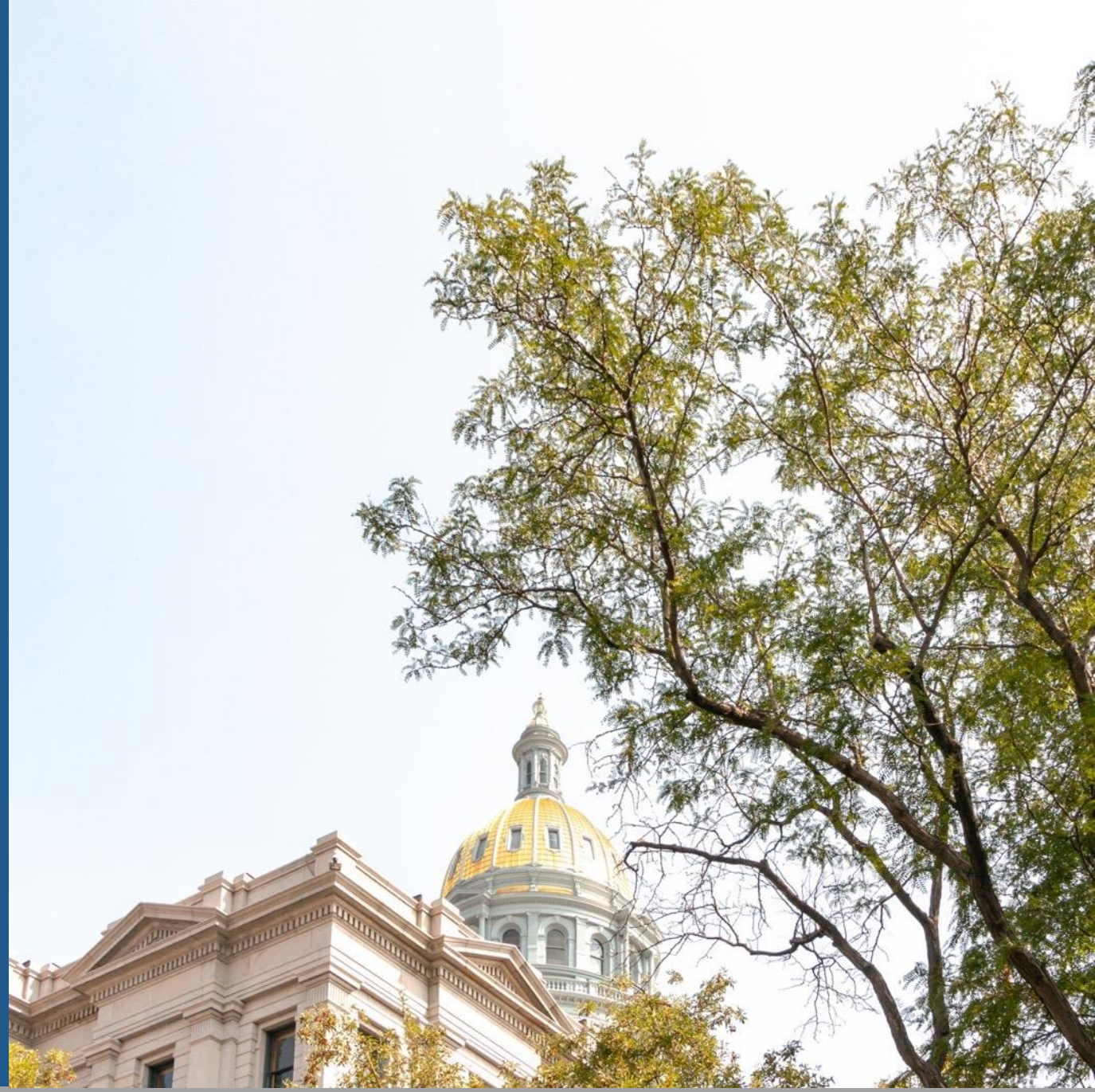
Federal Legislative Update

Meeting of the NCSL Task Force on Artificial Intelligence, Cybersecurity and Privacy

May 17, 2024
Quebec City

Barrie Tabin, NCSL, legislative director, barrie.tabin@ncsl.org

Susan Parnas Frederick, senior federal affairs counsel, susan.frederick@ncsl.org



Agenda

- Privacy
  - American Privacy Rights Act
  - Children and Teens Online Privacy Protection Act (COPPA 2.0)
  - Kids Online Safety Act
  - TikTok Ban
- Artificial Intelligence
- Cybersecurity
- Q & A

American Privacy Rights Act

- Discussion draft legislation co-authored by Senator Maria Cantwell (D-WA), Chair of the Senate Committee on Commerce, Science and Transportation, and Cathy McMorris Rodgers (R-WA), Chair of the House Committee on Energy and Commerce.
- Draft has bipartisan, bicameral support, although some opposition.
- Draft is a comprehensive federal framework for how companies collect, share and use people's information that preempts most state privacy laws; some carve outs for state consumer protection, health and biometric privacy laws outside of the comprehensive privacy laws.
- Preemption could raise issues for NCSL and other organizations representing states and local governments.
- Includes controversial private right of action, which allows individuals to sue companies for privacy violations.

American Privacy Rights Act - Definitions

- Covered entities - any entity that determines the purpose and means of collecting, processing, retaining, or transferring covered data and is subject to the Federal Trade Commission Act, including common carriers and most nonprofits. Service providers that process covered data on behalf of, and at the direction of, a covered entity.

- Covered data - information that identifies or is linked or reasonably linkable to an individual or device (not including employee data or publicly available information).

- Sensitive covered data – includes government identifiers; health information; biometric information; genetic information; financial account and payment data; precise geolocation information; log-in credentials; private communications; information revealing sexual behavior; calendar or address book data, phone logs, photos and recordings for private use; any medium showing a naked or private area of an individual; video programming viewing information; an individual's race, ethnicity, national origin, religion, or sex, in a manner inconsistent with a reasonable expectation of disclosure; online activities over time and across third party websites, or over time on a high-impact social media site; information about a covered minor; and other data as defined by the FTC.

- Exemptions – all levels of government, small businesses, some others.

American Privacy Rights Act - New Requirements on Covered Entities and Service Providers

- Sets standard for data minimization that would allow companies to collect and use data only for necessary and limited purposes for providing a service or product.
- Requires covered entities to comply with opt-out and consent requirements.
- For most covered data, covered entities need to give individuals a chance to opt out of the transfer of their data or the use of their data for targeted advertising.
- But for sensitive data, covered entities need to obtain an individual's affirmative, express consent before transferring that data.
- Different standard than many state models, where companies can collect and use data for purposes disclosed in privacy policies, and assumes users consent to information being collected unless they specifically opt out.

American Privacy Rights Act - New Requirements on Covered Entities and Service Providers, continued

- Allows consumers to request access to their data, as well as the ability to correct, export or delete data.
- Must make publicly available data privacy and security practices, including how consumers can opt out of collection (transparency).
- Sets limits on artificial intelligence by allowing people to opt out of algorithms used for decisions related to housing, employment, financial and health care opportunities, as well as targeted advertising.
- Large data holders – need to conduct algorithm impact assessments and privacy impact assessments and make annual certifications to the FTC regarding compliance.
- Data brokers - required to register with FTC. Agency to establish a central data broker registry with a "Do Not Collect" mechanism allowing individuals to opt out of data brokers' collection of their covered data. Data brokers need to develop public facing websites with a link to the FTC's data broker registry.

American Privacy Rights Act - Enforcement

- Gives FTC authority to enforce violations, including civil penalties and injunctive relief.
- Provides FTC with rulemaking authority (e.g., defining categories of sensitive covered data, how covered entities might comply with data minimization, and algorithm impact assessments).
- Directs FTC to create a new bureau to carry out new responsibilities.
- Authorizes state attorneys general to bring civil actions on behalf of their states' residents.
- Private Right of Action.

Children and Teens Online Privacy Protection Act (COPPA 2.0)
(S. 1418)

- Cosponsored by Sens. Ed Markey (D-MA) and Bill Cassidy (R-LA) and Reps. Tim Walberg (R-MI) and Kathy Castor (D-FL).
- Amends COPPA of 1998 to strengthen protections relating to the online collection, use, and disclosure of personal information of children and teens, among other things.
- Most material change proposed in COPPA 2.0 is to cover teens age 13 to age 16 by prohibiting internet companies from collecting personal information from users who are 13 to 16 without their consent.
- Bans targeted advertising to kids and teens and requires direct notice if data is being stored or transferred outside the U.S.

- Creates an eraser mechanism for parents and kids by requiring companies to permit users to delete information when technologically feasible.
- FTC & State AG enforcement authority
- Preempts state laws that conflict with COPPA 2.0, while permitting state laws that offer greater protections for kids and teens.
- No private right of action.
- FTC issued a rulemaking to expand COPPA's privacy protections early this year, moving closer to a COPPA 2.0.

Kids Online Safety Act (S. 1409) – Sens. Richard Blumenthal (D-CT) and Marsha Blackburn (R-TN) & Reps. Gus Bilirakis (R-FL) and Kathy Castor (D-FL)

Application

- Covered platform means an online platform, online video game, messaging application, or video streaming service that connects to the internet and that is used, or is reasonably likely to be used, by a minor.
- Exemptions - internet service providers, email services, educational institutions, some others.

Duty of Care

- A covered platform must exercise reasonable care in the creation and implementation of any design feature to prevent and mitigate harms to minors.
- Requires independent audits and research on how social media impacts the mental health and well-being of kids and teens.

Other Safeguards

- Safeguard controls to parents and minors to limit others' ability to communicate with the minor, to prevent others from viewing the minor's personal data, to limit features that increase time spent on the platform and to delete the minor's account or any associated personal data.
- Strongest privacy settings automatically required for kids under 13.

Preemption

- Preempts state laws that conflict with KOSA, while permitting state laws that offer greater protections for kids.

Enforcement

- FTC
- Attorneys General
- No private right of action

New Law That Could Ban TikTok

- ***Protecting Americans from Foreign Adversary Controlled Applications Act*** prohibits the distribution and maintenance of apps controlled by foreign adversaries that pose a clear threat to national security and requires app owners to stop their operations or divest themselves of their U.S.-based operations.
- In the case of TikTok, Beijing's-based ByteDance would need to divest itself of control of the app within the year or be banned from U.S. app stores and hosting services. Congress approved the law as part of a broader foreign aid package for Ukraine, Israel, and Taiwan. (HR 815).
- TikTok has filed a lawsuit challenging the law arguing that it violates the first amendment's freedom of speech.
- As part of the same package, Congress also passed and the President signed ***Protecting Americans' Data from Foreign Adversaries Act,*** which prevents data brokers from selling sensitive information to China, Russia or other "foreign adversaries."

Artificial Intelligence

- Senate AI Working Group created in May 2023 including Sens. Chuck Schumer (D-NY), Todd Young (R-IN), Martin Heinrich (D-NM) and Michael Rounds (R-SD).
- The Senate AI Working Group released its AI Roadmap this week. Individual topic bills rather than one comprehensive bill.
- In early February House leadership appointed a 24-member bipartisan Task Force on AI chaired by Reps. Jay Obernolte (R-CA) and Ted Lieu (D-CA).
- National Science Foundation launched the National Artificial Intelligence Research Resource (NAIRR), a two-year pilot program to provide access to advanced computing, datasets, models, software, training and user support to U.S.-based researchers and educators.
- FTC finalized its new rule prohibiting the use of artificial intelligence to impersonate governments and businesses.
- FCC issued a declaratory ruling clarifying telemarketing calls using an artificial or prerecorded voice simulated or generated through AI technology can be made only with the prior express written consent of the called party.

Artificial Intelligence -Senate AI Working Group Roadmap Highlights

- Supporting Innovation
  - Appropriating $32 billion a year for nondefense AI innovation (recommended by National Security Commission on AI).
  - Authorizing the National AI Research Resource (NAIRR) by passing the CREATE AI Act (S. 2714) and funding it as part of the cross-government AI initiative.
  - Focus on startups to compete in the AI marketplace, including legislation to support the dissemination of best practices to incentivize states and localities to invest in similar opportunities as provided by the NAIRR.

- AI and the Workforce
  - Development of legislation related to training, retraining, and upskilling the private sector workforce to successfully participate in an AI-enabled economy.
  - Consider impact of AI on long-term future of work.
  - Consider legislation to improve the U.S. immigration system for high-skilled STEM workers.
  - Consider Workforce Data for Analyzing and Tracking Automation Act (S. 2138) to authorize the Bureau of Labor Statistics to record the effect of automation on the workforce and measure those trends over time, including job displacement, the number of new jobs created, and the shifting in demand skills.

Artificial Intelligence -Senate AI Working Group Roadmap Highlights, continued

- High Impact Uses of AI
  - AI use cases should not directly or inadvertently infringe on constitutional rights, imperil public safety, or violate existing antidiscrimination laws.
  - Encourages Senate committees to explore how AI may affect some parts of our population differently, both positively and negatively.
  - Specifically discussing developing AI legislation related to critical infrastructure, financial services, housing, to address online child sexual abuse material, to protect children from potential AI-powered harms online, to deter the use of fraud, for testing and deployment of autonomous vehicles, and for use in health care with measures to protect patients.

- Elections and Democracy
  - Encourages Senate committees, AI developers and deployers to advance effective watermarking and digital content provenance as it relates to AI-generated or AI-augmented election content.

Artificial Intelligence -Senate AI Working Group Roadmap Highlights, continued

- Privacy and Liability
  - Committees should consider whether there is a need for additional standards, or clarity around existing standards, to hold AI developers and deployers accountable if their products or actions cause harm to consumers, or to hold end users accountable if their actions cause harm, as well as how to enforce any liability standards.
  - Strong comprehensive federal data privacy law to protect personal information.

- Transparency, Explainability, Intellectual Property, and Copyright
  - Consider legislation to establish an approach to public-facing transparency requirements for AI systems, including best practices for when AI deployers should disclose that their products use AI (for example, data training sets, software products or use of likeness, name, voice).
  - Consider legislation aimed at establishing a public awareness and education campaign to provide information regarding the benefits, risks, and prevalence of AI in the lives of individuals in the U.S.

Artificial Intelligence -Senate AI Working Group Roadmap Highlights, continued

- Safeguarding Against AI Risks
  - AI Working Group encourages the relevant committees to consider a resilient risk regime that focuses on the capabilities of AI systems, protects proprietary information, and allows for continued AI innovation in the U.S.
  - Develop framework that specifies what circumstances would warrant a requirement of pre-deployment evaluation of AI models.
  - Develop legislation aimed at advancing R&D efforts that address risks posed by various AI system capabilities, including by equipping AI developers, deployers, and users with the knowledge and tools necessary to identify, assess, and effectively manage those risks.

Artificial Intelligence -Senate AI Working Group Roadmap Highlights, continued

- National Security
  - The AI Working Group will collaborate with committees and executive branch agencies to stay informed about the research areas and capabilities of U.S. adversaries.
  - The development of career pathways and training programs for digital engineering in AI and resources for a strong digital workforce within the armed services.
  - Relevant committees, in collaboration with the private sector, should continue to address and mitigate the rising energy demand of AI systems to ensure the U.S. can remain competitive and keep energy costs down.

Cyber Incident Reporting for Critical Infrastructure Act of 2002 (CIRCIA) NPRM

- Tasks CISA with developing reporting requirements
- Comments due July 3 and finalized October 2025
- 16 Critical infrastructure entities are covered

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Government Facilities Sector – must meet 1 of 3 criteria:

Population of 50,000 or more

State and local education agency and some colleges

Involved in elections e.g. voter registration databases, voting systems, “and communication technologies used to report, display, validate, or finalize election results."

What's the Big Deal?

- **No preemption of state authority to regulate cyber**
- **States are exempt from enforcement provisions of CIRCIA**

BUT…

REPORTING REQUIREMENTS

CISA estimates at least 210,000 CIRCIA reports, and they are NOT worried about getting too many

24-hour reporting requirement for ransomware payments

72-hour reporting requirement for substantial cyber incidents as defined by CISA

Substantial means one of the following has happened:

- A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
- A serious impact on the safety and resiliency of a covered entity's operational systems and processes;
- A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; or
- Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise.

Substantial cyber incident does NOT include:

- Lawfully authorized activities of a U.S., state, or local government entity;
  - warrant or other judicial process
- Incidents perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system
  - Penetration testing that goes awry and causes disruption

Incidents That Likely Qualify as "Substantial"

- DDOS attack that renders a covered entity's service unavailable for a long time
- Cyber incident that results in encryption of core services
- Cyber incident that significantly increases the potential for the release of a hazardous substance
- Cyber incident that disrupts or corrupts the 911 network
- Unauthorized access to a business system using compromised credentials from a managed service provider or from a tampered software update

Incidents Likely Not Qualifying as "Substantial"

- Minor cyber disruptions causing brief lapses in services
- Malicious software download that is caught by anti-virus software and quarantined

Records Preservation

- 2 years from last report
- For ransomware – communications with threat actor and details of any payments
- States and other covered entities not required to create any data or records it doesn't already have

Federalism Considerations

- CISA does not believe this NPRM preempts any existing state laws but wants to know whether that is correct.
- CIRCIA exempts reports from disclosure under state and local freedom of information laws (same as federal FOIA)

Questions & Answers

Stay Connected

- Learn about NCSL training
- Subscribe to policy newsletters
- Read State Legislatures magazine
- Listen to an NCSL podcast
- Watch recorded policy webinars and training sessions
- Attend a meeting or training
- Follow @NCSLorg on social media

2024 Legislative Summit

NCSL LEGISLATIVE SUMMIT 24 LOUISVILLE | KY

Aug. 5-7, 2024