

Federal & State Student Privacy Law Updates

**We WANT
your input!**



Amelia Vance



amelia@publicinterestprivacy.org

- 10+ years focused on child and student privacy
- President & Founder of the Public Interest Privacy Center, a pending nonprofit
- Chief Counsel for the Student & Child Privacy Center at AASA, the School Superintendents Association
- Adjunct Professor for Privacy Law and EU Data Protection at William & Mary Law School since 2022 (previously taught at Penn State)
- Co-Chair of the Federal Education Privacy Coalition

About PIPC

- PIPC is a non-profit organization with extensive expertise in the student and child privacy legal landscape and in directly supporting research organizations, policymakers, state and local education agencies, privacy and child advocates, and education membership associations. We bridge the gap between dense legal and regulatory requirements and on-the-ground applications that meet the highest ethical and privacy protective standards.
- Our vision is that high-impact stakeholders at every tier will have the information and tools necessary to protect all children's fundamental right to privacy. By educating and equipping high-impact groups and fostering a culture of privacy, PIPC will help create an environment where all children will enjoy privacy-protected benefits of emerging technologies and data use.
- In addition to our grant-funded projects—primarily focused on creating free publications and providing trainings, news updates, and analysis to policymakers and national organizations—PIPC provides consulting services in our areas of expertise. This includes personalized trainings and workshops, building and implementing privacy programs. We also provide memos on issues such as the likely effect on an organization of new state or federal laws, existing laws applicable to AI in education, the differences in HIPAA and FERPA's deidentification standards, best practices for initial vetting of third party applications used in R&D projects, and what is permissible under FERPA when creating a unique cross-agency ID for integrated data systems.

Legal Disclaimer

The information provided in this presentation does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available are for general informational purposes only. Information in this presentation may not constitute the most up-to-date legal or other information. Event attendees should contact their attorney to obtain advice with respect to any particular legal matter. No one should act or refrain from acting on the basis of information in this presentation without first seeking legal advice from counsel in the relevant jurisdiction. Only your individual attorney can provide assurances that the information contained herein – and your interpretation of it – is applicable or appropriate to your particular situation.



Why is the Federal Landscape so Active?

Perhaps YouTube Fixed Its Algorithm. It Did Not Fix its Extremism Problem

CAMERON BALLARD / NOV 9, 2023

FTC awarding more than \$5M in refunds to Ring customers over privacy settlement

BY NICK ROBERTSON - 04/25/24 1:18 PM ET

Grindr secretly shared user data, angering users of the hookup app

The dating app allegedly disclosed users' HIV statuses to third-party firms

BY KRYSTLE VERMES PUBLISHED 2 DAYS AGO

The Washington Post
Democracy Dies in Darkness

Dating apps are collecting more of your information than you think

Research from the Mozilla Foundation says these apps are getting 'thirstier' for our data

By Chris Velazco
April 23, 2024 at 12:30 p.m. EDT

The Verge

Menu +

TECH / LAW / POLICY

Telehealth firm Cerebral fined \$7 million over 'careless' privacy violations

The firm used it of sloppy data handling and patient data with third parties like without consent.

I weekend editor who covers the latest in tech and he has written news, reviews, and more as a tech journalist since

2:39 PM EDT

TARGET

Target hit with class-action lawsuit claiming it violated Illinois' biometric privacy law

The law was the basis for several recent big settlements in Illinois, including against Facebook, Google, TikTok and Snapch

How G.M. Tricked Millions of Drivers Into Being Spied On (Including Me)

This privacy reporter and her husband bought a Chevrolet Bolt in December. Two risk-profiling companies had been getting detailed data about their driving ever since.

Bloomberg

Meta Gets EU Warning Over Use of Sexual Orientation Data

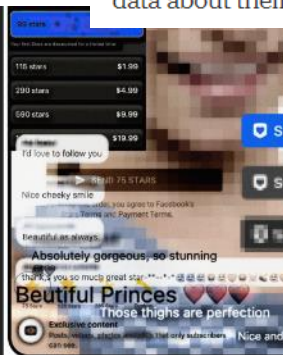
- EU court aide gives non-binding opinion in targeted ads case
- Court dispute pits Facebook against privacy activist Schrems

Facebook Twitter LinkedIn Email RSS Print

By Samuel Stoltz

April 25, 2024 at 5:17 AM EDT

Updated on April 25, 2024 at 5:52 AM EDT



Meta Staff Found Instagram Tool Enabled Child Exploitation. The Company Pressed Ahead Anyway.

Employees offered suggestions to reduce risks of misuse of subscription accounts featuring minors. Meta took another approach and says its programs are well monitored.



Senate Passes Spying Bill, Rejecting Privacy Concerns

Abortion-related medical records are used against patients. A new HIPAA rule reduces that. e officials say tool is vital to disrupting terror plots, ks

3-minute read

Letitia James, Kris Mayes and Dana Nessel Special to the USA TODAY Network
Published 5:38 a.m. ET April 25, 2024 | Updated 5:38 a.m. ET April 25, 2024

Follow

20, 20

Georgia Passes Law To Protect Firearm Retailers And Privacy For Buyers

GON Staff | April 25, 2024



~~404~~

Let's Talk About the Flock Study That Says It Solves Crime

JASON KOEBLER • MAR 20, 2024 AT 11:06 AM

A Flock study called "instrumental in reported crime" by a researcher who is now questioning how it was done.

Meta says vetting teens' ages should fall on app stores, parents

The tech giant is calling for legislation requiring that parents vet their kids' app usage on app stores like Google and Apple

By [Cristiano Lima-Strong](#) and [Naomi Nix](#)
Updated November 15, 2023 at 10:34 a.m. EST | Published

TikTok and others change platforms to protect kids. Advocates say it's just a start

MARCH 29, 2024 · 10:01 AM ET
By [Rhitu Chatterjee](#)

Parents



TikTok Says It Has Safety Measures in Place, But Just How Safe Is It for Kids?

Here's what you need to know about if TikTok is safe for kids and what parents can do to take action

By [Maressa Brown](#) | Updated on March 30, 2024
Medically reviewed by [Emily Edlynn, PhD](#)

INVESTIGATIONS

On popular online platforms, predatory groups coerce children into self-harm

Vulnerable teens are blackmailed into degrading and violent acts by abusers who then boast about it

PESC

Screens are poisoning kids' minds



Erica Pandey, author of [Axios Finish Line](#)

NO ONE KNOWS EXACTLY WHAT SOCIAL MEDIA IS DOING TO TEENS

Years and years of research add up to an uncomfortable reality: The connection between social media and mental health is more complicated than it seems.

THE FIFTY

Anxiety and depression is spiking among young people. No one knows why.

...s of children suffering anxiety and depression, stat...
...g new interventions to get to the root of the crisis —
...ey don't know what that is.

We Tested Kids' Smart Toys for Privacy. Here's How You Can, Too

March 28, 2024 11:01 ET

2024 State of the Union

“Pass bipartisan privacy legislation to protect our children online.”

<https://www.nytimes.com/2024/03/08/us/politics/state-of-the-union-transcript-biden.html>

TECH

The AI camera stripping away privacy in the blink of an eye

Artistic project aims to spark debate about AI deepfakes

By Kurt Knutsson, CyberGuy Report · Fox News

≡

THE WALL STREET JOURNAL



For Data-Guzzling AI Companies, the Internet Is Too Small

Firms such as OpenAI and Anthropic are working to find enough information to train next-generation artificial-intelligence models

Data is among several essential AI resources in short supply. EMIL LENDOF/THE WALL STREET JOURNAL, ISTOCK

By Deepa Seetharaman [Follow](#)

April 1, 2024 5:30 am ET

Mar 14, 2024 - Technology

Generative AI's privacy problem



Ina Fried, author of [Axios AI+](#)

≡

WIRED

SECURITY

POLITICS

GEAR

MORE ▾

[GIVE A GIFT](#)

MATT BURGESS

REECE ROGERS

SECURITY

APR 10, 2024 7:38 AM

How to Stop Your Data From Being Used to Train AI

Some companies let you opt out of allowing your content to be used for generative AI. Here's how to take back (at least a little) control from ChatGPT, Google's Gemini, and more.



Access 4
Learning
Community

&

PESC®

Maryland Passes 2 Major Privacy Bills, Despite Tech Industry Pushback

One bill would require apps like Instagram and TikTok to prioritize young people's safety, and the other would restrict the collection of consumer data.



Donate

Who's selling your digital data? California gives you tools to protect your online privacy

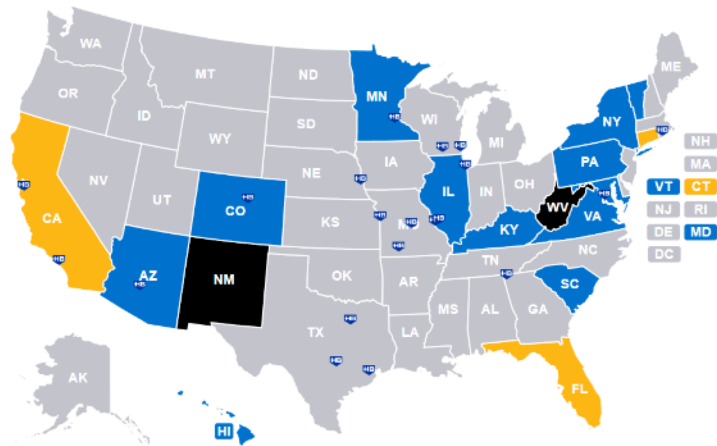


BY KHARI JOHNSON
APRIL 24, 2024



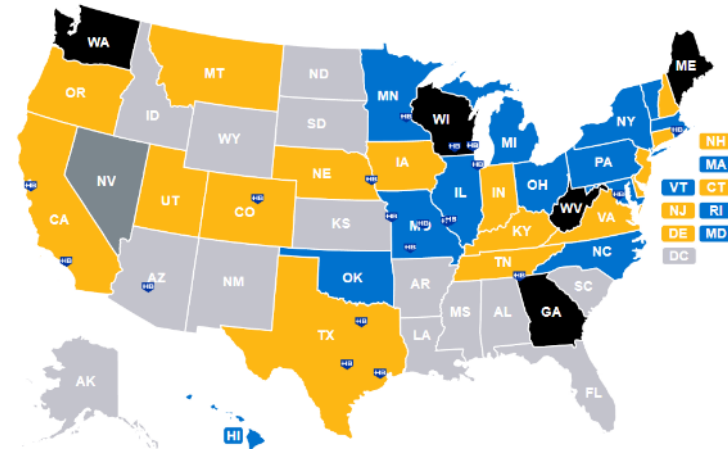
2024 State Children's Privacy Law Tracker

Click the states to view various resources.



2024 State Privacy Law Tracker

Click the states to view various resources.



- Enacted legislation
- Active legislation
- Did not pass in 2024
- Excluded legislation
- Legislature not in session in 2024
- No bill proposed

The Washington Post
Democracy Dies in Darkness

Florida latest to restrict social media for kids as legal battle looms

By [Maria Luisa Paol](#) and [Cristiano Lima-Strong](#)
March 25, 2024 at 4:31 p.m. EDT



Background: COPPA

Examples of When Parental Consent May Not Be Feasible When Sharing Student Data:

Scenario	Explanation
Student Grades	When a student transfers to a new school, their grades must go with them.
Student Medical Information	Requiring parental consent for sharing student medical information may result in students not receiving necessary care in medical emergencies.
Foreign Language App	Requiring parental consent to use a translation app with students may result in teachers not being able to communicate with english language learners.
Approved Apps	Parental consent may not be necessary if a teacher finds educational technology that has been thoroughly vetted for privacy, security, and legal compliance.
Transportation Services	Requiring parental consent to share student addresses with transportation services may result in some students not having access to reliable transportation to and from school.
Free Lunch Data	Information about student eligibility to participate in the National School Lunch Program may need to be shared with school and district staff to facilitate the program. Requiring parental consent to share this information may result in eligible students not receiving this service and going hungry.

COPPA in Schools

- The Children's Online Privacy Protection Act
- Only applies to operators of commercial websites and online services (including mobile apps)
- Site/Service must
 - 1) be directed to children, or
 - 2) have “actual knowledge” that children <13 are using the site for the law to apply
- Companies subject to COPPA must obtain parental consent before **collecting personal information *from* children** but, in some circumstances, the school may consent.

COPPA and Schools: On Shaky Legal Ground?

- In the Statement of Basis and Purpose to the 1999 COPPA Rule, the FTC Commission noted that the Rule “does not preclude schools from acting as intermediaries between operators and schools in the notice and consent process, or from serving as the parents' agent in the process.”
- Stakeholders have been pushing the FTC to codify this guidance for many years. Many commenters in 2019 pushed for the FTC to codify the guidance and align the exception with FERPA’s school-official exception.



COPPA NPRM

COPPA NPRM: Timeline

- **December 20, 2023:** FTC announced a notice of proposed rulemaking (NPRM) for the Children's Online Privacy Protection Rule (COPPA Rule)
- **January 11, 2024:** NPRM published in the Federal Register
- **March 11, 2024:** Comments Due

COPPA NPRM: School Authorization Exception

The NPRM proposes explicitly codifying the existing guidance that permits schools to authorize the collection of personal information for educational purposes.

- Operators would not be required to obtain parental consent where an operator obtains “school authorization for the collection of the child’s personal information for a school-authorized education purpose.”
- Operators are required to have a written agreement with the school that:
 - (i) Indicates the name and title of the person providing authorization and attests that the person has the authority to do so;
 - (ii) Limits the operator’s use and disclosure of the personal information to a school-authorized education purpose only and no other purpose;
 - (iii) Provides that the operator is under the school’s direct control with regard to the use, disclosure, and maintenance of the personal information collected from the child pursuant to school authorization; and
 - (iv) Sets forth the operator’s data retention policy with respect to such information

COPPA NPRM: Impact on AI

- **Secondary Use:** Restrictions on using data for product improvement and development (audio files and education data)
 - Education data cannot be used to develop different products (including data sets to train algorithms)
 - May restrict the ability to create diverse sets of training data and beneficial education innovation
- **Data Retention:** Data cannot be retained indefinitely
 - Implications for AI products built using PII
 - Value of de-identifying data to be used to train algorithms

The logo for PIP (Public Information Privacy) consists of the letters 'P', 'I', and 'P' in a dark purple color, followed by a 'C' in a teal color. The 'I' is replaced by a stylized house icon with a white star on its roof. The background of the letters is a circular graphic with concentric arcs in shades of teal and white.

PIPC

COPPA 2.0

COPPA 2.0: Timeline

- **May 2023:** Reintroduced by Senators Markey and Cassidy
- **July 2023:** Unanimously passed out of Senate Commerce
- **February 15, 2024:**
 - Senators Cantwell and Cruz added as co-sponsors (chair and ranking member of Senate Commerce)
 - Updated text introduced (not yet on congress.gov):
https://www.markey.senate.gov/imo/media/doc/coppa_20billtext.pdf
- **April 9, 2024:** House companion to COPPA 2.0 released:
<https://www.congress.gov/bill/118th-congress/house-bill/7890>
- **May be attached to FAA reauthorization vote**

COPPA 2.0: Major Changes

- **Expands age of COPPA protections to 17**
- Parents own all rights for children under 13, teens (and also parents, in most cases) own rights for teens
- Changes COPPA's knowledge standard to "actual knowledge or knowledge fairly implied on the basis of objective circumstances that a user is a child or teen"
- Does not permit collecting personal information in a manner that violates certain requirements. Operators must:
 - Provide a clear and conspicuous notice of what info is collected, how it is used, disclosure practices, rights and opportunities for parents or teens
 - Obtain consent before using or disclosing info for a purpose that would be a material change from the original purpose for which they obtained consent
- Prohibits individual-specific advertising to children or teens
- Requires data minimization
- Does not allow operators to retain information for longer than reasonably necessary

COPPA 2.0: Major Changes

- **Rights and Opportunities for Parents**

- Describe the specific types of info collected from the child, the method by which the operator obtained the info, and the purposes
- Delete info at any time and refuse to permit further use or future online collection of info from that child
- Opportunity to challenge accuracy and have inaccurate info corrected
- Obtain info collected from the child

- **Rights and Opportunities for Teens**

- Describe the specific types of info collected from the teen, the method by which the operator obtained the info, and the purposes
- Delete info at any time and refuse to permit further use or future online collection of info from that teen
- Opportunity to challenge accuracy and have inaccurate info corrected
- Obtain info collected from the teen

- Requires operators to establish, implement, and maintain reasonable security practices
- Operators cannot discontinue services after a deletion request if they are capable of providing their service without that information.

COPPA 2.0 School Consent Amendment (1/2)

(3) APPLICATION TO OPERATORS ACTING UNDER AGREEMENTS WITH EDUCATIONAL AGENCIES OR INSTITUTIONS.—The regulations may provide that verifiable consent under paragraph (1)(A)(ii) is not required for an operator that is acting under a written agreement with an educational agency or institution (as defined in section 444 of the General Education Provisions Act (commonly known as the ‘Family Educational Rights and Privacy Act of 1974’) (20 U.S.C. 1232g(a)(3)) that, at a minimum, requires the—

(A) operator to—

- (i) limit its collection, use, and disclosure of the personal information from a child or teen to solely educational purposes and for no other commercial purposes;
- (ii) provide the educational agency or institution with a notice of the specific types of personal information the operator will collect from the child or teen, the method by which the operator will obtain the personal information, and the purposes for which the operator will collect, use, disclose, and retain the personal information;
- (iii) provide the educational agency or institution with a link to the operator’s online notice of information practices as required under subsection (b)(1)(A)(i); and “(iv) provide the educational agency or institution, upon request, with a means to review the personal information collected from a child or teen, to prevent further use or maintenance or future collection of personal information from a child or teen, and to delete personal information collected from a child or teen or content or information submitted by a child or teen to the operator’s website, online service, online application, or mobile application;

https://www.markey.senate.gov/imo/media/doc/coppa_20billtext.pdf

COPPA 2.0 School Consent Amendment (2/2)

- (B) representative of the educational agency or institution to acknowledge and agree that they have authority to authorize the collection, use, and disclosure of personal information from children or teens on behalf of the educational agency or institution, along with such authorization, their name, and title at the educational agency or institution; and
- (C) educational agency or institution to—
 - (i) provide on its website a notice that identifies the operator with which it has entered into a written agreement under this subsection and provides a link to the operator's online notice of information practices as required under paragraph (1)(A)(i);
 - (ii) provide the operator's notice regarding its information practices, as required under subparagraph (A)(ii), upon request, to a parent, in the case of a child, or a parent or teen, in the case of a teen; and
 - (iii) upon the request of a parent, in the case of a child, or a parent or teen, in the case of a teen, request the operator provide a means to review the personal information from the child or teen and provide the parent, in the case of a child, or parent or teen, in the case of the teen, a means to review the personal information.

https://www.markey.senate.gov/imo/media/doc/coppa_20billtext.pdf



KOSA: Timeline

- **May 2023:** Reintroduced by Senators Blumenthal and Blackburn
- **July 2023:** Unanimously passed out of Senate Commerce in
- **February 15, 2024:**
 - The bill has 63 co-sponsors
 - Updated text introduced (not yet on congress.gov):
<https://www.blumenthal.senate.gov/imo/media/doc/21424kosabilltext.pdf>
- **April 9, 2024:** House companion to KOSA released (not yet on congress.gov):
<https://bilirakis.house.gov/sites/evo-subsites/bilirakis.house.gov/files/evo-media-document/KOSA%20Language.pdf>
- **May be attached to FAA reauthorization vote**

Key KOSA Provisions

- **Goes up to age 17**
- Covered platforms have a duty of care to “exercise reasonable care in the creation and implementation of any design feature to prevent and mitigate” these harms:
 - Mental health disorders: anxiety, depression, eating disorders, substance use disorders, and suicidal behaviors
 - Patterns of use indicating or encouraging addiction-like behaviors
 - Physical violence, online bullying, and harassment
 - Sexual exploitation and abuse
 - Promotion and marketing of narcotic drugs, tobacco products, gambling, or alcohol
 - “Predatory, unfair, or deceptive marketing practices, or other financial harms”
- Safeguards for minors
- Requires parental tools
- Requires a reporting mechanism
- Disclosure requirements
- Large platforms must provide public reports

Key KOSA Provisions

- Research on social media and minors
- Guidance on market research
- Age verification study and report
- Creates Kids Online Safety Council
- Enforcement by FTC and, in limited circumstances, state AGs
- **Filter Bubble Transparency Act**
 - Added as an amendment at the July 2023 mark-up
 - Applies to all services, not just those being used by minors

Issues with KOSA for Education Stakeholders: High Priority

“Parental Tools” in Edtech

- The “Parental Tools” section could interfere with the contractual relationship between schools and edtech vendors by requiring that parents have access to the settings of edtech used in the classroom.

Explanation

- *Account settings generally include the ability to expand the data collected by a platform (thereby undermining the privacy protections a school may have put into place), to close an account (which can include that child’s progress and the learning goals achieved on a platform), and to delete all of that user’s data (perhaps enabling a parent acting in bad faith to delete their child’s homework).*

Issues with KOSA for Education Stakeholders: High Priority

Student Opt-Outs of Personalized Learning at School

- Students may be able to opt-out of adaptive learning functionalities in technologies that schools routinely use, such as learning management systems and edtech platforms.

Explanation

- *This may allow students to circumvent personalized edtech platforms their teacher is using as part of the core curriculum. If a school chooses to purchase and allow teachers to use a personalized language learning app with their students, the students should not then be allowed to switch to an alternate version of the platform.*



APRA: Overview

- Comprehensive consumer privacy bill incorporating parts of the previously introduced ADPPA and state consumer privacy laws
- Discussion draft released April 5, 2024 by Senator Cantwell and Representative McMorris Rodgers—Chairs of the House and Senate Commerce Committees
- Received broad support in April 17 hearing in the House Committee on Energy and Commerce Innovation, Data and Commerce Subcommittee
 - Many members emphasized the need to include protections for children
- Designed to supersede the patchwork of state laws and establish a unified national privacy standard

APRA: Key Provisions

- **Covered entities:**
 - Similar to some state laws, APRA would apply to nonprofit organizations.
 - Government entities (including school districts) are exempt. Additionally, entities acting as service providers to government entities (such as edtech providers) are also exempt.
- **Data minimization:** Generally, data collection, processing, retention, and transferring is prohibited unless necessary, proportionate, and limited
- **Consumer rights:** access, correction, deletion and portability.
 - Consumers have the right to opt out of targeted advertising and data transfers.
- **Impact assessments:** Large data holders must conduct impact assessments weighing the benefits of data processing against the potential adverse consequences to individual privacy.

APRA: Key Provisions

- **Data security:** Reasonable data security practices, including regular training, are required.
- **Transparency:** Publicly available privacy policies must include specific information detailing data privacy and security practices.
- **Dark patterns:** Prohibition on dark patterns if they interfere with notice, consent, or choice.
- **Algorithms:** Platforms must evaluate most algorithms to reduce the risk of harm.
 - Consumers must be given the right to opt out of using algorithms used to make certain consequential decisions related to housing, employment, education enrollment or opportunity, health care, insurance, credit, or access to places of public accommodation.'

APRA: Children and Students

- There are limited child-specific protections in APRA, which opens up the possibility of tying KOSA or COPPA 2.0 into the bill
- **Covered Entities:** Government entities (including school districts) and entities acting as service providers to government entities (such as edtech providers) are exempt.
- **Sensitive data:** information about minors (under 17) is considered “sensitive data” requiring additional protections.
 - Opt-in consent is required before sensitive data can be transferred
- **Impact Assessments:** Entities conducting impact assessments must describe how they mitigate a variety of harms, including harms to minors.
- **Algorithms:** Consumers must be given the right to opt out of using algorithms used to make certain consequential decisions related to housing, employment, education enrollment or opportunity, health care, insurance, credit, or access to places of public accommodation.



Kids Off Social Media Act & the Eyes on the Board Act

KOSMA

- Combination of Senator Schatz social media bill and Senator Cruz social media ban in schools bill
- Introduced May 1, 2024
- Co-sponsored by Senators Chris Murphy (D-Conn), Katie Britt (R-Ala.), Peter Welch (D-Vt.), Ted Budd (R-N.C.), John Fetterman (D-Pa.), Angus King (I-Maine), and Mark Warner (D-Va.)
- Sets a minimum age of 13 to use social media platforms and prevent social media companies from feeding algorithmically-boosted content to users under the age of 17
- Blocks social media access on school devices and networks (with a broad definition of “social media”)
- May be attached to FAA reauthorization vote

<https://www.commerce.senate.gov/2024/5/sens-cruz-schatz-lead-colleagues-with-new-bill-to-keep-kids-safe-healthy-and-off-social-media>



AI Federal Executive Actions

WH.GOV



OFFICE OF SCIENCE AND TECHNOLOGY POLICY

BLUEPRINT FOR AN AI BILL OF RIGHTS

MAKING AUTOMATED SYSTEMS WORK FOR
THE AMERICAN PEOPLE



Safe and Effective Systems



Algorithmic Discrimination
Protections



Notice and Explanation



Data Privacy



Human Alternatives,
Consideration, and Fallback

<https://www.whitehouse.gov/ostp/ai-bill-of-rights/>

AI Executive Order

“To help ensure the responsible development and deployment of AI in the education sector, the Secretary of Education shall, within 365 days of the date of this order, develop resources, policies, and guidance regarding AI... include the development of an “AI toolkit” for education leaders implementing recommendations from the Department of Education’s AI and the Future of Teaching and Learning report, including appropriate human review of AI decisions, designing AI systems to enhance trust and safety and align with privacy-related laws and regulations in the educational context, and developing education-specific guardrails.”

[Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence](#)

AI Executive Order

“Independent regulatory agencies are encouraged, as they deem appropriate, to consider using their full range of authorities to protect American consumers from fraud, discrimination, and threats to privacy and to address other risks that may arise from the use of AI, including risks to financial stability, and to consider rulemaking, as well as emphasizing or clarifying where existing regulations and guidance apply to AI, including clarifying the responsibility of regulated entities to conduct due diligence on and monitor any third-party AI services they use, and emphasizing or clarifying requirements and expectations related to the transparency of AI models and regulated entities’ ability to explain their use of AI models.”

[Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence](#)

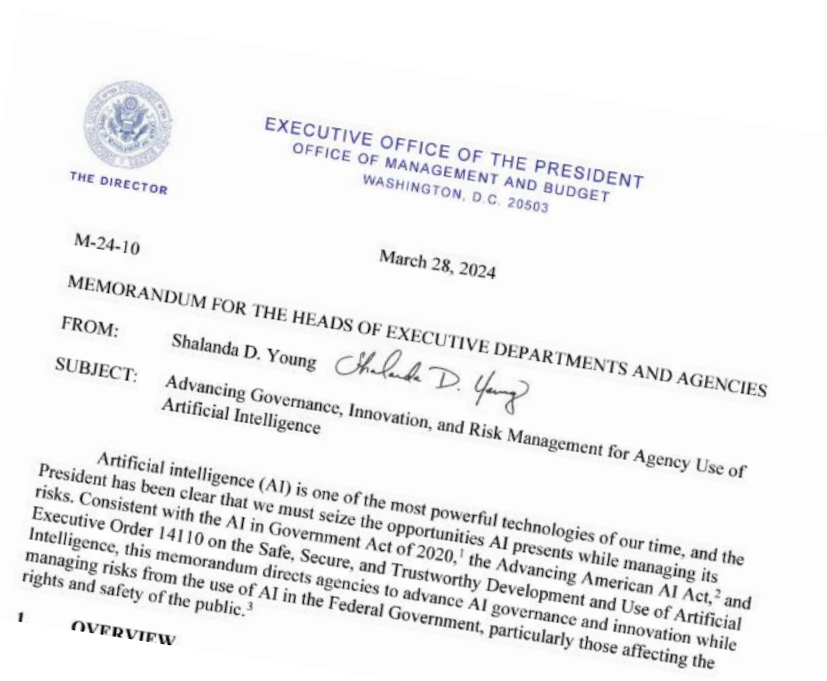
Federal Actions Related to AI & Data Sharing

Oct 2022	White House: Blueprint for an AI Bill of Rights
Jan 2023	NIST: AI Risk Management Framework (AI RMF 1.0)
Feb 2023	White House: Executive Order to Strengthen Racial Equity and Support for Underserved Communities Across the Federal Government
April 2023	FTC, DOJ, CFPB & EEOC: Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems
April 2023	NTIA: AI Accountability Policy Request for Comment
May 2023	USED Report: Artificial Intelligence and the Future of Teaching and Learning
May 2023	OSTP RFI: National Priorities for Artificial Intelligence
July 2023	White House: Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI
July 2023	Workforce RFI: Federal-State Unemployment Compensation (UC) Program; Confidentiality and Disclosure of State UC Information
Oct 2023	White House: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
Nov 2023	OMB: Implementation Guidance Following President Biden's Executive Order on Artificial Intelligence

The OMB Memorandum (March 28, 2024)

Goals

- Strengthening AI Governance
- Advancing Responsible AI Innovation
- Managing Risks from the Use of AI



Strengthening AI Governance

- Designating Chief AI Officers
- Convening Agency AI Governance Bodies
- Compliance Plans
- AI Use Case Inventories

Advancing Responsible AI Innovation

- AI Strategies
- Removing Barriers to the Responsible Use of AI
- AI Talent
- AI Sharing and Collaboration
- Harmonization of Artificial Intelligence Requirements

Managing Risks from the Use of AI

- Implementation of Risk Management Practices and Termination of Non-Compliant AI.
- Determining Which Artificial Intelligence Is Presumed to Be Safety-Impacting or Rights-Impacting
- Minimum Practices for Safety-Impacting and Rights-Impacting Artificial Intelligence

Purposes Presumed to Be Rights-Impacting

In education contexts, detecting student cheating or plagiarism; influencing admissions processes; monitoring students online or in virtual-reality; projecting student progress or outcomes; recommending disciplinary interventions; determining access to educational resources or programs; determining eligibility for student aid or Federal education; or facilitating surveillance (whether online or in-person);

Minimum Practices for Either Safety-Impacting or Rights-Impacting AI

- Complete an AI impact assessment. Agencies must document (at minimum):
 - The intended purpose for the AI and its expected benefit
 - The potential risks of using AI
 - The quality and appropriateness of the relevant data
- Test the AI for performance in a real-world context
- Independently evaluate the AI
- Conduct ongoing monitoring

Minimum Practices for Either Safety-Impacting or Rights-Impacting AI

- Regularly evaluate risks from the use of AI
- Mitigate emerging risks to rights and safety
- Ensure adequate human training and assessment
- Provide additional human oversight, intervention, and accountability as part of decisions or actions that could result in a significant impact on rights or safety
- Provide public notice and plain-language documentation.

Minimum Practices *Before* Initiating Use of New or Existing Rights-Impacting AI

- Identify and assess AI's impact on equity and fairness, and mitigate algorithmic discrimination when it is present.
- Consult and incorporate feedback from affected communities and the public
- Conduct ongoing monitoring and mitigation for AI-enabled discrimination
- Notify negatively affected individuals
- Maintain human consideration and remedy processes
- Maintain options to opt-out for AI-enabled decisions

Managing Risks in Federal Procurement of AI

- Aligning with the Law
- Transparency and Performance Improvement
- Promoting Competition in Procurement of AI
- Maximizing the Value of Data for AI
- Overfitting to Known Test Data
- Responsible Procurement of AI for Biometric Identification
- Responsibly Procuring Generative AI
- Assessing for Environmental Efficiency and Sustainability



State Laws

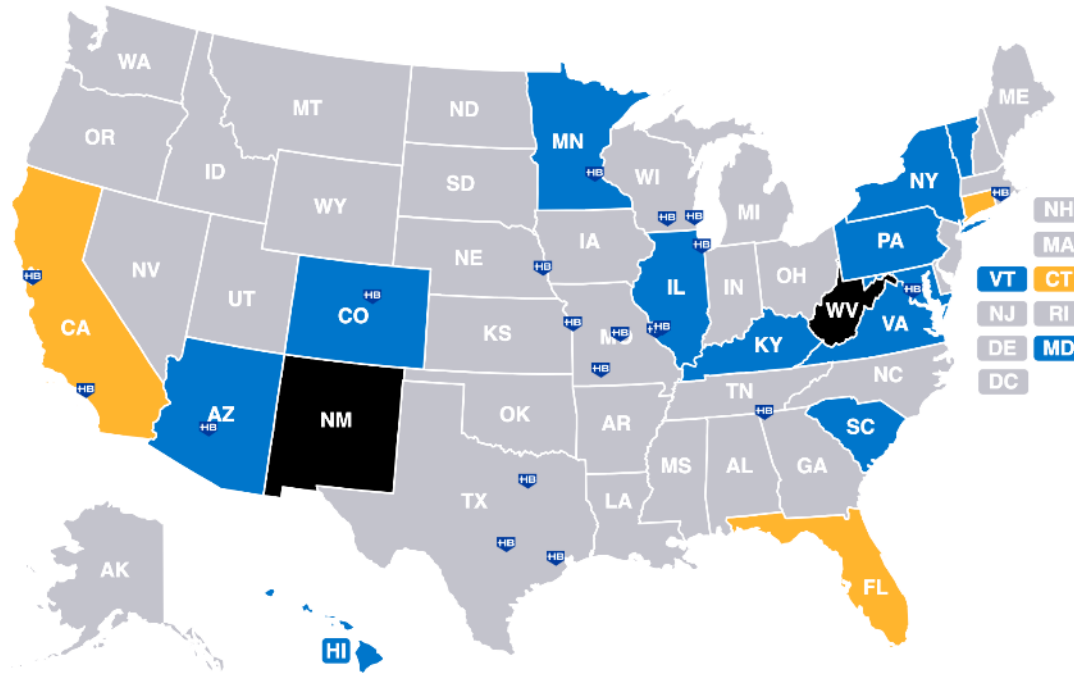
Laws We're Watching

- Utah HB 182 passed, which amends student survey requirements
- West Virginia SB 466 passed, requiring “the board of education to create a safety while access to social networking sites” and other provisions.
- Indiana HB 1243 passed, requiring recommendations for reducing amount of redundant data districts must submit to state agencies and create a data inventory
- New Hampshire’s student data minimization bill, HB 1469
- New Hampshire student privacy bill HB 1695, which prohibits transfer of student PII without written consent.

2024 State Child Privacy Law Legislation Tracker

2024 State Children's Privacy Law Tracker

Click the states to view various resources.



Questions?

amelia@publicinterestprivacy.org



PUBLIC
INTEREST
PRIVACY
CENTER