Planet, THE NEW YORK TIMES
26 (Oct. 12, 2021), <https://www.nytimes.com/2021/07/29/technology/big-tech-profits.html>.

27 ³³ Olivier Sylvain, Intermediary Design Duties, 50 CONN. L. REV. 203, 218 (2018)
28

1 third-party content. Here, Meta enacted its E2EE system despite its knowledge that
2 doing so would pose a significant risk of harm to its minor users. Accordingly, the
3 imposition of liability should center on Meta’s business decision to hide user content
4 under all circumstances, including from law enforcement investigating serious crimes
5 against children, and *not* on their decision to publish or host it in the first instance.
6 Simply put, “[w]hen a plaintiff brings a claim that is based not on the content of the
7 information shown” but rather on the defendant’s own conduct “the CDA does not and
8 should not bar relief.” *Id.* at 82; *see also* FTC v. Accusearch Inc., 570 F.3d 1187, 1204
9 (Tymkovich, J.) (10th Cir. 2009); Bauer v. Armslist, LLC, 572 F. Supp. 3d 641, 663-
10 64 (E.D. Wis. 2021) (describing Section 230 as a “definitional provision” requiring a
11 “fact-based inquiry.”).

12 When courts elide this distinction, they “frustrate[d] the core concepts
13 explicitly furthered by the [Communications Decency] Act and contravene[d] its
14 express purpose” transforming it “from an appropriate shield into a sword of harm.”
15 Doe v. Am. Online, 783 So. 2d 1010, 1019 (Fla. 2001) (Lewis, J., dissenting). Indeed,
16 without an obligation for online service providers to design and implement features
17 aimed at preventing foreseeable harms, no matter how easily they could so, and no
18 requisite standard of care by which to conform their conduct, consumers—especially
19 children and victims of abuse—are left to bear the consequences.

20 ///

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

28 ///

1 **CONCLUSION**

2 For all the foregoing reasons, amici respectfully requests that this Court grant
3 Plaintiff the State of Nevada’s request for a Preliminary Injunction and enjoin Meta
4 from continuing to endanger the children on their platforms.

5 Respectfully submitted 14th day of March, 2024.

6 **BRAVO SCHRAGER LLP**

7
8 By: /s/ Daniel Bravo

9 Bradley S. Schrager, Esq. (SBN 10217)
10 Daniel Bravo, Esq. (SBN 13078)
11 6675 South Tenaya Way, Suite 200
12 Las Vegas, Nevada 89113
13 Tele.: (702) 996-1724
14 bradley@bravoschrager.com
15 daniel@bravoschrager.com

16 Marci A. Hamilton, Esq.
17 CEO & Founder, CHILD USA
18 3508 Market Street, Suite 202
19 Philadelphia, PA 19104
20 marcih@sas.upenn.edu

21 Jessica Schidlow, Esq.
22 Legal Director, CHILD USA
23 jschidlow@childusa.org

24 Carina Nixon, Esq.
25 Senior Staff Attorney, CHILD USA
26 cnixon@childusa.org

27 Dani Pinter
28 Senior Legal Counsel, NCOSE
1201 F. St. NW, Suite 200
Washington D.C. 20004
dpinter@ncoselaw.org

Counsel for Amicus Curiae