



# ADAPTING TO THE FUTURE OF CHILD PREDATION

WHY CRIMINAL JUSTICE  
MUST BE AT THE CORE OF  
ANY EFFORT TO PREVENT  
CHILD EXPLOITATION ONLINE

*A report by Stop Child Predators*

December 2023

# TABLE OF CONTENTS

01

Summary

03

Good Bills vs.  
Bad Bills



06

First, Enforce  
Existing Laws

09

What Does it  
Mean to “Protect”  
Children?

12

The  
Government  
Makes a  
Lousy Parent

15

The Danger of  
Failing to Connect  
the Policy Dots

17

Conclusion

# SUMMARY

**Dozens of bills have been introduced in Congress that purport to address the issue of child exploitation online. Some are well intended while others are transparently self-serving. What most of them have in common, however, is a complete lack of focus on supporting, or including, law enforcement at any level whether international, federal, state, or local as a part of a solution for online child exploitation. Of even greater concern is the apparent failure to adequately implement and enforce existing laws or link efforts to mitigate child trafficking, child exploitation and missing children in either the digital or real world.**

We acknowledge that tech companies share significant responsibility to ensure a safer online world for children (and everyone). To this end, collaborations such as the [We Protect Global Alliance](#), have developed a [Model National Response](#) and a Global Strategic Response to guide tech companies, governments and stakeholders in the creation of multi-pronged systems and interventions that acknowledge the responsibility of all parties to create a world that protects children from sexual exploitation. Additionally, in 2020, the governments of the United States and four other countries collaborated with six of the largest tech companies to develop [Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse](#), putting forth a framework that includes policies and practices that can, and must, be implemented by tech companies.

The framework also outlines responsibilities of tech companies to report suspected exploitation and abuse activities to government and law enforcement.

While there have been growing demands – reflected in some recent legislative activity – to force technology companies to serve as a digital police force, tech companies are not law enforcement. They cannot issue search warrants or arrest people. Compelling them to act in this role may compromise actual law enforcement responses when crimes are identified. As the number of cybertips reported to the National Center for Missing & Exploited Children, overwhelmingly by the tech companies, continues to increase, the number of arrests and convictions of perpetrators is not keeping pace. No tech company can effectively combat child exploitation without a serious, concerted law enforcement effort to identify, prosecute, and convict offenders. Without adequate policing by actual law enforcement, no platform, no community, no family, no child will be protected from possible victimization.

**Without adequate policing by actual law enforcement, no platform, no community, no family, and no child will be protected from possible victimization.**

There is significant evidence, reflected in cybertips, that on-line, child sexual exploitation material is generated by well organized criminal enterprises, both domestic and international. Responding to these threats requires a sophisticated, coordinated law enforcement response best carried out by skilled investigators with the ability to network efficiently with well-trained municipal, state, federal, and international law enforcement agencies.



The generally hostile tone and harsh criticism some have directed at tech companies, overlooks the critical role they play in existing law enforcement efforts. As the main mandated reporters in the digital space, tech companies provide the only consistently reliable reporting of CSAM (Child Sexual Abuse Material) and other forms of child exploitation.

Yet some bills pending in Congress would expose these companies to liability when they report instances of CSAM and/or other forms of abuse on their various platforms.

When CSAM was conveyed through the mail, no one suggested suing the Postal Service. They hired more postal inspectors. Exposing tech reporters to this kind of liability would create an irreconcilable conflict of interest that would only serve to limit law enforcement's access to information and further compromise already limited arrest and conviction rates. We desperately need to expand and fund law enforcement to investigate, prosecute, and garner convictions for these crimes. This is how we create a real deterrent to child exploitation.

While some in Congress want to vilify tech companies, they are not the ones victimizing children: the predators are. Unfortunately, most policy responses to this problem lay blame on the tech companies and their platforms while completely ignoring the actual bad actors and the need to arm law enforcement with the funding and tools they need to mount a meaningful response. Furthermore, by placing perceived civil justice ahead of criminal justice, child predators know they can operate with almost complete impunity.

**We must anchor any attempt to protect children in a serious and concerted effort to take down predators wherever they are, online or off. We must disrupt both organized and freelance criminal activity and create real deterrence to these crimes. Furthermore, any policy development in this area should recognize and address the very real connection between online exploitation of children and real-world problems that feed into digital victimization.**





# GOOD BILLS VS. BAD BILLS

Many vehicles have been introduced in Congress by well-intended members seeking to mitigate online child exploitation. Some of these bills are duplicative. Others present serious and unavoidable constitutional concerns that do not provide adequate, enforceable protection for children. Most do not provide the funding needed to have a real impact on outcomes. All but one fail to address the most pressing element in any successful child protection exercise, strong financial and political support for the role law enforcement must play if we are going to protect children in any meaningful way and prevent abuse in the future.

For the purposes of this discussion, we will highlight two bills in Congress that represent two ends of the policy making spectrum when it comes to efficacy vs. inadequacy.

No two pieces of legislation highlight the disconnect and disparities of policy making in this arena more effectively than the Invest in Child Safety Act (INVEST) versus the EARN IT Act. INVEST (sponsored by Sens. Wyden (D-OR), Gillibrand (D-NY), Brown (D-OH) and Hirono (D-HI) and Reps. Eshoo (D-CA), Fitzpatrick (R-PA), Bacon (R-NE) in the House) and EARN IT (sponsored in the Senate by Sens. Blumenthal (D-CT) and Graham (R-SC) and in the House by Reps. Garcia (D-TX) and Wagner (R-MO)) make very different proposals for addressing this serious issue.

## THE INVEST IN CHILD SAFETY ACT (INVEST)

INVEST seeks to provide federal, state, and local agencies with the resources to combat the root causes of CSAM proliferation by directing \$5 billion in mandatory funding for investigations, prevention, and support for CSAM victims. The bill would be fully paid for by extending customs user fees.

It would quadruple the number of prosecutors and agents in DOJ's Child Exploitation and Obscenity Unit, add 90 new full-time investigators in DOJ and 100 new FBI task force investigators, and provide funding to NCMEC to hire 65 additional analysts and to make major system upgrades. It will also double the funding for state Internet Crimes Against Children task forces and require tech companies to increase the time they hold evidence of CSAM in a secure database, to enable law enforcement to prosecute older cases.

## THE EARN IT ACT

In sharp contrast to INVEST's aggressive efforts to right-size law enforcement funding, EARN IT includes no funding for federal or local law enforcement. Simply put, EARN IT aims to curb the proliferation of CSAM images online by amending existing laws to increase liability for websites and online platforms that host user-generated content. It simply creates a federal commission to develop voluntary best practices for websites and platforms to implement to aid in preventing and reducing CSAM. This element is completely inadequate for effectively fighting predators. It is also duplicative in view of pre-existing efforts by groups like We Protect and others. The bill also conspicuously fails to provide any direct funding for state or federal agencies for prevention or treatment.

PROPOSAL	PURPOSE	PROVISIONS
INVEST IN CHILD SAFETY ACT (INVEST)	to provide federal, state, and local agencies with the resources to combat the root causes of CSAM proliferation	<ul style="list-style-type: none"> <li>• \$5 billion in mandatory funding for investigations, prevention, &amp; victim support.</li> <li>• 4x increase in prosecutors &amp; agents in DOJ's Child Exploitation and Obscenity Unit.</li> <li>• 90 new full-time investigators in DOJ &amp; 100 new FBI task force investigators.</li> <li>• NCMEC funding 65 additional analysts &amp; needed system upgrades.</li> <li>• 2x funding for state Internet Crimes Against Children task forces.</li> </ul>
EARN IT ACT	To create a federal commission to develop voluntary best practices for websites and platforms to implement to aid in preventing and reducing CSAM and to make technology companies liable for reporting.	<ul style="list-style-type: none"> <li>• No funding for federal or local law enforcement.</li> <li>• No direct funding for state or federal agencies for prevention or treatment</li> </ul>

In a simplistic and some would say naïve effort to ensure “penalties” for tech companies, EARN IT seeks to pierce the veil of tech’s long-standing exemption from civil liability because of [Sec. 230 of the Communications Decency Act](#). Based on the rhetoric around EARN IT, the average person would think that there is no law enforcement recourse to hold platforms that engage in bad acts accountable. However, what virtually everyone overlooks is that tech companies are liable under federal criminal law if they engage in illegal activity. So, in what can only be described as a dual lack of insight, concerned onlookers attempting to mitigate sexual exploitation online neatly overlook both criminal justice for perpetrators as well as criminal penalties for technology platforms that fail to aggressively protect children, or even conspire with predatory content providers.

**Beyond that glaring omission when it comes to accountability, anyone who has taken a cursory glance at [arrest and conviction rates](#) of child predators is aware that they fall far behind the escalation of these activities.**

This is a serious problem. Anyone who ignores the importance of bolstering law enforcement capabilities before all else is jeopardizing the safety of children. No platform, no community, no family, no child will be safe if we allow offenders from multi-national criminal enterprises or individuals downloading CSAM in their basements to continue their activities without aggressive law enforcement intervention and effective prosecution.

Any suggestion that tech companies should be subjected to greater liability ignores one of the most salient and powerful facts about the current cybertips program. Tech companies [provide](#) the vast majority of reports that are currently referred to NCMEC’s cybertips system. In 2022, 99% of cybertips were reported to NCMEC by electronic service providers (ESPs.) In fact, since the enactment of [18 USC 2258A](#), technology platforms are

[bound](#) by the same federally-mandated reporting rules that have been the bedrock of child abuse prevention since the 1970’s.

EARN IT would create a glaring conflict of interest for tech companies. Indeed, most mandated reporters in other fields are explicitly shielded from liability to encourage, not dissuade, timely and accurate reporting of potential child exploitation to law enforcement. Creating significant liability for the only reliable reporting system that exists today will only serve to exacerbate the problems we are seeking to address and divert attention even further away from actual perpetrators. It also ignores the fact that the federal criminal justice system is readily available to hold any platform accountable that flouts the law.

At the same time EARN IT seeks to compromise the only reliable CSAM reporting system in use today, it also encourages trading one form of child exploitation for another. Encryption has become the backbone of consumer protection in this country for everyone. Weakening encryption is a recipe for disaster, not just for every American consumer, but for the millions of children who have “clean” credit records, that typically aren’t examined until they are adults, who are the most attractive victims for identity thieves.

**Nearly a million children a year are victims of identity theft, and that number is growing.**

**Thus, EARN IT not only fails to prevent child exploitation, but it also compromises the the most reliable and effective reporting system we have and removes what protections exist**

to limit one of the most pernicious forms of child exploitation today: identity theft. We believe that any proposal that compromises the only reliable reporting system we have by putting civil liability ahead of criminal justice will only exacerbate an already severe problem that is spiraling out of control.

# ENFORCE EXISTING LAWS



Passing bills into law without implementing them effectively is pointless.

Perhaps one of the best examples of this disconnect is the Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act (PROTECT Our Children Act of 2008).

Initially sponsored by then-Senator and Chairman of the Senate Judiciary Subcommittee on Crime and Drugs, Joseph R. Biden (D-DE), the [PROTECT Our Children Act](#) was passed to address the rapid proliferation of online CSAM. The law laid the groundwork for a coordinated cross-sectoral response focused on prevention, interdiction, and community outreach and education. The law mandated that a senior official at the Department of Justice, designated by the Attorney General, develop, implement, and provide biennial updates to a 19-pronged National Strategy for Child Exploitation Prevention and Interdiction (National Strategy).

The Act also provided funding to local law enforcement through the ICAC (Internet Crimes Against Children) network. Founded in 1998 under the Department of Justice Office of Juvenile Justice and Delinquency, the ICAC network includes 61 task forces comprised of 5,230 federal, state, and local law enforcement, and

prosecutorial agencies throughout the country.

We know that ICACs work. In headline after headline from around the country, ICAC teams put the evidence together to take down predators, whether in large, organized syndicates or individual perpetrators.

## **Tennessee:**

[“ICAC investigation leads to federal jury conviction for child exploitation offender”](#)

## **Idaho:**

[“Caldwell Man Sentenced to Over 11 Years in Federal Prison for Possession of Child Pornography”](#)

## **California:**

[“LAPD:139 arrests made in operation targeting online crimes against children”](#)

We also know that much more needs to be done to keep pace with recruitment and training of professionals and the growing numbers of reports of exploitation and abuse.



Unfortunately, by December of 2022, this is what a report from the Government Accountability Office (GAO) had to say about PROTECT's implementation:

"In the past 14 years, 9 detailees have rotated through the national coordinator position. DOJ has only issued a strategy twice, hasn't fully included 12 of 19 elements, and hasn't updated it since 2016 to address advances in technology."

The DOJ had fallen into noncompliance and officials have attributed these delays to several factors - including staffing and resource constraints, while reports to the CyberTipline skyrocketed. In 2022, the CyberTipline received 32,059,029 reports regarding 88,377,207 digital files. For perspective, that's more than [one report per second](#) - each containing several images, videos, or other media. In a June 2023 [report](#) to Congress, the DOJ described the increasing disparity between cybertips and funding as a "crisis."

**In addition, only a small percent of these reports are ever investigated,** again largely due to a lack of human and financial resources. In a recent 90-day period, there were 99,172 IP addresses throughout the US distributing known CSAM images and videos through peer-to-peer networks.

Law enforcement only had the capacity to [investigate](#) 782, less than 1%, even though 75% of similar cases result in "successful prosecutions."

All internet activity is de facto "interstate commerce," and thus, per the Constitution, requires a federal response that leverages state activity when it comes to combating crimes. Indeed, these are often global activities that require a well-organized,

well trained, well-funded law enforcement response. The PROTECT Act provided a framework in which states and other hyperlocal jurisdictions could create a cohesive approach to preventing online crimes against children – complementing the efforts of law enforcement.

**LESS  
THAN 1%**

The amount of CSAM reports from the CyberTipline that law enforcement had capacity to investigate.

PROTECT was promoted with a lot of lofty, bipartisan rhetoric. Unfortunately, a bill that could have been providing serious protection to children over the last 15 years - a vehicle that might have prevented the victimization of millions of kids – has, for the most part, languished without effective or consistent implementation.

PROTECT is just one example of Congressional discourse that has failed to result in actual safety for children. In the 15 years since PROTECT was passed, the problems have escalated dramatically - creating an even greater gap between law enforcement capacity and increased criminal activity. Fortunately for children, INVEST provides robust support for PROTECT's original goals, and the funding to ensure that both the spirit and the letter of the bill(s) are realized.

An investigative report by the New York Times in 2019 revealed that reports of images of child sexual abuse have skyrocketed, from 3,000 reports in 1998 to over 18.4 million in 2018. Federal, state, and local enforcement agencies have been inundated with more

requests than they can possibly investigate resulting in the lack of the necessary investigations that would lead to the prosecution and conviction of the perpetrators.

**Despite this crisis, the Department of Justice has largely failed to implement the 2008 law. As of 2019, it has produced only two of the six mandatory reports and consistently sends only half of the \$60 million that was authorized for state and local law enforcement each year.**

High levels of appointee and staff turnover have further hindered progress.

# WHAT DOES IT MEAN TO “PROTECT” CHILDREN?

While many in Congress are enthusiastically focused on protecting children “online” they seem less concerned about the circumstances of children in real life. Of the 32 million reports to the CyberTipline in 2022, 89.9% were attributed to locations outside the U.S. The recent GAO report on the PROTECT Act points out:

Livestreaming is on the rise, enabled by the connectivity and availability of inexpensive streaming devices. Available data indicates that the individuals who “consume” livestreamed abuse are predominantly from Europe, North American and Australia according to a 2021 WeProtect Global Alliance. The majority of identified livestreaming victims live in SouthEast Asia, in particular the Philippines according to the same threat assessment.

To put it bluntly, a handful of plaintiffs’ attorneys in places like New York and Washington, DC are hardly going to solve this problem. Victims in developing countries would have an exceedingly difficult time accessing legal services much less establishing jurisdiction and pursuing civil claims, especially without criminal convictions. In short, policy recommendations like the EARN IT Act fail completely to address the complex, global nature of this problem, whether interdicting the activity or supporting victims, many of whom reside outside the US.

To be clear, civil justice for victims is extremely important. Currently, victims are free to sue their abusers in civil court. In 2006, Masha’s Law, a bill designed to increase civil penalties for child pornography was passed providing more equitable civil justice for victims of abuse and trauma. At the time the civil penalty to download a song was three times the civil penalty to download CSAM. Masha’s Law closed that loophole, making the penalties equal. The bill achieved final passage in seven months and was signed into law by President Bush as a part of the

Adam Walsh Child Protection and Safety Act of 2006.

A successful criminal prosecution can greatly bolster any civil claim a victim may have against an abuser. A negative outcome for a perpetrator in a criminal trial lays the strongest possible foundation for a victim to prevail in civil court.

**Thus, the overall trend of focusing on civil justice while effectively ignoring criminal justice potentially robs victims of a positive result in any civil claim.**

Nevertheless, we cannot simply emphasize civil justice at the expense of successful criminal prosecutions. To do so would simply ensure that unlimited generations of new child victims would be targeted perpetuating a cycle that is already spiraling out of control. Also, current efforts to establish greater liability for organizations most responsible for identifying who and where perpetrators may be seems not just shortsighted but entirely counterproductive by robbing victims of important information needed for them to access both criminal and civil justice.

# The Problem

with current U.S. child protection laws

- The lack of enforcement of existing laws;
- Relying on the wrong agency to assess the efficacy of prevention and response practices; and
- A lack of focus on preventing abuse, neglect, and exploitation





Bills like these do nothing to prevent the abuse, neglect, and exploitation of children. Rather, they simply attempt to “respond” after the fact. Furthermore, again, like far too many other child welfare and protection laws, they misidentify who should be responsible for ensuring compliance with existing laws.

The problem is not the lack of child protection laws, but : (1) the lack of enforcement, (2) relying on the wrong agency to assess the efficacy of prevention and response practices, and (3) the lack of focus on preventing abuse, neglect, and exploitation. The addition of new laws, protocols, and/or policies to protect children does nothing if we do not adequately address these.

We know, firsthand, from decades of disastrous child protection practice that relying on Child Protection Services to self-report on everything from how many children died in their care, to how many foster children go missing, that these agencies are not forthcoming about their shortcomings. Reporting requirements are haphazardly enforced and the consequences for missing, incomplete, or inaccurate data about the welfare of children in state or county care are minimal, if non-existent.

In this case, the continuous expectation from Congress that technology companies rather than law enforcement take the lead on the issue of monitoring illegal activity online places an undue burden on the private sector. Simultaneously, it does not help law enforcement identify, or courts punish, predators. As a result, we’re seeing far too many predators being released onto the streets, putting more children at risk.

Nothing is more important than ensuring predators face justice. It is certainly not pushing the private sector to create a huge surveillance apparatus, which creates numerous privacy complications.

### **Law enforcement in the digital world should be carried out by law enforcement agencies, not private businesses.**

Shifting the policing of technology companies to law enforcement eliminates the view that companies are “not doing enough.” Clearly, several leaders in the tech industry have moved aggressively toward compliance with federal reporting laws. However, for companies that do not work with law enforcement to combat crimes against children, the prospect of serious criminal prosecution rather than an annoying civil suit would provide a far more effective incentive to engage more fully in prevention.

While it may be satisfying for policymakers to create new laws to “protect” children, if they are the wrong laws, or do nothing to protect the actual safety of children, they are pointless. More concerning is that if a misguided or ineffectual bill passes, policy makers will simply check the box on that topic and move on. Typically, it is decades before a critical issue like this is revisited. So having created the appearance of “addressing” the issue, the “solution” is only an illusion and often one that is dangerous for children.

We must focus on the safety and well-being of the children before they are victimized, and to do so, must engage with a myriad of agencies and organizations in drafting the appropriate language to ensure effective implementation of any initiative. Law enforcement at all levels is a critical partner in both the prevention of, and response to, the abuse, neglect, and exploitation of children. Those responsible for enforcement and compliance must be an independent entity that neither benefits from, nor is harmed by, complying with, or ignoring the law or policy.

**In this case, we believe law enforcement agencies are the appropriate entities to investigate crimes and arrest and prosecute the criminals who commit them.**

# THE GOVERNMENT MAKES A LOUSY PARENT



One of the ironies of the child protection debate is how readily elected officials from both sides of the aisle are turning to the government to dictate policy around children and access to the Internet. One example of this disconnect is the Kids Online Safety Act (KOSA.) While on the surface KOSA seems well intended, the bill represents the worst kind of box checking when it comes to public policy. One could readily see an already overburdened and conflicted Congress passing a bill with a deceptively attractive title and then consider a serious issue “addressed” for what could be a generation.

Though superficially focused on “online safety,” KOSA clearly opens the door to intrusive government intervention into what should be family decisions. Worse yet, the legislation delegates enforcement to individuals state Attorneys General in a framework that has already proven to be erratic and inconsistent when it comes to child welfare in America.

One cannot underestimate the important role parents play in protecting their children. In fact, in child welfare practice, if a child is exposed to a dangerous environment or addictive substance parents/guardians are held responsible for compromising the child’s well-being. As we have seen in decades of abuses because of government overreach in child protection we are on a slippery slope when we ascribe to the government

responsibilities better carried out by parents.

If we allow the government to determine at what age our children engage in certain activities online, what’s next? The government can tell you how much television your children can watch, how often you can take your children to church, etc. It is not an overstatement to say that the same draconian and often extremely damaging government interventions we have seen abrogate the rights of parents in real life could become routine in online “child welfare” policy.

**Bills like KOSA create a slippery slope into intrusive policy making in digital child welfare yet fail to provide any meaningful protection for children.**

Historically speaking, the government has not been the best “caretaker” of children. Often, ineffectual, or even abusive, child welfare policies have extended to draconian and often dangerous undermining of parental rights. We have no farther to look than the American child welfare system to see every possible reason to leave many of these decisions to parents.

**There are roughly 500,000 children in the highly regulated US foster care system who are here to tell you that the government makes a lousy parent.**

Every year, more than 20,000 children “age out” of the system overwhelming to lives of homelessness, unemployment, mental health issues and an array of consequences of living in a system that has for the most part neglected them in virtually every possible way. Most have not graduated from high school. Few will attend college, and many have chronic, persistent medical issues fueled by years of health care neglect. All these young people are at the highest possible risk for exploitation and trafficking.

**Historically speaking, the government has not been the best “caretaker” of children.**

In fact, multiple studies have demonstrated a clear link between youth who are victims of sex trafficking (in all its forms, not just online) in the United States, and who also have a history of child welfare involvement. For example, in 2015, Los Angeles County [found](#) that 85% of identified survivors of child sex trafficking had prior child welfare involvement. In a 2018 Field Center [publication](#), nearly 300 youth were interviewed in a multi-city study and found that 41 percent of those who were sex trafficked had at least one out of home placement in their lives, and 63 percent reported involvement with the child welfare system.

As some in Congress have turned up the volume on tech companies when it comes to protecting kids, they have been less than enthusiastic when it comes to holding their state Governors accountable for the woeful condition of child welfare in America. Children are abused, neglected, lost, and even killed while in the care of the state every day. According to [NCMEC](#), in 2020, 19% of the children who ran from the care of social services and were reported missing to them were likely victims of child sex trafficking. Yet to the extent there is any outrage, it is muted.

**85 %**

of survivors of child sex trafficking in LA County were previously in the child welfare system

**41 %**

of those who were sex trafficked had at least one out of home placement in their lives

**63 %**

of child sex trafficking victims were previously in the child welfare system

The child welfare and other child and family serving systems are no doubt responsible to set up and oversee policies and practices that address the risk factors that put children and young adults at risk for trafficking, with a goal to prevent maltreatment and child welfare involvement at all. This paper does not diminish any of these responsibilities. But they, too, require a robust law enforcement partnership to be successful.

In a 2022 Information Memorandum (IM) as to requirements under the Preventing Sex Trafficking and Strengthening Families Act of 2014, the Administration for Children and Families provided guidance to states and jurisdictions. The IM and related reports and resources define extensive expectations for the child welfare system to develop policies and report suspected trafficking (in addition to requirements to report missing children).

Law enforcement is identified as a critical partner, but sustainability plans are not clearly funded. In fact, a May 2022 Inspector General report from the US Department of Health & Human Services, highlights this problem. State agencies reported that obtaining assistance from law enforcement was one of the most frequent challenges regarding missing children.

**Legislation such as the INVEST Act would not only bolster the implementation of existing laws like the PROTECT Act, but it would also provide additional resources to justice and law enforcement agencies to ensure more seamless integration for child welfare agencies to succeed in their efforts to protect children who are being trafficked or at risk of trafficking.**



The  
Danger

OF FAILING TO  
CONNECT THE  
POLICY DOTS



## What happens when well-intended elected officials fail to connect the dots between issues, they say they care about?

One has only to look at Congressional pressure to force the US Department of State to lower standards when it comes to international adoption and orphan hosting programs to see a perfect storm when it comes to encouraging exploitation.

When Haiti was hit with an earthquake in 2010, thousands of children were displaced. However, most of them had families who were actively searching for them. Nevertheless, children were removed without any authority and orphanages were emptied even though they had not been damaged by the quake. [Demands](#) came from all quarters for the State Department to expedite visas, even for children who had no proof of identity. In one notorious case, Ed Rendell, then Governor of Pennsylvania, engineered a “rescue mission” of 54 children who were airlifted from Haiti to the US. Unfortunately, 12 of the children were not orphans and were not in the adoption pipeline.

Days after the war in Ukraine began, the State Department was [bombarded](#) by demands to bring Ukrainian children to the US, demands that continue 18 months later. Few of the children displaced by the war in Ukraine are orphans. In fact, just as in Haiti, most have families actively looking for them. Worse yet, the Russian government has abducted tens of thousands of children to be placed in illegal adoptions, re-education camps and other unknown locations. The Ukrainian government has been extremely clear that adoption is not an option and that hosting programs (that are often used to shoehorn into adoptions) are not acceptable. They are determined to ensure that all the children displaced by the war are reunited with their families.

The Ukrainians recognize the real and pressing danger of child trafficking and exploitation of their children. But many members of Congress continue to demand that children who may, or may not, be orphans

be released to individuals who have not had a home study or any other assessment of their suitability to adopt. As we have learned from Haiti, and other countries, these children are increasingly exploited or abused.

Additionally, the number of international adoptees who are abandoned by their custodians in a practice known as “rehoming” where the children are effectively traded, often on the internet, to total strangers continues to increase. Where are the members of Congress pressing for “internet safety” for these children? The answer is often that they are nowhere to be found.

**Whether holding the US child welfare system accountable for its failures or synchronizing adoption policy with responsible child protection rules, any member of Congress seeking to protect children should ensure well informed, consistent policy development that encompasses both digital and real-world concerns and solutions.**

Members should look beyond the restrictions of the committee system to see how recommendations can be implemented more seamlessly across those jurisdictional boundaries. Since the days of the Orphan Trains in the 1850s, child welfare in America has been viewed as a state law issue. But even then, these were fundamentally interstate and now intercountry activities that require a more sophisticated, thoughtful, and inclusive approach to avoid unintended consequences and dangerous loopholes for children.

# CONCLUSION

There has been a lot of criticism of tech companies during the debate about child exploitation. However, there has not been nearly enough discussion about how to prevent abuse or how to stop the cycle of exploitation. Tech companies have been the main – indeed the majority – of reporters of online child exploitation and abuse. The number of cybertips reported to NCMEC has exploded in the past ten years. But arrest rates have failed to keep pace and increasingly the courts are failing to ensure meaningful sentences when convictions are secured. These issues are complicated, but as the DOJ lays out in their recent report to Congress many of them have to do with inadequate funding, with administrative inefficiency and a lack of coordinated and consistent oversight.

As we have seen with mandated reporting in child welfare, many allegations do not translate to substantiation. Failure to triage reports often leads to inordinate focus on trivial, false, or misreported accusations while serious concerns are ignored. In DOJ's own words, the CyberTipline is "overwhelmed" and is a "system in crisis." It seems advisable to begin any serious effort to understand what is really going on with a hard look at what those millions of reports represent.

**Ultimately, child protection in America is in crisis in virtually every sector, whether in the digital or physical world. This is not a problem that can be solved simply by blaming technology. We are all to blame. The solutions will not be achieved by looking for the deepest pockets. They will only come when we take a hard look at the big picture, factor in the impact the internet has had on every aspect of child welfare and child protection and make a meaningful investment in rightsizing the infrastructure – from law enforcement to the courts to victims' services – that finally addresses this scourge effectively.**

Until now, Congress and supporters of bills like EARN IT have almost completely ignored the critical role law enforcement must play in attacking this issue. Some members of Congress have advanced a narrative about defunding the FBI, a gift to child predators around the globe.

Whether arresting and convicting criminals preying on children or criminally prosecuting companies that conspire with them to platform their exploitation, nothing will change.

**Until we get serious about advancing real solutions, this catastrophe will continue to metastasize.**

The answer lies in every law enforcement agency in America from the FBI to your local sheriffs' offices. Those efforts are most effectively seeded by the critical information provided by technology companies working to keep up with criminal activity almost untouched by any serious effort in public policy to address it.

Any suggestion that we can effectively address an epidemic of child exploitation that continues to spread, whether online or in real life, without a significant, long term, bipartisan commitment to criminal justice is just magical thinking. Simply counting cybertips without taking predators off the street will only encourage more, not less, abuse.

**We must demand that our public officials act, and act now. From the White House to Congress, to state and local governments, law enforcement funding and accountability in the form of arrests and successful convictions are the only metric that will, in the long, run change the culture of this problem and protect children.**

## **ABOUT THE AUTHORS**

**Maureen Flatley** is an expert in government reform and oversight involving children. She has spent decades advocating in the US and abroad for children who are victims of abuse, neglect, and exploitation on and offline. She has been an architect of a range of bills in Congress that dramatically reformed systems that serve children. In 2006 in the interests of amplifying civil justice for victims of online exploitation she was instrumental in the creation and passage of Masha's Law, a bill that tripled the civil penalty for downloading CSAM. She continues to work to ensure effective, consistent, actionable policy development to protect children wherever they are.

**Agatha A. Tomasik, CFRE**, serves as the Executive Director of Stop Child Predators. She has more than 20 years of experience in advocacy for children and victims of crime, work with the criminal justice system, and nonprofit management. She has presented at conferences on public policy, nonprofit advancement, and victimology. A graduate of American University's School of Public Affairs and a certified domestic violence advocate, Agatha resides in Washington, DC.

**Susan Grundberg, MSSW, MPA**, has spent more than 30 years in human services and has successfully conceived of and implemented system and organizational reforms in both nonprofit and government leadership capacities, including four years as Associate Commissioner for Child Welfare Programs with NYC's Administration for Children's Services. Susan now serves as an advocacy, implementation, and capacity building consultant, partnering with organizations and jurisdictions working to design and implement innovative solutions to the most complex challenges.

**Ambassador Susan S. Jacobs (Retired)** was appointed the first Special Advisor for Children's Issues at the Department of State by Secy. Hilary Clinton, a position in which she served from 2010 until her retirement in 2017. During her tenure, she traveled to more than 40 countries to discuss and implement effective child protection policy. In addition, she led U.S. delegations to international conferences and commissions concerned with issues affecting children. Throughout her career, she held various overseas postings including Israel, India, and El Salvador. Prior to her appointment as Special Advisor, Ambassador Jacobs served as the Deputy Assistant Secretary in the Bureau of Legislative Affairs and as Ambassador to Papua New Guinea, the Solomon Islands and Vanuatu. As the chair of the International Social Service governing board, she continues to dedicate her life to improving the condition of children around the world.

**Felicity Sackville Northcott, PhD**, has more than 20 years of experience working on a range of issues related to child welfare, child protection, and the nexus of international law and social work. Dr. Northcott has trained hundreds of judges, lawyers, social workers, and other stakeholders on their responsibilities under various international conventions related to cross border child protection. Most recently she served as the Director of Global Missing Children's Issues at ICMEC.



# **ABOUT STOP CHILD PREDATORS**

A national nonprofit focused on child advocacy, Stop Child Predators (SCP) was founded in 2005 after the kidnapping of nine-year old Jessica Lunsford. She was abducted, raped, and murdered by a twice-convicted sex offender. At that time, the average child molester spent only three years of a seven-year sentence in prison before being released back into society. In response to this heinous crime, SCP crafted The Sexual Offenses Against Children Act – or Jessica’s Law – which mandates a minimum 25-year prison sentence and lifetime electronic monitoring for adults convicted of lewd and lascivious act against children under the age of 12. Since then, the landscape for exploitation has shifted from in person to online, SCP has continued to convene policymakers, advocates, and law enforcement to develop effective, actionable strategies to protect children.



Stop Child Predators  
5185 MacArthur Boulevard NW, Suite 575  
Washington, DC 20016

@StopPredators  
[stop-child-predators.org](http://stop-child-predators.org)