CONNECTICUT VOICES FOR CHILDREN

JANUARY 2025

BEYOND THE ALGORITHM

AI GOVERNANCE FOR BUILDING SAFE DIGITAL FUTURES

Carmen N. Clarkin, M.P.H. Research & Policy Associate, Connecticut Voices for Children
Emily Knox, Ph.D. Research & Policy Director, Connecticut Voices for Children

GLOSSARY

Algorithm - A structured sequence of instructions enabling machines to process data, identify patterns, and make decisions autonomously.

Algorithmic Bias - Systematic errors in AI outputs caused by imbalanced training data or flawed system design. These biases can perpetuate discrimination and inequality.

Artificial Intelligence (AI) - A machine-based system that can, for a given set of human- defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

Microtargeting - A strategy that uses detailed personal data to deliver highly tailored content or advertisements to specific individuals or small groups, often through automated systems that predict user behavior. While effective for personalization, it has raised concerns about discrimination, privacy violations, and the amplification of harmful or misleading content.

Children's Online Privacy Protection Act (COPPA) - A U.S. law protecting the online privacy of children under 13 by regulating data collection and requiring parental consent.

Deepfake - AI-generated media that manipulates existing images, videos, or audio to create realistic but fabricated content. Deepfakes pose many risks including, but not limited to: the spread of misinformation, cyberbullying, identity theft, privacy breaches, fraud, and the creation of non-consensual explicit material.

Deceptive Design - User interface techniques that manipulate individuals into making unintended or less favorable choices. Such designs exploit cognitive biases, especially among children.

Digital Footprint - The data trail left behind from online activities, including browsing, social media interactions, app usage and more. A digital footprint can have lasting privacy implications.

Social Media - Online platforms that enable users to create and share content while interacting with others. Social media collects vast amounts of user data, often influencing opinions and behaviors via algorithms.

Surveillance Culture - A societal environment where individuals are constantly monitored through technologies, raising ethical and privacy concerns.

PAPER OVERVIEW

Artificial Intelligence (AI) is a rapidly advancing technology capable of processing massive amounts of data, opening up a world of new opportunities and risks for children in today's digital world. AI's integration into everyday life has quickly made it an essential part of various industries, including healthcare, education, finance, and housing. This integration poses unique challenges that require legislative and regulatory attention, to protect users, particularly children. Though AI holds immense promise, if left unregulated, exploitation of its processing power can harm children's well-being both in the present and future. Practices, such as predatory marketing, biased microtargeting and over surveillance, leave children at risk of long-term adverse outcomes, including privacy violations and limited or inequitable access to opportunities. Addressing these issues will require a concerted effort from policymakers, technology companies, educators and other stakeholders to ensure that AI is used responsibly and beneficially for all children.

INTRODUCTION

In this rapidly evolving digital age, Artificial Intelligence (AI) has emerged as a new frontier not only for innovation, but also for advocacy. While much of the discourse focuses on its benefits, technological advancements, and ethical concerns, discussions about AI's long-term impacts on children's safety and opportunities are often overlooked. Current conversations tend to emphasize AI's role in academics or algorithmic influence through social media, but fail to address the long term impacts of AI on a young person's safety and future opportunities.

In an era defined by digital interactions, where children are on the internet from increasingly early ages, personal information is constantly being collected and processed, often without users' full knowledge. Due to the rapid evolution of the technology, AI models have the ability to process large amounts of data faster than traditional methods. AI's ability to process and analyze massive datasets at unprecedented speeds raises pressing concerns, especially for children who are the first generation with such extensive digital footprints to come of age in a time when their digital information can be readily accessed and exploited using AI powered technology. This data can influence life-altering decisions in areas like college admissions, credit score, housing loans and more.

As AI continues to become a larger part of everyday life, there is a critical need for an equity-based framework to guide its use. Clear standards and safeguards are needed to protect users, particularly children, who are more vulnerable to deceptive design practices and the long-term consequences of their digital activity.

This report addresses some of the unique risks that AI, if left unregulated, poses to children and proposes policy recommendations that prioritize actionable protections around algorithmic transparency, accountability, and accessibility in order to ensure safety and equity in today's technology dominated landscape.

Public interest in AI has surged as the technology has evolved, becoming both more complex and accessible. Defined broadly, AI is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.[1] While many are familiar with tools like predictive AI (e.g. spell check) or generative AI (e.g. ChatGPT, Microsoft Copilot etc.), AI encompasses far more. Today, different kinds of AI are used to do everything from predicting patient outcomes in medical settings to screening applications for jobs, housing, and loans.[2,3] It can generate schedules and outlines, create realistic media and provide customer service. Not only are AI tools used by large companies and easily accessible to the public via specific websites, but many forms of AI have also been incorporated into online platforms, social media apps, operating systems and web browsers. As such, AI has become ubiquitous, it is a tool that most people interact with daily, often without even realizing it.

As AI rapidly evolves, protecting users and promoting equity requires regulatory safeguards against both malicious actors and the biases embedded within AI itself.

Bias embedded in AI systems can exacerbate inequalities in critical areas like healthcare, education, finance, housing, and employment. In addition to basic equity concerns around how AI is still capturing, recreating, and amplifying the bias of past human decisions, there are also significant data privacy concerns around what information is being used to train AI models. The algorithms that dictate what an AI system does are designed by humans and trained on existing data.[4] Some AI systems collect data through both passive and active user input, including interactions with minors who may not fully understand that their data is being collected in exchange for use of a platform.

Thoughtful regulatory action is essential to mitigate AI's risk, from embedded bias to privacy concerns. Opponents of regulation argue that it could stifle innovation. However, history shows that robust regulation can coexist with technological progress. Like AI, automobiles were once an innovative and transformative new technology that, over time, required protective measures to ensure public safety. Just as seat belts and speed limits facilitated safe adoption of cars, AI regulations can balance innovation with accountability, shaping a framework that evolves alongside this powerful technology, addressing both its adaptive nature while simultaneously confronting its potential for harm.

Despite AI's rapid growth, U.S. regulations remain insufficient to address its unique challenges. Over 30 states, including Connecticut, have passed or proposed laws that attempt to address growing concerns around this new technology, but are often narrow in scope and inadequate for the technology's complexity.[5] The existing legal guidance at the federal level either consists of voluntary guidelines rather than enforceable laws or is an addendum to existing regulations in issue areas that are not adequately equipped to handle the inherently complex and rapidly advancing nature of AI.[6,7] This lack of comprehensive oversight exposes individuals, particularly children, to new forms of exploitation and harm.

Research shows that the groups who already face systematic disadvantage– defined by factors such as race, gender, ability, sexual orientation and socioeconomic status– are disproportionately affected by AI's negative impacts.[8]

The disparate burden of these consequences among specific populations is especially clear when examining the impact and implications of AI on children. Looking both domestically and at the European Union, there are numerous guidelines and strategies that can be used to help mitigate AI's risks both now and in the future.

LITERATURE REVIEW

The increasing prominence of AI in public discourse has led to widespread awareness of its potential benefits and risks. As AI becomes more integrated into daily life, concerns about digital safety have intensified. Addressing the specific privacy risks posed by AI is essential, especially for children and youth who are more vulnerable to manipulative data processing techniques. Key issues include the formation of digital footprints, the storage of behavioral and learning data, and the role of surveillance and microtargeting, all of which are shaping children's futures.

Definition & Complexity of a Child's Digital Footprint

As individuals interact with the digital world, they develop what is known as a digital footprint, a mosaic of data that when examined in aggregate, creates a strikingly clear portrait of a user.

Digital footprints are composed of information that an individual leaves behind across different platforms and services, from likes and searches to credit card information and shopping habits.[9] As the internet has evolved, digital footprints have become more complex. The data that makes up an individual's digital footprint is no longer limited to IP addresses and browsing history—it contains an expansive array of personal, professional and financial information collected both actively and passively, through interactions with apps, online platforms, smart devices and more.[10] While certain data tracking disclosures are required by law, personal information that makes up an individual's data footprint is often accumulated covertly and without a true choice to opt out. Today, with increased surveillance culture and private recording devices like cell phones and Ring cameras, it is difficult not to amass a significant digital presence that contributes to the growth of a digital footprint even if one is not actively online.

For children, digital footprints both shape and are shaped by how they play, socialize and learn, and are especially extensive because of their early and frequent online interactions.[11] A majority of children, regardless of socioeconomic background, will have access to a device that allows them to connect to the internet and interact with AI.[12] Even prior to being online, many children have access to toys, games and apps on smartphones or tablets that collect information on their usage and behavior, while also utilizing algorithms and AI to do everything from targeted advertising to predicting what content should be presented next. In this way, digital footprints grow continuously, creating detailed profiles that can be accessed by or sold to third parties.

Before a child is even born, their digital footprint can begin to form through shared pregnancy announcements and sonograms.[13] As babies, smart devices contribute to creating lasting digital records of children's addresses, parents' income, biometric data and other potentially sensitive information.[14] Smart cribs and other high tech baby gadgets like the Owlet smart sock[15] and video enabled baby monitors that connect to an app on parent's phones can also contribute to the growth of a child's digital footprint.[16]

In 2017, privacy concerns around children's data led to the cancellation of Mattel's "Aristotle," an AI-powered device marketed as both a virtual assistant and educational tool. The device combined

the capabilities of a smart speaker with a camera enabled baby monitor. It was marketed as being able to interact with and soothe a crying infant in addition to being an educational toy meant to grow with a child, even providing language lessons for older children.[17] A major point of concern, as highlighted in a letter from U.S. Senator Edward Markey (Democrat) and U.S. Representative Joe Barton (Republican) was the device's ability to create an "in-depth profile of children and their family"[18] and the idea that children would be forming bonds with data-collecting devices. However, even though Aristotle never made it to the shelves, other devices and toys that should elicit similar concerns have made it to market and are in use across the U.S.

Dr. Tiffany Munzer, a developmental behavioral pediatrician and clinical lecturer at the University of Michigan notes that "most interactive toys, games and internet platforms made for children depend on AI technology."[19] This means that these forms of entertainment geared towards children also rely on data input and collection. That data, then, has the potential to become part of a child's digital footprint, adding to the ever-growing shadow of information that follows them. This trend is not new; as early as 2015 toys like CloudPets,[20] Hello Barbie,[21] My Friend Cayla dolls[22] and Fisher Price teddy bears[23] were found to collect and store recordings of children and their families in clear violation of privacy rights. Between 2015 and 2016 several of these toys and their parent companies also experienced data leaks, further jeopardizing children's information.

Children and adolescents actively contribute to their own digital footprints through direct interactions with online platforms.[24] Social media platforms specifically employ algorithms to analyze user data and curate personalized content. This practice results in the creation of an even more detailed digital footprint that reflects users' online behavior, preferences, and social interactions based on comments, likes and time spent on specific content.[25, 26, 27] In this way social media is one of the biggest ways that data is collected on individuals, both actively and passively. According to the U.S. Surgeon General, 40 percent of children ages 8-12 use social media.[28] Additionally,

according to a 2023 Pew survey of 13- to 17-year-olds, about one third of teens report being on social media sites almost constantly everyday.[29] This level of engagement raises important questions about how the data generated by these interactions is used and the long-term implications for children's privacy and autonomy.

By the time children begin school, their digital footprints expand further, often including sensitive learning and education data. AI-powered online learning platforms, widely adopted during the COVID-19 pandemic, can significantly contribute to their digital footprints. These platforms, as well as other EdTech software used for record keeping purposes in schools often capture sensitive information about children's thinking patterns, learning styles, and engagement levels.[30] While AI offers valuable support as an educational tool—especially for students with increased learning needs including but not limited to language translation supports—the potential privacy risks of its use in education remain under-discussed.[31]

The digitization and storage of children's learning and behavioral data raises serious concerns about how this sensitive information is both used and protected.[32] The Federal Trade Commission (FTC) has expressed significant concerns about the privacy practices of EdTech platforms, particularly regarding the excessive collection and use of children's personal data, emphasizing the problematic

nature of “Parents [having] to choose between their children’s privacy and their participation in the digital classroom.”[33]

There is also justified apprehension around the security of the data that EdTech companies collect. EdTech companies are extremely vulnerable and are frequent targets of cyber-attacks.[34] Between 2016 and 2021, 55 percent of data breaches experienced by K-12 schools occurred because of attacks carried out on EdTech vendors.[35] In 2022, breaches exposed personal data of students from New York and Chicago, including race, test scores, tardiness rates, special education status, migrant status, behavior incidents, and descriptions of disabilities.[36, 37] The insidious nature of data breaches, with potential negative effects manifesting years or even decades later, makes it difficult to grasp the full extent of harm. Not only could compromised information influence things like college admissions and hiring decisions, but other significant opportunities as well because they heighten the chances of identity theft and financial fraud. The persistence of sensitive information on the internet further exacerbates this issue, as it can be accessed and misused by malicious actors at any time and can be difficult to subsequently secure once it has been leaked.

Microtargeting & Surveillance

Today's pervasive data collection practices have created an ecosystem where online and offline activities leave lasting digital footprints. AI-powered behavioral advertising raises concerns about both data privacy and manipulation. Third-party companies collect vast amounts of personal data to create highly targeted ads, often exploiting cognitive biases to influence consumer behavior.[38] As more data on individuals becomes available via interactions with different platforms, third-party companies use AI to tailor advertisements to specific users based on their observed behavior.[39] As the International Digital Accountability Council notes "not only do companies deploy personal information for private benefit, they often do so covertly."[40]

Major technology companies have faced criticism for data surveillance practices that inform microtargeting. For instance, Google, Amazon, Apple, Microsoft and Facebook have been found to employ human operators and subcontractors to review sensitive audio recordings from smart devices. For example, in spite of Amazon's Echo smart speaker allegedly being a voice activated device, Amazon employees and subcontractors in both the US and India were found to listen in on private household conversations. At Google, third party contractors were found to systematically eavesdrop and listen to stored audio recordings from various devices from Google Home speakers to smartphone apps, accessing sensitive and confidential information, including in some cases the location of children.[41, 42] Moreover, a whistleblower at a subcontractor for Apple disclosed that data is collected by Siri, the company's voice assistant that is installed in all Apple devices from iPhones and Apple watches that people carry with them all day, to the company's HomePod smart speakers that they keep in their homes. Similar to other smart device manufacturers, the whistleblower alleged that Apple employs people to analyze this data that was found to include highly sensitive information such as confidential medical records, illicit drug transactions, and private sexual encounters.[43] In this way, surveillance culture is not limited to digital footprints from online activity and interactions with smart speakers, but rather it has become so pervasive as to be practically inescapable. As such, there is arguably no true "opt-out" of data collection and use in today's evolving technological world.

The Dangers of Deceptive Design

Children are particularly susceptible to deceptive design practices that exploit cognitive biases in order to gain access to their personal data.[44] The FTC highlights that "the use of manipulative design techniques in the digital world can pose heightened risks to consumers" and deceptive design "can be found in a variety of industries and contexts, including ecommerce, cookie consent banners, children's apps, subscription sales, and more."[45]

Social media applications are known to use more deceptive design patterns than traditional websites. These platforms rely on vague language that users must scroll through extensively in order to access the site and bury "opt-out" options in complex settings. These practices create the illusion of consent and choice, while making true "opt-out" decisions practically inaccessible.[46]

Studies show that when deceptive design is implemented, users are two to four times more likely to make choices contrary to their best interests than they would when presented with clear, straightforward options.[47] Tactics such as hiding information, using trick questions and nudge strategies[48] are commonly and successfully used to steer users toward decisions that benefit platforms, often at the expense of the user themselves.

The design tactic of making it more difficult to access certain options, such as "opting out" of data sharing, effectively discourages individuals from exercising their own online autonomy and the use of multiple deceptive design patterns have a compounding effect.[49] For instance, Meta (the parent company of Facebook and Instagram) employs numerous deceptive design techniques in order to give the illusion of choice. To comply with regulations in the European Union, Meta provided a "right to object" link through app notifications.[50] However, the notification's link opened a page containing only a prominent "close" button which, if clicked, allowed Meta to use the user's data to train AI systems. The actual opt-out link was hidden in the notification text, and after the notification disappeared, users had to navigate deep into privacy settings to access it. Even then, users were required to fill out a form providing personal information and a reason for objecting, with no guarantee that the request would be honored.[51] In the U.S., Meta offers even fewer options, only allowing users to opt out of third-party data training, not Meta's AI training.[52, 53, 54] Furthermore, users have to do this on a per-app basis, further compounding difficulties in securing their data.[55]

Developmental Vulnerabilities for Young People

Deceptive design in online platforms geared towards young people poses unique risks due to children's inherent developmental vulnerabilities. While discussions of children's rights online often center around issues like child abuse material, the broader risks posed by AI's growing capability creates significant and underexplored threats to children's safety and well-being.[56] These risks extend beyond traditional online dangers and into the complex realm of data and psychological manipulation. According to a 2024 report by the Privacy and Access Council of Canada, researchers found that in a sample of apps and online platforms, 97 percent used deceptive design, and that "the use of deceptive design patterns is often worse among websites and apps that are geared towards children."[57] From a developmental perspective, early childhood and adolescence encompass critical windows of cognitive and emotional growth.[58] Research shows that children's brains undergo substantial structural and functional changes during these formative periods[59] and therefore their brains are far more malleable, making youth more susceptible to manipulation via deceptive design.

Research shows that although a child's brain is approximately full size by the age of six years old, they continue to learn and develop significantly into young adulthood.[60] Neurologically, the human brain goes through several periods of development throughout the life course. During specific developmental windows, children's brains are extremely pliable, making them susceptible to external influences.[61] During sensitive periods such as youth and early adolescence, young people are more easily influenced and external input has a larger overall impact.[62, 63] Though evolutionarily, these windows of development are meant to facilitate learning, periods of plasticity and increased susceptibility to influence can also be exploited, leading to detrimental long-term consequences.

In the past, conversations around the influential nature of AI technology on young people's psyche have focused on the way AI powered algorithms promote specific content that could be harmful to children such as suggesting posts and videos relating to self-harm, eating disorders or dangerous activities and "challenges." However, the expanding capabilities and widespread use of large language model (LLM)-based chatbots have introduced new, complex ethical and psychological concerns. It is unclear presently all the ways in which AI, specifically AI powered chatbots, can and will impact child development and well-being.[64] This issue was poignantly highlighted in February 2024, when a Florida family suffered a devastating tragedy. Sewell Setzer III, a 14-year-old boy, died by suicide following interactions with a lifelike, anthropomorphized chatbot. Over time, the AI became a significant emotional attachment for him, contributing to increased social isolation and deepening depression.[65] In the aftermath of this tragedy, his mother filed a lawsuit against CharacterAI, the company responsible for the chatbot in question. The case, *Garcia v. CharacterAI,* alleges that the company deliberately targeted children through manipulative practices and collected sensitive juvenile data while failing to implement essential safeguards to prevent harm. The plaintiff also asserts that the chatbot was marketed as safe for younger audiences despite its potentially harmful and unregulated design.[66]

Presently, more than 20 million people use the CharacterAI service and spend more than an hour interacting with the chatbots daily. The chatbots are designed to create interactions that feel real to users. According to

documents in the case file, CharacterAI now offers a call chat feature that allows an individual to call their customized character, further blurring the distinction between fiction and reality.[67] What is particularly concerning is that CharacterAI has marketed their product as safe for children under 13, but *Garcia* alleges CharacterAI uses sex and social approval to capitalize on cognitive vulnerabilities of children to increase engagement and gain access to a trove of rare and valuable data.[68] In the suit, *Garcia* highlights that Character AI distributes their product to children for free, and what revenue they receive from paying customers does not cover the high cost of running the LLM. For this reason *Garcia* alleges that the data of users, particularly young users like Setzer who Character AI markets to and attracts, is the product itself.[69]

In attempts to gain access to the data of young users, platforms that lack crucial safeguards for children reveal how dangerous AI can be when left unregulated. With advances in AI technology and improvements to LLMs like the one used by Setzer, a booming and largely unregulated industry of AI companionship apps has taken off. Many of the chatbots are customizable, remember past conversations, adapt to the communication style of the user, and are often designed to simulate romantic or intimate relationships. Some of these apps claim to be targeted at ending the loneliness epidemic, though there is little research to support these claims. In fact, users have reported that they often feel abandoned when they are unable to use the app because it provided a judgment-free friend who always responded and could be tailored to interact with them in the exact ways they wanted, unlike a human companion.[70] The absence of built-in safety features and parental controls for underage users creates a significant risk of harm. Without adequate oversight, children are vulnerable to manipulation and exposure to harmful content. What happened to Setzer is a stark example of how programming used by Character AI and others that is meant to make the AI seem more human and increase user engagement can have devastating outcomes. As alleged in *Garcia* "a child could express suicidality and then seek to move on from that topic, only to be repeatedly pulled back to it by a CharacterAI bot".[71]

The United Kingdom recognizes children's personal data as especially vulnerable, with the EU AI act designating children as a protected class due to their heightened susceptibility to influence.[72] In the U.S., however, we continue to rely on patchwork policy and disclosures that are often shrouded in layers of deceptive design. In this way, disclosure and transparency have become a regulatory crutch, not just in the tech world but across sectors.

Disclosure alone does not bar harmful or underhanded practices that can often be used to mislead. Disclosure and transparency only truly work when things are simple, accessible and in plain language.

Otherwise "disclosure devolves into a tool that gives advantages to the well-educated and affluent over the poor and disadvantaged. [..]The wealthy access those finite services, at the expense of the uneducated"[73] and these predatory practices perpetuate cycles of generational exploitation and poverty.

Without the proper policies and adequate enforcement mechanisms in place, AI can and will cause harm, particularly for those who lack the resources to pursue recourse.

POLICY ANALYSIS

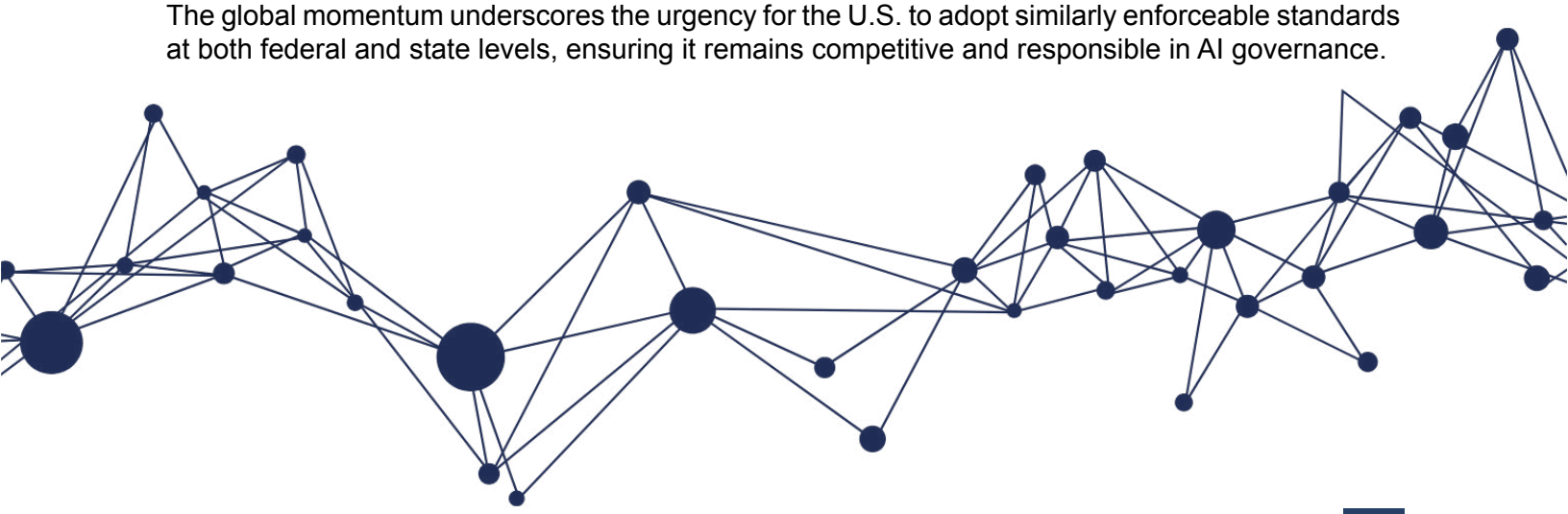
The regulatory landscape surrounding artificial intelligence in the U.S. is currently fragmented, with states taking the lead in enacting AI-specific policies in the absence of a comprehensive federal framework. As AI technology evolves rapidly and integrates into diverse sectors like healthcare, finance, education, and social media, existing regulations fall short in ensuring adequate protections, especially for vulnerable populations such as children. This section examines the state, federal, and international regulatory environments, emphasizing the critical role that state-level policies must play in safeguarding equity and mitigating the harms associated with AI. With AI becoming increasingly central to high-impact sectors, there is a need for clear, enforceable, and equity-focused regulation.

International Landscape: Global Benchmarks for AI Governance

Globally, the risks posed by unregulated AI and digital technologies are being addressed through varied approaches. For example, Australia recently proposed stringent social media legislation to protect children under 16 from potential harms, such as mental health issues and exposure to harmful content. This legislation includes age-verification measures, and places the burden of compliance on social media platforms rather than on parents or children.[74, 75] Australia's move underscores the growing recognition of the significant risks that unregulated digital platforms pose to vulnerable populations, particularly when AI algorithms amplify harmful content or enable unchecked access.

Similarly, the European Union (EU) has led the way in establishing comprehensive AI regulations that are future focused and able to adapt to rapidly changing technology. The EU's Artificial intelligence act, proposed in April of 2021, provides a robust framework that balances innovation with stringent safety and accountability standards. This Act is structured to analyze and classify AI systems according to the level of risk to users– ranging from minimal to unacceptable—and imposes strict requirements on high-risk systems, particularly those in sensitive areas such as education, healthcare, and law enforcement.[76] High-risk AI systems must undergo rigorous assessment, establish clear mechanisms for users to report misuse, and receive government approval before deployment. AI applications posing unacceptable risks to citizens' rights are banned under the act.

By prioritizing transparency, accountability, and ethical deployment, the EU has set a global benchmark for AI governance. These international efforts reflect a broad consensus on the need for strong governance frameworks to address the risk of AI, particularly when it comes to vulnerable populations. The global momentum underscores the urgency for the U.S. to adopt similarly enforceable standards at both federal and state levels, ensuring it remains competitive and responsible in AI governance.



Federal Landscape: Limited, but Growing Initiatives

Federal efforts to regulate AI in the U.S. remain in the early stages. As of November 2024, over 140 AI-related bills are currently under consideration in Congress,

but with wide variations in scope and enforceability.[77] Although this legislative activity reflects a growing recognition of AI's significance,

the existing lack of cohesive, binding standards underscores the need for a unified regulatory approach.

While a few of these bills show significant potential, even promising bills may encounter legal and operational challenges, particularly around enforceability.

Acknowledging potential issues that the government needs to be ready to face when it comes to AI in relation to data security, the executive branch has begun to put out directives to agencies and general guidance to the public. The White House's 2024 National Security Memo highlighted the risks of "data spillage," where AI systems may inadvertently or deliberately reveal sensitive information, highlighting that it is a risk tied to the development and deployment of AI that "may impact human rights, civil rights, civil liberties, privacy, safety, national security, and democratic values."[78] This memorandum outlines a national strategy to strengthen U.S. leadership in AI, with emphasis on national security and global competitiveness.[79] The directive emphasizes the importance of safeguarding AI development, promoting ethical use in line with democratic values, and fostering international collaboration on AI standards. However, while this memorandum encourages protective measures across sectors and underscores the principles of AI safety, transparency, and civil rights, it largely serves as guidance rather than enforceable policy.

Key initiatives, like the *Blueprint for an AI Bill of Rights* released by the White House in 2022, represent one of the most significant steps toward a national framework for AI governance.[80] This framework outlines five guiding principles aimed at ensuring that AI systems respect civil rights, protect privacy, and operate in ways that are safe and transparent. The blueprint emphasizes the importance of protecting against algorithmic discrimination, ensuring that there is proper notice and explanation as to when and how AI is being used, as well as the importance of having human alternatives whenever possible. As with other federal efforts, however, the Blueprint remains non-binding and lacks enforceable mechanisms, serving more as a guiding document than a regulatory mandate. Other federal efforts executed in compliance with the 2023 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence[81] such as the National Institute of Standards and Technology (NIST) AI Risk Management Framework,[82] have similarly focused on providing voluntary guidelines rather than enforceable laws.

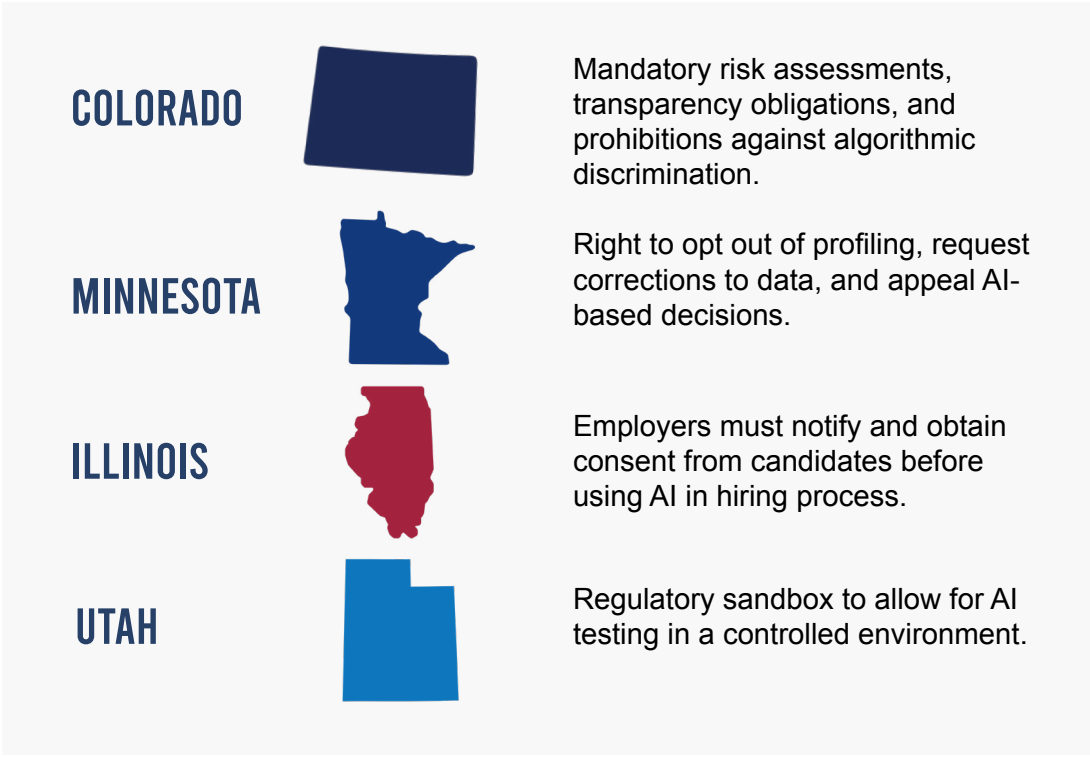
One established tool addressing children's data privacy that has been implemented to help mitigate some of the harms of AI is the 1998 Child Online Privacy Protection Act (COPPA).[83] The FTC has emerged as a crucial player in enforcing the COPPA within the evolving landscape of AI data collection practices. Since 2020, the FTC has begun investigating prominent and well-known

companies such as YouTube, Microsoft (Xbox), Amazon (Twitch), Meta (Facebook), X (formerly known as Twitter), Snap, ByteDance (TikTok), Discord, Reddit, and WhatsApp while also bringing litigation against those found to be in violation of the act.[84] In 2024, the FTC released a report on data and AI usage by the companies and found that a "trend among the Companies was that they failed to adequately protect children and teens" and that "There was a widespread application of Algorithms, Data Analytics, or artificial intelligence ("AI"), to users' and non-users' personal information."[85] While COPPA enforcement provides a layer of accountability, this mechanism alone offers only a thin layer of protection and can only be utilized under specific circumstances. Given the scale and complexity of AI's impact on children's data privacy, there is a need for additional legal tools and updated protections that can more effectively address AI-related privacy concerns for young users. This challenge is exacerbated by the recent supreme court decision to overturn the Chevron Doctrine, which had historically allowed federal agencies like the FTC to interpret and implement broad statutory mandates. Without Chevron deference, the FTC's ability to adapt existing regulations to address emergent AI risks is significantly weakened.[86, 87, 88] Compounding this challenge, the change in administration following the 2024 election signals a potential shift towards federal deregulation and revised agency directives, which may further reduce accountability and enforcement at the federal level. As a result, it will be incumbent on legislators at the state level to implement measures to safeguard citizens.

State-level Landscape: Proactive, but Incomplete

In response to federal inaction, many states have taken proactive measures to address AI's risks, particularly concerning data privacy and algorithmic transparency. Over the past five years more than 30 states have passed or proposed laws to address growing concerns around this new technology.[89] For example, California's Age-Appropriate Design Code Act, passed in September 2022, sought to set new standards for digital platforms by regulating how children's data is collected, used, and protected. Though originally seen as a model for prioritizing user safety in AI design, a lawsuit led to an injunction.[90] Another recent California bill, AB 2013, has fared better by addressing data transparency that requires clearer disclosures from companies.[91] Similarly, states like Massachusetts, and New Jersey have introduced measures to protect against algorithmic discrimination, deepfakes, and misuse of AI-driven media, although many of these bills have yet to be fully implemented.

Colorado has led with the 2024 AI Act, which imposes stringent requirements on high-risk AI systems, including mandatory risk assessments, transparency obligations, and prohibitions against algorithmic discrimination. This law targets AI used in consequential decisions in areas such as education, healthcare, and employment and includes transparency measures for consumer-facing systems.[92] Likewise, Minnesota's HF 4757 adopts comprehensive data privacy protections, granting consumers the right to opt out of profiling, request corrections to data, and appeal AI-based decisions.[93, 94, 95] Illinois has implemented more targeted measures with its Artificial Intelligence Video Interview Act, requiring employers to notify and obtain consent from candidates before using AI in hiring processes, helping address concerns about bias in employment.[96, 97]



Utah has adopted an innovative approach through its regulatory sandbox model, which allows organizations to test new technologies and services, including AI, in a controlled environment. Enacted in 2020, Utah's sandbox[98] requires AI systems to disclose their use while fostering collaboration through a state task force. This model enables stakeholders to evaluate impact and risks while

informing future policy development, offering a pathway for responsible AI innovation.[99, 100] Similarly, Texas has proposed a regulatory sandbox to explore industry-neutral applications of AI and other emerging technologies, emphasizing flexibility while maintaining consumer protections.[101, 102]

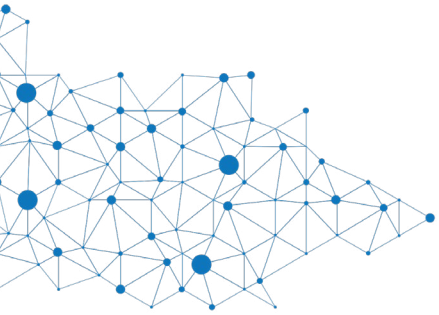
While these state-level efforts represent significant progress, they remain fragmented, leaving significant gaps in protections for children and other vulnerable groups across sectors. Without a unified federal standard, state-level policies that prioritize equity and safeguard at-risk populations remain critical for filling these regulatory voids. Innovations, like regulatory sandboxes, highlight how states can balance fostering innovation with managing risks, offering a valuable framework for broader adoption. Together, these state initiatives demonstrate the potential for comprehensive AI governance while paving the way for cohesive federal legislation in the future.

Connecticut's Policy Landscape: Pioneering State-Level AI Policies

Connecticut's recent legislative actions exemplify how states can lead in AI governance, serving as a potential model for other states and the federal government. In 2022, Public Act 22-15: An Act Concerning Personal Data Privacy and Online Monitoring, established foundational data protection measures, marking an initial step toward comprehensive resident protections.[103] Building on this, Public Act 23-561[104] (2023) strengthened Connecticut's data protections by amending the Connecticut Data Privacy Act to include safeguards for consumer health data and children's online privacy, such as banning the processing of children's data for targeted advertising without consent. These provisions align closely with the broader goals of Public Act 23-16,[105] also passed in 2023, which set up an Office of Artificial Intelligence and created a provisional task force to study AI's broader impact. The recommendations of this task force later informed the introduction of SB 2: An Act Concerning Artificial Intelligence in 2024.

Senate Bill 2 sought to tackle many of the key issues arising in the AI space. The bill included measures to prevent algorithmic discrimination, create transparent risk management frameworks, and regulate AI-generated deceptive media that could influence elections. The bill also prioritized public education on responsible AI use, working with stakeholders to train students, teachers, and the workforce to navigate AI ethically.[106] Moreover, SB 2 sought to criminalize non-consensual AI-generated content, a critical provision for protecting individual privacy.[107] While the bill did not make it to a House vote, its language provides a valuable starting point for future legislation.

Connecticut's policy landscape demonstrates the importance of state-level action in the absence of enforceable federal guidelines. By pursuing forward-thinking AI policies, Connecticut not only protects its residents but also serves as a model for other states looking to establish similarly robust protections. The state's ongoing efforts underscore the potential for state governments to mitigate risks, promote equity, and build a foundation for cohesive AI governance in the U.S.



POLICY RECOMMENDATIONS

As AI continues to become embedded in various aspects of society—including education, healthcare, and digital platforms that children use daily—there is an opportunity and an imperative for the state of Connecticut. Given that much of AI policy has been left to the states, we are positioned to define a path that prioritizes data privacy, equity, transparency and accountability that reflects a proactive and adaptable approach to AI regulation.

Safeguarding children's rights in this rapidly evolving digital age requires a multifaceted approach, one that necessarily incorporates both protective measures and educational initiatives that promote the development of AI literacy and critical thinking. This dual focus not only strengthens regulatory protections but also empowers young people to navigate a digital landscape shaped by AI.[108] Connecticut's recent legislative efforts, such as SB 2 (from the 2024 Connecticut legislative session), offer a valuable foundation for state-led AI governance. Although SB 2 did not pass, its framework reflects a proactive approach and provides a starting point for policy making. Building on SB 2 and informed by other state and federal policies, the following recommendations address the regulatory need surrounding AI's impact on children and historically disadvantaged populations, promoting governance that is not only proactive, but also adaptable to the constantly evolving technology. Based on our research and discussions with issue area experts we propose the following policy recommendations.

1. CENTER FAIRNESS, TRANSPARENCY, & DISCLOSURE

These recommendations aim to build public trust in AI by ensuring that users are aware of when and how AI systems are influencing their lives. By creating clear guidelines for transparency and disclosure, Connecticut can empower individuals with informed consent and control over their interactions with AI.

- Establish clear disclosure requirements ensuring individuals know when they are interacting with AI systems.
- Implement plain language guidelines for disclosures so users can easily understand how and when AI is being applied.
- Implement opt-out mechanisms that are accessible, easily understood, and allow users to limit data collection and AI training.

2. ENSURE ACCOUNTABILITY & BIAS MITIGATION

By establishing measures for bias detection and continuous monitoring, these recommendations seek to foster a more accountable AI ecosystem, where systems are regularly assessed for fairness. This accountability will help protect vulnerable populations from discriminatory practices and unintended biases that can perpetuate inequities.[109]

- Implement regular AI assessments and continuous monitoring to identify and mitigate harmful, biased and/or disparate outcomes when deploying AI systems.

- Establish and utilize a permanent AI working group that meets regularly to identify public concerns around the use of AI as it continues to develop and implement recommendations on how to address the most pervasive issues.
- Align definitions with international AI standards, which describe AI as machine-based systems producing outputs that can influence environments, with variations in autonomy and adaptability.[110]

PROMOTE DATA PROTECTION & PRIVACY

Strengthening data protections is essential for safeguarding individuals, particularly children, from the risks associated with extensive data collection and misuse. These recommendations aim to provide robust safeguards against data exploitation.

- Expand and strengthen data protections, with enhanced standards specifically focused on safeguarding children's data.
- Extend and enforce protections to prevent deepfakes and the non-consensual dissemination of AI-generated content.
- Pass legislation that provides a way for users to flag a party using AI or an AI system for review based on bias, discrimination, and or misuse.

SUPPORT ETHICAL INNOVATION

To encourage responsible AI development, these recommendations focus on incentivizing ethical practices and providing educational resources. Supporting ethical innovation can foster a balanced approach that promotes growth and responsible use of AI without stifling smaller companies or startups.

- Incentivize innovation and promote "good actors" by establishing an AI technology grant program that sets high standards without excluding smaller companies and startups. To qualify, developers must meet state-established standards and demonstrate how their AI solutions address critical social challenges and contribute to the public good.
- Establish a regulatory sandbox to allow developers to test AI solutions in a controlled environment while addressing risks and ensuring compliance. A state task force would oversee the sandbox, using insights to inform future AI policies.
- Establish safe use of AI training programs for educators and students that focus on how to properly and safely use artificial intelligence as a supplementary classroom instruction tool.
- Develop and implement accessible ethical use training programs for state employees and the general public to promote responsible and informed engagement with AI technologies.

IMPLEMENT RISK-BASED & SECTOR-SPECIFIC REGULATION

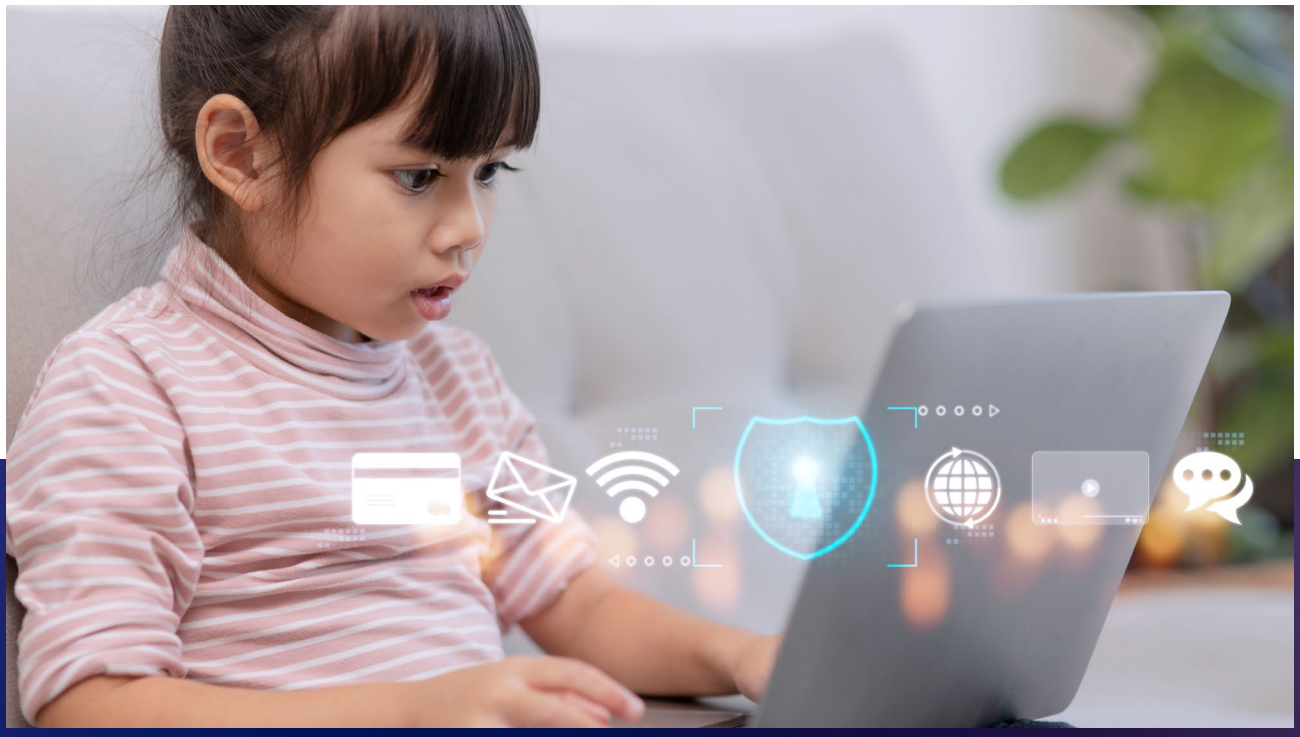
Adopting a risk-based approach enables targeted regulation for high-impact AI applications while allowing for flexibility in lower-risk contexts. By aligning with international best practices, Connecticut can ensure AI applications in sensitive areas are appropriately monitored, building safety and fostering ethical compliance.

- Establish a regulatory body to oversee and enforce AI standards, ensuring regulatory consistency across jurisdictions.
- Adopt a comprehensive policy modeled after the AI Act in the EU to create a functional regulation process based on the risk category that an AI system falls into.
- Provide funding for the establishment of an AI safety review process.
- Model legislation after California, Texas, Minnesota and Washington that regulates how AI can be used in campaigns and elections, implementing disclosure requirements, and restrictions on using AI to falsely portray a candidate in a way that would influence an election.

ENFORCE CONSUMER PROTECTION

As AI expands into commercial spaces, measures are needed to safeguard consumers and ensure fair market practices, especially to protect against predatory pricing and other exploitative practices.

- Explicitly prohibit price fixing via artificial intelligence, algorithm or other technology.
- Build on SB 2 An Act Concerning Artificial Intelligence, recommendations from the AI Board, the AI Lab and existing AI legislation in other states to establish AI regulation for non-government entities.



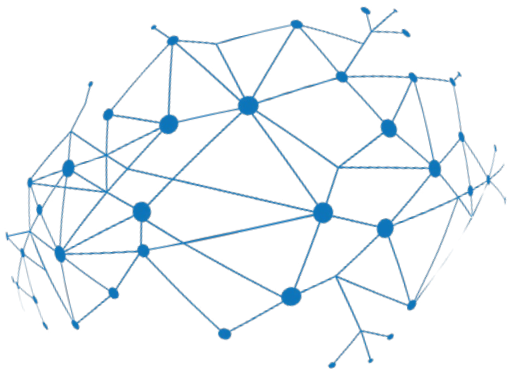
DISCUSSION & CONCLUSION

The rapid innovation in the field of Artificial Intelligence (AI) must be balanced with comprehensive regulation to mitigate social risk and ensure the safety of children and families. The unique risks that AI, if left unregulated, poses to children is significant and therefore, AI guardrails need not only focus on algorithmic transparency, but also accessibility and accountability, allowing legislators, consumers and other stakeholders to engage in productive actions, not simply discussions around ensuring safety and equity in an increasingly technological age.

When it comes to AI regulation in the U.S., recourse and balance is limited due to a lack of proper mechanisms to pursue meaningful AI accountability. Though some have begun to seek recourse through the courts in order to address some of the numerous ways AI regulations fall short[111] there is no private right to action and no clear reporting mechanism to flag non-compliant systems,[112] both of which would provide additional modes of accountability.[113] There is, however, an opportunity for Connecticut to begin creating the framework that is needed to uphold a healthy AI ecosystem. At present, a minimally regulated landscape poses issues to responsible AI growth. The ability for robust competition is an important part of holding corporations accountable and ensuring the highest standards. In theory, by enforcing stricter guidelines, companies responsible for severe data breaches or significant bias issues will lose eligibility for contracts, fostering a fairer competitive landscape and encouraging accountability.

AI's processing capacity raises new questions, including privacy concerns, with long-term implications that require intentional tailored solutions with the capacity to both evolve alongside AI and foster healthy and responsible AI growth. Focusing on frameworks that are human-centered and build in equity and accountability measures is a choice that will impact future generations of Connecticut residents as AI continues to become an even larger part of our everyday lives.

Currently, policies like COPPA, originally designed to address different issues, are being repurposed to address aspects of AI governance. However, these retrofitted mechanisms of enforcement often lack the scope and specificity needed to address the inherent complexity of AI. Relying on such piecemeal regulations leaves significant gaps in the legal framework necessary for promoting responsible AI development. Establishing concrete methods of accountability and creating new policies that are effective and sustainable in the face of rapid technological advancement, in conjunction with other efforts, will help to cover regulatory gaps that leave children exposed to data manipulation and potential exploitation. Comprehensive AI legislation is critical for building a robust accountability framework to address the inequities in AI systems, which can profoundly influence a child's long term socioeconomic opportunities. By addressing the ways in which AI and data processing practices negatively impact children, we can mitigate the risks associated with AI and foster a future where technology advances responsibly, without compromising individual privacy.



Though many people in the tech space conceptualize making AI "more human" as making it more human-like,

the real goal needs to be making AI more human-centered. This means recognizing and addressing instances where harm occurs.

It requires implementing robust feedback mechanisms and review processes to offer real solutions and prevent further harm. The digital world offers tremendous opportunities for exploration and learning for children. However, without adequate safeguards, it also presents a landscape ripe for exploitation. Safeguarding children in this context requires intentionality. This is the new frontier for children's advocacy. Just as children need guidance and protection in the physical world, they also require robust safeguards within the digital landscape to ensure they thrive. By fostering an equitable environment where every child is empowered to practice digital autonomy and navigate AI responsibly, Connecticut can take another step towards becoming a state where all children achieve their full potential.

ACKNOWLEDGMENTS

Connecticut Voices for Children extends our sincere thanks to Kevin De Liban, Director of Advocacy at Legal Aid of Arkansas and Founder of TechTonic Justice; Jordan Jefferson, Director of the Lynne L. Pantalena Law Library and Associate Professor of Law at Quinnipiac University; and Dr. Nicholas Pratt, MD, RN, of Yale Medicine Department of Psychiatry for their input and review of this paper.

ENDNOTES

1 Organization for Economic Co-operation and Development. (n.d.). *Artificial intelligence.* Retrieved November 8, 2024, from https://www.oecd.org/en/topics/policy-issues/artificial-intelligence.html

2 Clarkin, C. N., O'Brien, P. R., Ruth, L., Byrne, E., Teeling, N., Sabin, E., Abdo-Katsipis, C. B., Diaz, R., & Adelaiye, S. (2024, June 13). 2024 *candidate briefing book*. Connecticut Voices for Children. https://ctvoices.org/publication/2024-candidate-briefing-book/

3 Lerude, B. (2023). *States take the lead on regulating artificial intelligence.* Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-artificial-intelligence

4 Clarkin, C. N., O'Brien, P. R., Ruth, L., Byrne, E., Teeling, N., Sabin, E., Abdo-Katsipis, C. B., Diaz, R., & Adelaiye, S. (2024, June 13). *2024 candidate briefing book.* Connecticut Voices for Children. https://ctvoices.org/publication/2024-candidate-briefing-book/

5 Lerude, B. (2023). *States take the lead on regulating artificial intelligence.* Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-artificial-intelligence

6 Algorithmic Accountability Conference 2024 Yale Law School. Nov 1, 2024

7 Goel, H., & Chaudhary, G. (2024). Securing the digital footprints of minors: Privacy implications of AI. *Balkan Social Science Review, 23*, 235–260.

8 ibid

9 Wilton, R., & Richardson, C. (2024, October). *Take a step towards privacy: Understanding digital footprints*. Internet Society Foundation. https://www.internetsociety.org/blog/2024/10/understanding-digital-footprints/

10 Abrantes, B. F., & Ostergaard, K. G. (2022). Digital footprint wrangling: Are analytics used for better or worse? A concurrent mixed methods research on the commercial (ab)use of dataveillance. *Journal of Marketing Analytics, 10*(3), 187–206. https://doi.org/10.1057/s41270-021-00144-5

11 Auxier, B., Anderson, M., Perrin, A., & Turner, E. (2020, July 28). *Children's engagement with digital devices, screen time.* Pew Research Center. https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/

12 Goel, H., & Chaudhary, G. (2024). Securing the digital footprints of minors: Privacy implications of AI. *Balkan Social Science Review, 23*, 235–260.

13 McAfee. (2021, January 21). *The connected lives of babies: Protecting their first footprints in the digital world.* https://www.mcafee.com/blogs/family-safety/the-connected-lives-of-babies-protecting-their-first-digital-footprints/

14 Peachman, R. R. (2017, October 5). Mattel pulls Aristotle children's device after privacy concerns. *The New York Times.* https://www.nytimes.com/2017/10/05/well/family/mattel-aristotle-privacy.html

15 Owlet Care. (n.d.). *Owlet Dream Sock.* Retrieved November 13, 2024, from https://owletcare.com/products/owlet-dream-sock?srsltid=AfmBOopmHfSqrZ6cGsBwEYGW_U_mttoGkfBcN0on1L4eIcT-JFw-M7CK-

16 Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., & Nicholson, J. (2023). The digital harms of smart home devices: A systematic literature review. *Computers in Human Behavior, 145,* 107770. https://doi.org/10.1016/j.chb.2023.107770

17 Peachman, R. R. (2017, October 5). Mattel pulls Aristotle children's device after privacy concerns. *The New York Times.* Retrieved from https://www.nytimes.com/2017/10/05/well/family/mattel-aristotle-privacy.html

18 Markey, E. J. (2017). *Letter to Mattel regarding the Aristotle children's device* [PDF]. https://www.markey.senate.gov/imo/media/doc/Mattel%20letter.pdf

19 Munzer, T. (n.d.). How will artificial intelligence (AI) affect children? *HealthyChildren.org.* https://www.healthychildren.org/English/family-life/Media/Pages/how-will-artificial-intelligence-AI-affect-children.aspx

20 Larson, S. (2017, February 27). Stuffed toys leak millions of voice recordings from kids and parents. *CNN Money.* https://money.cnn.com/2017/02/27/technology/cloudpets-data-leak-voices-photos/index.html

21 Coblentz, E. (2023, November 17). New report outlines risks of AI-enabled smart toys on your child's wish list. *USA Today.* https://www.usatoday.com/story/money/shopping/2023/11/17/toys-that-spy-on-children-growing-concern-report/71609172007/

22 Electronic Privacy Information Center. (2016). *Complaint and request for investigation, injunction, and other relief: In the matter of Genesis Toys and Nuance Communications, Inc.* [PDF]. https://epic.org/wp-content/uploads/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf

23 Coblentz, E. (2023, November 17). New report outlines risks of AI-enabled smart toys on your child's wish list. *USA Today.* https://www.usatoday.com/story/money/shopping/2023/11/17/toys-that-spy-on-children-growing-concern-report/71609172007/

24 The White House. (2022). *Blueprint for an AI Bill of Rights: Making automated systems work for the American people.* https://www.whitehouse.gov/ostp/ai-bill-of-rights/

25 Anderson, M., Faverio, M., & Gottfried, J. (2023, December 11). *Teens, social media, and technology 2023: YouTube, TikTok, Snapchat and Instagram remain the most widely used online platforms among U.S. teens.* Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/

26 Goel, H., & Chaudhary, G. (2024). Securing the digital footprints of minors: Privacy implications of AI. *Balkan Social Science Review, 23*, 235–260.

27 Ophir, Y., Asterhan, C. S. C., & Schwarz, B. B. (n.d.). The digital footprints of adolescent depression, social rejection, and victimization of bullying on Facebook. *Computers in Human Behavior.* Retrieved from https://www.elsevier.com/locate/comphumbeh

28 U.S. Department of Health and Human Services. (2023). *Social media and youth mental health: The U.S. Surgeon General's advisory.* https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf

29 Anderson, M., Faverio, M., & Gottfried, J. (2023, December 11). *Teens, social media and technology 2023: YouTube, TikTok, Snapchat and Instagram remain the most widely used online platforms among U.S. teens.* Pew Research Center. https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/

30 Goel, H., & Chaudhary, G. (2024). Securing the digital footprints of minors: Privacy implications of AI. *Balkan Social Science Review, 23,* 235–260.

31 Barua, P. D., Vicnesh, J., Gururajan, R., Oh, S. L., Palmer, E., Azizan, M. M., Kadri, N. A., & Acharya, U. R. (2022). Artificial intelligence enabled personalized assistive tools to enhance education of children with neurodevelopmental disorders—A review. *International Journal of Environmental Research and Public Health, 19(3*), Article 1192. https://doi.org/10.3390/ijerph19031192

32 Goel, H., & Chaudhary, G. (2024). Securing the digital footprints of minors: Privacy implications of AI. *Balkan Social Science Review, 23,* 235–260.

33 Federal Trade Commission. (2022, May 19). *FTC to crack down on companies that illegally surveil children learning online.* https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-crack-down-companies-illegally-surveil-children-learning-online

34 117th Congress. (2021). S.1917 - K-12 *Cybersecurity Act of 2021*. U.S. Congress. https://www.congress.gov/bill/117th-congress/senate-bill/1917/text

35 U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. (2023). *Protecting our future: Partnering to safeguard K–12 organizations from cybersecurity threats.* https://www.cisa.gov/sites/default/files/2023-01/K-12report_FINAL_V2_508c_0.pdf

36 Psilakis, A. (n.d.). EdTech data breach emphasizes need for bolstered data privacy and security protections. *IDAC Blog.* https://digitalwatchdog.org/edtech-data-breach-emphasizes-need-for-bolstered-da-

ta-privacy-and-security-protections/

37 Chicago Public Schools. (2022, May 20). *Breach notification for May 20, 2022: Battelle for Kids.* https://www.cps.edu/about/policies/student-online-personal-protection-act/breach-notifications/#:~:text=What%20happened%3F,%2D2018%20and%202018%2D2019

38 Micheli, Lutz & Büchi (2018) *Digital footprints: an emerging dimension of digital inequality. Journal of Information, Communication and Ethics in Society, 16 (3)*, 242-251. www.emeraldinsight.com/1477-996X.htm

39 Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale Journal of Law and Technology, 21*(1), 106–168. https://yjolt.org/sites/default/files/21_yale_j.l._tech._106_0.pdf

40 ibid

41 Tubaro, P., & Casilli, A. A. (n.d.). Human listeners and virtual assistants: Privacy and labor arbitrage in the production of smart technologies. In *Digital work in the planetary market.* Retrieved from: https://www.researchgate.net/profile/Paola-Tubaro/publication/361093702_Human_Listeners_and_Virtual_Assistants_Privacy_and_Labor_Arbitrage_in_the_Production_of_Smart_Technologies/links/629b981f416ec50bdb0ab908/Human-Listeners-and-Virtual-Assistants-Privacy-and-Labor-Arbitrage-in-the-Production-of-Smart-Technologies.pdf

42 Federal Trade Commission. (2023, July 21). *Amazon.com (Alexa), U.S. v.* [Case no. 2:23-cv-00811-TL]. Western District of Washington. https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3128-amazoncom-alexa-us-v

43 Tubaro, P., & Casilli, A. A. (n.d.). Human listeners and virtual assistants: Privacy and labor arbitrage in the production of smart technologies. In *Digital work in the planetary market.*

44 Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Analysis, 13*(1), 43–109. https://doi.org/10.1093/jla/laaa006

45 Federal Trade Commission. (2023, July 21). *Amazon.com (Alexa), U.S. v.* [Case no. 2:23-cv-00811-TL]. Western District of Washington. https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3128-amazoncom-alexa-us-v

46 ibid

47 Federal Trade Commission. (2022, September). *Bringing dark patterns to light.* https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf

48 A nudge is "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not." (Thaler & Sunstein 2008, p. 6)

49 Federal Trade Commission. (2022, September). *Bringing dark patterns to light.* https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf

50 As of May 2024 this link was only available to European users.

51 Delli Santi, M. (2024, July 16). Meta wants to make us its AI guinea pigs. *Open Rights Group*. Retrieved from https://www.openrightsgroup.org/blog/meta-wants-to-makes-us-its-ai-guinea-pigs/

52 Facebook. (n.d.). *Privacy policy*. Retrieved November 13, 2024, from https://www.facebook.com/privacy/policy/

53 Instagram. (n.d.). *Privacy and generative AI.* Retrieved November 13, 2024, from https://privacycenter.instagram.com/privacy/genai

54 Large, J. (2024, September 26). Meta AI scraping: How to opt out. *IPVanish*. Retrieved from https://www.ipvanish.com/blog/meta-ai-scraping/

55 Hong, YK (2024) *Opt out of biometric theft, facial recognition tech, and data scraping.* Retrieved November 13, 2024, from https://keepbeyond.com/optout/

56 Goel, H., & Chaudhary, G. (2024). Securing the digital footprints of minors: Privacy implications of AI. *Balkan Social Science Review, 23*, 235–260.

57 Privacy and Access Council of Canada. (2024, July 9). *Privacy sweep finds majority of apps and websites use deceptive design to influence privacy choices, including sites targeting children*. https://pacc-ccap.ca/privacy-sweep-finds-majority-of-apps-and-websites-use-deceptive-design-to-influence-privacy-choices-including-sites-targeting-children/

58 Center on the Developing Child (2007). *The Science of Early Childhood Development* (InBrief). Retrieved from www.developingchild.harvard.edu.

59 Haidt, J. (2024). *The anxious generation: How the great rewiring of childhood is causing an epidemic of mental illness.* Penguin Press.

60 ibid

61 ibid

62 Gwon, S. H., & Jeong, S. (2018). Concept analysis of impressionability among adolescents and young adults. *Child Health Nursing Research, 24*(4), 419–429. https://doi.org/10.4094/chnr.2018.24.4.419

63 Yang, Angela "Lawsuit claims Character.AI is responsible for teen's suicide" *NBC News.* October 23, 2024. https://www.nbcnews.com/tech/characterai-lawsuit-florida-teen-death-rcna176791

64 Pratt, N., Madhavan, R., & Weleff, J. (2024). Digital dialogue—How youth are interacting with chatbots. *JAMA Pediatrics, 178*(5), 429–430. https://doi.org/10.1001/jamapediatrics.2024.0084

65 Yang, Angela "Lawsuit claims Character.AI is responsible for teen's suicide" *NBC News*. October 23, 2024. https://www.nbcnews.com/tech/characterai-lawsuit-florida-teen-death-rcna176791

66 *Garcia v. Character Technologies, Inc.*, No. 6:24-cv-01903 (M.D. Fla., filed Dec. 11, 2024). Retrieved from https://www.courtlistener.com/docket/69300919/garcia-v-character-technologies-inc/

67 ibid/

68 ibid

69 ibid

70 Roose, K. (2024, October 23). Can A.I. be blamed for a teen's suicide? *The New York Times.* Retrieved October 24, 2024, from https://www.nytimes.com/2024/10/23/technology/characterai-lawsuit-teen-suicide.html

71 *Garcia v. Character Technologies, Inc.*, No. 6:24-cv-01903 (M.D. Fla., filed Dec. 11, 2024). Retrieved from https://www.courtlistener.com/docket/69300919/garcia-v-character-technologies-inc/

72 European Commission. (2021). *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

73 Eisinger, J. (2015, February 11). In an era of disclosure, an excess of sunshine but a paucity of rules. *The New York Times.* https://archive.nytimes.com/dealbook.nytimes.com/2015/02/11/an-excess-of-sunlight-a-paucity-of-rules/

74 Pal, A., & Kaye, B. (2024, November 7). Australia proposes 'world-leading' ban on social media for children under 16. Reuters. Retrieved from https://www.reuters.com/technology/cybersecurity/australia-proposes-ban-social-media-those-under-16-2024-11-06/

75 Kim, V. (2024, November 28). Australia has barred everyone under 16 from social media. Will it work? *The New York Times.* Retrieved from https://www.nytimes.com/2024/11/28/world/asia/australia-social-media-ban-law.html?smid=nytcore-ios-share&referringSource=articleShare

76 Clarkin, C. N., O'Brien, P. R., Ruth, L., Byrne, E., Teeling, N., Sabin, E., Abdo-Katsipis, C. B., Diaz, R., & Adelaiye, S. (2024, June 13). *2024 candidate briefing book*. Connecticut Voices for Children. https://ctvoices.org/publication/2024-candidate-briefing-book

77 Brennan Center for Justice. (2024, November 1). *Artificial intelligence legislation tracker*. https://www.brennancenter.org/our-work/research-reports/artificial-intelligence-legislation-tracker

78 The White House. (2024, October 24). *Memorandum on advancing the United States' leadership in artificial intelligence; harnessing artificial intelligence to fulfill national security objectives; and fostering the*

safety, security, and trustworthiness of artificial intelligence. https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/

79 ibid

80 The White House (2022) Blueprint for an AI Bill of Rights: Making automated systems work for the American people. *whitehouse.gov.* https://www.whitehouse.gov/ostp/ai-bill-of-rights/

81 The White House. (2023, October 30). *Executive order on the safe, secure, and trustworthy development and use of artificial intelligence*. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on

82 National Institute of Standards and Technology. (n.d.). *AI risk management framework.* U.S. Department of Commerce. https://www.nist.gov/itl/ai-risk-management-framework

83 105th Congress. (1998). S.2326 - *Children's Online Privacy Protection Act of 1998*. U.S. Congress. https://www.congress.gov/bill/105th-congress/senate-bill/2326

84 Federal Trade Commission. (2024, August 2). *FTC investigation leads to lawsuit against TikTok and ByteDance for flagrantly violating children's privacy law.* https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law

85 Federal Trade Commission. (2024, September). *A look behind the screens: Examining the data practices of social media and video streaming services* [Staff report]. https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf

86 Bardeen, S., & Gray, B. (2024, July 17). Unpacking the Supreme Court's recent ruling on the "Chevron Doctrine." *Public Policy Institute of California (PPIC) Blog*. Retrieved from https://www.ppic.org/blog/unpacking-the-supreme-courts-recent-ruling-on-the-chevron-doctrine/

87 Howe, A. (2024, June 28). Supreme Court strikes down Chevron, curtailing power of federal agencies. *SCOTUSblog*. Retrieved from https://www.scotusblog.com/2024/06/supreme-court-strikes-down-chevron-curtailing-power-of-federal-agencies/

88 Natural Resources Defense Council (NRDC). (2024, June 28). The Supreme Court ends Chevron deference—What now? *NRDC*. Retrieved from https://www.nrdc.org/stories/what-happens-if-supreme-court-ends-chevron-deference

89 Clarkin, C. N., O'Brien, P. R., Ruth, L., Byrne, E., Teeling, N., Sabin, E., Abdo-Katsipis, C. B., Diaz, R., & Adelaiye, S. (2024, June 13). *2024 candidate briefing book.* Connecticut Voices for Children. https://ctvoices.org/publication/2024-candidate-briefing-book

90 Jiang, K. (n.d.). *Netchoice v. Bonta: California Age-Appropriate Design Code Act update.* California Lawyers Association. Retrieved November 13, 2024, from https://calawyers.org/privacy-law/netchoice-v-bonta-california-age-appropriate-design-code-act-update/

91 California Legislature. (2024). *Assembly Bill No. 2013: An act to add Title 15.2 (commencing with Section 3110) to Part 4 of Division 3 of the Civil Code, relating to artificial intelligence (Chapter 817).* California Legislative Information. Retrieved from https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2013

92 Colorado General Assembly. (2024). SB24-205: *Consumer protections for artificial intelligence.* https://leg.colorado.gov/bills/sb24-205

93 Minnesota Legislature. (2023). *HF 3625: A bill for an act relating to public safety; modifying the deep fake election crime. Minnesota Revisor of Statutes.* Retrieved from https://www.revisor.mn.gov/bills/text.php?session=ls93&number=HF3625&session_number=0&session_year=2023&version=list

94 Cook, M. (2024, February 21). *Bill would ban deepfakes in political campaigns.* Minnesota House of Representatives. Retrieved from https://www.house.mn.gov/sessiondaily/Story/18085

95 Stauss, D., & Hammer, B. (2024, May 19). Minnesota Legislature passes Consumer Data Privacy Act. *Byte Back*. Retrieved from https://www.bytebacklaw.com/2024/05/minnesota-legislature-passes-consumer-data-privacy-act/

96 Illinois General Assembly. (2023). *Bill status of HB3563: DOIT-AI Task Force (Public Act 103-0451)*. Retrieved from https://www.ilga.gov/legislation/BillStatus.asp?DocNum=3563&GAID=17&DocTypeID=HB&SessionID=112&GA=103

97 Stauss, D., Malugade, L., & Davis, O. (2024, August 21). Illinois passes bill to regulate use of artificial intelligence in employment settings. *Byte Back.* Retrieved from https://www.bytebacklaw.com/2024/08/illinois-passes-bill-to-regulate-use-of-artificial-intelligence-in-employment-settings/

98 Utah Legislature. (2024). *SB0149: Artificial Intelligence Policy Act*. Utah 2024 General Session. Retrieved from https://le.utah.gov/~2024/bills/static/SB0149.html

99 Bednarz, J., & Jolivette, K. (2024, November 20). Utah sandbox inspires similar regulatory initiatives in Canada and other states. IAALS Blog. Retrieved from https://iaals.du.edu/blog/utah-sandbox-inspires-similar-regulatory-initiatives-canada-and-other-states

100 Braff, D. (2024, October 15). New rules issued for Utah's regulatory sandbox program. *ABA Journal*. Retrieved from https://www.abajournal.com/web/article/new-rules-issued-for-utahs-regulatory-sandbox

101 Texas Legislature. (2024). *Texas Responsible AI Governance Act.* Retrieved November 13, 2024, from https://s3.documentcloud.org/documents/25257148/texas-responsible-ai-governance-act-traiga-1.pdf

102 TPR Staff. (2024, December 5). Texas lawmakers face decision on comprehensive AI regulation. *Texas Policy Research.* Retrieved from https://www.texaspolicyresearch.com/texas-lawmakers-face-decision-on-comprehensive-ai-regulation/

103 Connecticut General Assembly. (2022). *Public Act No. 22-15: An act concerning personal data privacy and online monitoring.* https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF

104 Connecticut General Assembly. (2023, June 7). *Substitute Senate Bill No. 3 - Public Act No. 23-56 - Connecticut [PDF]*. Retrieved from https://cga.ct.gov/2023/ACT/PA/PDF/2023PA-00056-R00SB-00003-PA.PDF

105 Connecticut General Assembly [Connecticut.gov]. (2023, June 7). Substitute Senate Bill No. 1103 - Public Act No. 23-16 - Connecticut [PDF]. Retrieved from https://www.cga.ct.gov/2023/act/Pa/pdf/2023PA-00016-R00SB-01103-PA.PDF

106 Connecticut General Assembly. (2024). *Senate Bill No. 2: An act concerning artificial intelligence*. https://www.cga.ct.gov/2024/TOB/S/PDF/2024SB-00002-R01-SB.PDF

107 ibid

108 Algorithmic Accountability Conference 2024 Yale Law School. Nov 1, 2024

109 Micheli, Lutz & Büchi (2018) *Digital footprints: an emerging dimension of digital inequality. Journal of Information, Communication and Ethics in Society, 16* (3), 242-251. www.emeraldinsight.com/1477-996X.htm

110 In AI legislation legislators should strive to utilize the Organization for Economic Co-operation and Development (OECD) definition for AI (commended by experts to be the most future forward wording) Organization for Economic Co-operation and Development. (n.d.). *Artificial intelligence*. Retrieved November 8, 2024, from https://www.oecd.org/en/topics/policy-issues/artificial-intelligence.html

111 Federal Trade Commission. (2024, August 2). *FTC investigation leads to lawsuit against TikTok and ByteDance for flagrantly violating children's privacy law.* https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law

112 a practice that is at work in the EU AI Act.

113 European Commission. (2021). *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206