Federal AI Legislation

An Analysis of Proposals from the 117th Congress Relevant to Generative AI tools

Anna Lenhart, Knight Policy Fellow
June, 2023

Institute for Data,
Democracy & Politics
THE GEORGE WASHINGTON UNIVERSITY

ACKNOWLEDGEMENTS

Thank you to B Cavello, Former TechCongress Fellow and Eleanor Tursman, Former TechCongress Fellow for initial support on the crowdsourced list. The list has also benefited from the insights of several hill staffers (current and former) who are doing the hard work of writing, researching and socializing these proposals. Lastly, thank you to Alyse Mier and the Institute for Data, Democracy & Politics (IDDP) team.

IDDP launched in 2019 with the support of the John S. and James L. Knight Foundation. IDDP's mission is to help the public, journalists and policymakers understand digital media's influence on public dialogue and opinion, and to develop sound solutions to disinformation and other ills that arise in these spaces.

INTRODUCTION

The following report is an analysis based on a list of "federal legislative proposals pertaining to generative AI" first circulated as a Google Document on April 12, 2023. In the weeks that followed current and former hill staffers that cover technology policy contributed to the list. This report aims to glean and summarize trends in recent proposals addressing risks from generative AI tools, while highlighting areas for further considerations.

The list began as a response to a narrative perpetuated by the media suggesting that Congress has yet to propose legislation "to protect individuals or thwart the development of A.I.'s potentially dangerous aspects."[1] This narrative fails to recognize the wide range of proposals written that aim to govern the processing of data, including the generative AI tools currently capturing the nation's imagination.

For the sake of this analysis, I considered the definition of generative AI to be "a subset of artificial intelligence algorithms that are used to create new content based on patterns in large amounts of existing content" including chatbots such as ChatGPT, video synthesis and image generators such as DALL-E, both as standalone tools or integrated into information technology (search engines, email, productivity tools, etc). [2] A primary part of this analysis is understanding which definitions of covered platforms/covered entities include generative AI tools. The bills included for analysis represent "proposals" from the 117th Congress, as they did not make it to the President's desk and have not been subject to legal interpretations in a court of law. The interpretations below represent best understanding based on congressional intent. Each section includes a summary of the proposals and considerations for Congress as bills are considered for reintroduction.

To reasonably scope the analysis, I focused on a specific subset of risks posed by generative AI tools: opacity and market power, discrimination, disclosure of personal information, manipulation, creation and proliferation of harmful content. There are several other policy portfolios in Congress that address concerns from generative AI that fell outside the scope of this analysis (intellectual property, semiconductor supply chain, media literacy, financial services, workforce, national security).

Additionally, I limited the analysis to bills introduced during the 117th Congress (2021-2022) at the federal level. Fortunately other organizations have trackers for international and state legislation, as seen on the next page.

---

[1] Kang, C., & Satariano, A. (2023, March 3). As A.I. Booms, Lawmakers Struggle to Understand the Technology. The New York Times. https://www.nytimes.com/2023/03/03/technology/artificial-intelligence-regulation-congress.html

[2] Cavello, B., & Tursman, E. (2023). Generative AI primer for journalists. Aspen Digital. https://techprimers.aspendigital.org/

INTRODUCTION

I attempted to order the bills based on relevance to generative AI tools and amount of congressional attention (hearings, markups, etc). **The bills listed do not represent endorsement from the authors or the Institute for Data, Democracy & Politics at George Washington University.**

Other organizations have been tracking developments regarding AI at the international and state level. To understand the implications for generative AI, I suggest interrogating the definitions using an approach similar to the analysis that follows.

Digital Policy Alert

Tracks tech policy development globally including "ML and AI Development.

Epic.org

The State of State AI Policy

U.S. Chamber of Commerce

State-by-State Artificial Intelligence Legislation Tracker

BCLP 2023

State-by-State Artificial Intelligence Legislation Snapshot

Definitions in legislative text often include cross references and carve outs. I focused on key definitions in the analysis below, but termtabs.com, created by Marissa Gerchick, is an interactive tool for more deeply understanding these definitions. I was grateful to have the termstabs.com tool available for this analysis.

TABLE OF CONTENTS

CREATION OF NEW AGENCIES

Challenges bills aim to address:

New ways to collect, share, and process data are continually evolving. Without government capacity, technical expertise and the ability to clarify and update rules as needed, we risk industry and market values wholly shaping technology (including generative AI tools).

Progress made by existing proposals:

The United States has a long history of regulating innovative technologies ranging from airplanes to medical devices to advanced energy generation through dedicated regulatory agencies. Members of Congress have proposed a variety of regulatory agencies solely dedicated to the digital market (including generative AI tools). These proposals include two notable features: a) the ability to hire technical staff and b) the ability to promulgate rules using the Administrative Procedure Act (APA), colloquially referred to as notice-and-comment. Each proposal differs in scope and structure.

Digital Platform Commission Act (H.R.7858) (S.4201)

Rep. (Now Sen.) Welch (D-VT), Sen. Bennet (D-CO)

Creates a new agency with commissioners to oversee digital platforms where *"digital platform means an online service that serves as an intermediary facilitating interactions—(i) between users; and(ii) between users and—(I) entities offering goods and services through the online service; or (II) the online service with respect to goods and services offered directly by the online service.*

The Agency can promulgate rules to protect consumers and initiate investigations.

Data Protection Act (S.2134)

Sen. Gillibrand (D-NY), Sen. Brown (D-OH)

Creates a director led agency with a range of rulemaking authority. The bill specifically denotes *"high risk data practices"* as including *"a systematic processing of publicly accessible data on a large scale."*

Online Privacy Act (H.R. 6027)

Rep. Eshoo (D-CA), Rep. Lofgren (D-CA)

Establishes a director led *Digital Privacy Agency* with a range of rulemaking authority related to data protections.

Covered Entities *"shall not process personal information or contents of communication for advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for employment, finance, health care, credit, insurance, housing, or education opportunities in a manner that discriminates against or otherwise makes opportunities unavailable on the basis of an individual's protected class status."*

The definition of personal information includes a carve out for "publicly available information"

Considerations for lawmakers moving forward:

What is the best structure for a new agency (independent agency led by commission or federal executive department led by a secretary)? How broad should the jurisdiction be? Should the agency focus on high risk or otherwise significant platforms?

Existing agencies already oversee AI tools (i.e. medical devices at the Food and Drug Administration (FDA), driver assistance at National Highway Traffic Safety Administration (NHTSA), deceptive forms of commerce at the Federal Trade Commission (FTC), etc). Similarly, several agencies can already enforce existing laws pertaining to generative AI tools. How would a new agency impact the purview of existing agencies? How will agencies interact or share information? How will the subject matter expertise that currently exists within sector-based agencies be respected and integrated?

Any new agency will only ever be as impactful as the laws it is directed to guide and enforce, the bills listed below vary in how much direction they provide a new agency. The subsequent sections dive into proposals focused on new laws (requirements and prohibitions) for online platforms.

RISK ASSESSMENT & TRANSPARENCY

Challenges bills aim to address:

Generative AI tools, like many data processing systems are often described as a "black box" highlighting that it is difficult to understand why the tools respond in specific ways and how they were designed. As the public, experts and governments consider a wide range of risks to consumers (discrimination, privacy, manipulation of political discourse and elections, public health, mental health, etc) in various contexts, they lack critical information. Opacity only further concentrates the decision-making power of companies creating such tools.

There is uncertainty regarding how companies are protecting consumers and considering the wider impacts of their products on society.

As consumers interact with generative AI tools, they may not understand the use limitations and risks.

Progress made by existing proposals:

Existing proposals mandate disclosures aimed at providing more information to the public (users, parents), researchers/auditors, regulators and combinations thereof. Disclosures include labels, reports, data sets, and risk assessments. Transparency, when implemented effectively, can allow for informed consumer choice (users and advertisers), shift incentives within companies to invest in better safety practices and responsible product design, and provide information needed to inform policy making. Transparency proposals can also create paths for independent actors (journalists, civil society) to be a check on the promises companies make.

As you will see from the proposals below, transparency bills trend towards two categories: 1) assessments and disclosures pertaining to automated decision systems, algorithms, or online platforms broadly and 2) assessment and disclosures pertaining to social media platforms. In some cases the covered platform definition is based on Interactive Computer Services (ICS) as defined in Section 230 of the Communications Decency Act complicating the analysis of the latter set of proposals. The circumstances under which a generative AI tool may be considered an ICS will evolve as the court reviews cases. Despite this definitional ambiguity, this latter set of proposals would cover platforms that embed generative AI tools and disseminate content created by generative AI tools.

Both sets of proposals in this category point towards mandating that platforms put in place and consider the safety/ risks of their products and disclose information related to those processes. Many of the ideas included in this section are also referenced in the data protection bills listed in the following section including limits on discriminatory data processing, mandates for impact assessments and clear privacy policies.

Algorithm Accountability Act (H.R.6580) (S.3572)

Rep. Clarke (D-NY), Sen. Wyden (D-OR), Sen. Booker (D-NJ)

Requires generative AI tools that are involved in “critical decisions” (eg. education, employment, essential utilities, family planning, financial services, healthcare, housing, legal service, etc) to assess impacts both prior and after deployment by a covered entity.

Requirements for assessments are incredibly detailed and broadly require covered entities to:

"*In the case of a new augmented critical decision process, evaluate any previously existing critical decision-making process used for the same critical decision prior to the deployment of the new augmented critical decision process, along with any related documentation or information;*

Identify and describe any consultation with relevant stakeholders as required
In accordance with any relevant National Institute of Standards and Technology or other Federal Government best practices and standards, perform ongoing testing and evaluation of the privacy risks and privacy-enhancing measures of the automated decision system or augmented critical decision process;

Perform ongoing testing and evaluation of the current and historical performance of the automated decision system or augmented critical decision process using measures such as benchmarking datasets, representative examples from the covered entity’s historical data, and other standards…

Support and perform ongoing training and education for all relevant employees, contractors, or other agents regarding any documented material negative impacts on consumers from similar automated decision systems or augmented critical decision processes and any improved methods of developing or performing an impact assessment for such system or process based on industry best practices and relevant proposals and publications from experts, such as advocates, journalists, and academics;

(Continued on next page)

Assess the need for and possible development of any guard rail for or limitation on certain uses or applications of the automated decision system or augmented critical decision process, including whether such uses or applications ought to be prohibited or otherwise limited through any terms of use, licensing agreement, or other legal agreement between entities;

Maintain and keep updated documentation of any data or other input information used to develop, test, maintain, or update the automated decision system or augmented critical decision process;

Evaluate the rights of consumers;

Identify any likely material negative impact of the automated decision system or augmented critical decision process on consumers and assess any applicable mitigation strategy;

Describe any ongoing documentation of the development and deployment process with respect to the automated decision system or augmented critical decision process Identify any capabilities, tools, standards, datasets, security protocols, improvements to stakeholder engagement, or other resources that may be necessary or beneficial to improving the automated decision system, augmented critical decision process, or the impact assessment of such system or process;

Document any of the impact assessment requirements described in paragraphs [above] that were attempted but were not possible to comply with because they were infeasible, as well as the corresponding rationale for not being able to comply with such requirements"

DEEP FAKES Accountability Act (H.R.2395)

Rep. Clarke (D-NY)

Requires *"any person who, using any means or facility of interstate or foreign commerce, produces an advanced technological false personation record with the intent to distribute such record over the internet or knowledge that such record shall be so distributed"* to embed a *"digital watermark"* and additional disclosures.

Additionally, *"any manufacturer of software, who in the course of conducting such business produces software, in or affecting interstate or foreign commerce, which such manufacturer reasonably believes, in the context of their intended distribution of the product, will be used to produce deep fakes…shall ensure such software has the technical capability to insert watermarks and disclosures of the nature described in such section into such deep fakes"*

FTC Whistleblower Act (H.R.6093)

Rep. Schakowsky (D-IL), Rep. Trahan (D-MA)

Allows for whistleblowers within companies building generative AI to bring information to the FTC when they notice illegal activity within the FTC's jurisdiction (structured similarly to other whistleblower program).

Terms-of-service Labeling, Design, and Readability Act or the TLDR Act (H.R.6407) (S.3501)

Rep. Trahan (D-MA), Sen. Cassidy (R-LA), Sen. Lujan (D-MN)

Mandates summary statements and structured data formats for terms of service. To the extent generative AI tools have privacy statements, or terms pertaining to acceptable use those would be structured and easy to read and compare.

Kids Online Safety Act (KOSA) (S.3663)

Sen. Blumenthal (D-CT), Sen. Blackburn (R-TN)

Requires platforms to disclose clear terms (for minors and parents), descriptions of algorithm use, advertising labels, transparency reports, systemic risk assessments and mitigation (description of safeguards), and third-party audit of these reports.

The text also creates a program for eligible researchers to get access to platform (generative AI tools) data to study harms to minors.

The provisions in this bill are tied to covered platforms where the term *"covered platform means a social media service, social network, video game, messaging application, video streaming service, educational service, or an online platform that connects to the internet and that is used, or is reasonably likely to be used, by a minor."* This definition will likely cover generative AI tools.

"An online platform that connects to the internet" would likely cover most generative AI tools.

Digital Services Oversight and Safety Act (H.R. 6796)

Rep. Trahan (D-MA), Rep. Schiff (D-CA), Rep. Casten (D-IL)

Outlines a comprehensive set of disclosures for interactive computer services (ICS).

[If a generative AI tool is not considered an ICS]

Sec 7 mandates that “large covered platforms” (aka large social media sites) conduct comprehensive risk assessment and risk mitigation audits, meaning social media companies would need to assess and mitigate (subject to audit) systemic risks including:

"*(A) The dissemination of illegal content or illegal goods, or the facilitation of illegal activity, through a hosting service.*

(B) Discrimination against individuals based on race, color, religion or creed, national origin or ancestry, sex (including gender, pregnancy status, sexual orientation, or gender identity), age, physical or mental disability, veteran status, genetic information, or citizenship by, or resulting from the activities of, a provider of a hosting service.

(C) Any malfunctioning or intentional manipulation of a hosting service, including by means of inauthentic use or coordinated, automated, or other exploitation of the service or risks inherent to the intended operation of the service, including the amplification of illegal content, and of content that is in breach of the community standards of the provider of the service and has an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, electoral processes, public security, or the safety of vulnerable and marginalized communities."

Many platforms will interpret systemic risks to include the spread of dangerous mis/disinformation created at scale by generative AI tools. Additionally, to the extent that generative AI is used within the hosting service it would be covered in the risk assessments and at least tangentially in the other transparency requirements of the bill.

[If a generative AI tool is considered an ICS]

Depending on the size of generative AI system in question it may be subject to a range of oversight and reporting including clear community standards, transparency reports, internal complaint systems, researcher access, risk assessment & mitigation reports, independent audits for all harms, advertisement libraries, high reach public content stream

Platform Accountability and Consumer Transparency (PACT) Act (S.797)

Sen. Schatz (D-HI), Sen. Thune (R-SD)

Outlines transparency requirements and narrows Section 230's safe harbor.

[If a generative AI tool is not considered an ICS]

Platforms that host user generated content will be required to submit biannual transparency reports which would likely be impacted by the amount and types of content created through generative AI.

The bill states that Section 230 shall not *"apply to a provider of an interactive computer service, with respect to illegal content shared or illegal activity occurring on the interactive computer service, if the provider—*

(i) has actual knowledge of the illegal content or illegal activity; and

(ii) does not remove the illegal content or stop the illegal activity—

(I) within 4 days of acquiring that knowledge, subject to reasonable exceptions based on concerns about the legitimacy of the notice; or

(II) if the knowledge is acquired from a notice that emanates from a default judgment or stipulated agreement—

(aa) within 10 days of acquiring that knowledge; or

(bb) if the provider seeks to vacate the default judgment or stipulated agreement [described earlier in bill] and the proceeding initiated under that subparagraph results in a determination that the default judgment or stipulated agreement should remain intact, within 24 hours of that determination."

To the extent content created by generative AI is illegal the interactive computer service hosting the content would need to remove it.

[If a generative AI tool is considered an ICS]

The generative AI tool would be required to have a complaint system for "potentially policy-violating content, illegal content, or illegal activity," complete transparency reports on the treatment of such content and would lose Section 230 immunity for actions taken by federal agencies.

Platform Accountability and Transparency Act (S.5339)

Sen. Coons (DE-D), Sen. Portman (R-OH), Sen. Klobuchar (D-MN), Sen. Cassidy (R-LA)

Requires covered platforms to make data available to researchers, journalists, and the public.

Covers any platform that *"(i) permits a person to become a registered user, establish an account, or create a profile for the purpose of allowing the user to create, share, and view user-generated content through such an account or profile; (ii) enables one or more users to generate content that can be viewed by other users of the platform; and (iii) primarily serves as a medium for users to interact with content generated by other users of the platform and for the platform to deliver ads to users"*

This definition will likely not cover standalone generative AI tools but would cover social media platforms that integrate generative AI or spread content created by generative AI tools.

Algorithmic Justice and Online Platform Transparency Act (H.R.3611) (S.1896)

Rep. Matsui (D-CA), Sen. Markey (D-MA)

Requires online platforms release disclosures and assessments to ensure the product doesn't discriminate.

Generative AI tools would likely be included under the definition of *"Algorithmic Process"* noted in the bill, however the definition for *"Online Platform"* includes the phrase *"and provides a community forum for user generated content."* Community forum is not defined in the text, a standalone generative AI tool may argue they are not providing a community forum.

To the extent an *"Online Platform"* utilizes an *"Algorithmic Process"* (including but not limited to generative AI) to *"withhold, amplify, recommend, or promote content (including a group) to a user of the online platform"* they would need to provide a notice regarding personal information and its use in the algorithmic process, content moderation transparency reports, advertisement libraries, and data portability.

(Continued on next page)

Additionally, *“if the online platform (except for a small business) utilizes an algorithmic process that relates to opportunities for housing, education, employment, insurance, credit, or the access to or terms of use of any place of public accommodations,* [disclosures would need to include] *an assessment of whether the type of algorithmic process produces disparate outcomes on the basis of an individual’s or class of individuals’ actual or perceived race, color, ethnicity, sex, religion, national origin, gender, gender identity, sexual orientation, familial status, biometric information, or disability status.”*

Section 6 of the bill prohibits conduct related to discrimination in public accommodations, equal opportunity, voting rights, discriminatory advertising.

Notably, the text also includes this safety provision:

"(e) Safety and effectiveness of algorithmic processes.—

(1) IN GENERAL.—It shall be unlawful for an online platform to employ an algorithmic process in a manner that is not safe and effective.

(2) SAFE.—For purposes of paragraph (1), an algorithmic process is safe—

(A) if the algorithmic process does not produce any disparate outcome as described in the assessment conducted under section 4(a)(2)(A)(iv); or

(B) if the algorithmic process does produce a disparate outcome as described in the assessment conducted under section 4(a)(2)(A)(iv), any such disparate outcome is justified by a non-discriminatory, compelling interest, and such interest cannot be satisfied by less discriminatory means.

(3) EFFECTIVE.—For purposes of paragraph (1), an algorithmic process is effective if the online platform employing or otherwise utilizing the algorithmic process has taken reasonable steps to ensure that the algorithmic process has the ability to produce its desired or intended result."

Stopping Unlawful Negative Machine Impacts through National Evaluation Act (S.5351)

Sen. Portman (R-OH)

Clarifies that *"A covered entity that uses artificial intelligence to make or inform a decision that has an impact on a person that is addressed by a covered civil rights law, including whether to provide a program or activity or accommodation to a person, shall be liable for a claim of discrimination under the corresponding covered civil rights law in the same manner and to the same extent (including being liable pursuant to that law's standard of culpability) as if the covered entity had made such decision without the use of artificial intelligence."*

The definition of *Artificial Intelligence System* defined in the bill would likely include generative AI tools.

The bill also directs NIST to *"establish a program for conducting technology evaluations to assess and assist in mitigating bias and discrimination in artificial intelligence systems of covered entities with respect to race, sex, age, disability, and other classes or characteristics protected by covered civil rights laws. In establishing such program, the Director shall ensure that such evaluations effectively approximate real-world applications of artificial intelligence systems."*

"Promoting Responsibility Over Moderation In the Social-media Environment Act" or the "PROMISE Act". (S.427) (HR.5803)

Sen. Lee (R-UT), Sen. Moran (R-KS), Sen. Braun (R-IN),
Rep. Rice (R-SC), Rep. Joyce (R-OH), Rep. Norman (R-SC)

[If a generative AI tool is not considered an ICS]

Any platform that hosts user generated content including that created with generative AI tools would likely need to disclose how they moderate such content.

[If a generative AI tool is considered an ICS]

Requires covered entities to *"implement and operate in accordance with an information moderation policy…disclose such information moderation policy in a publicly available and easily accessible manner; and shall not make a deceptive policy statement with respect to such information moderation policy."*

Where an "information moderation policy" *includes "a policy that accurately describes, in plain, easy to understand language, information regarding the business practices of a covered entity with respect to the standards, processes, and policies of the covered entity on moderating information provided by a user or other information content provider…"*

Considerations for lawmakers moving forward:

Consider the desired goals and outcomes from risk assessment and transparency reporting. How are these goals similar or different in the case of social media platforms versus standalone generative AI tools? To the extent generative AI tools should be included, clarify the legislative text and thoroughly consider if the type of reports required (“number of content removals”) makes sense or has the same meaning in the generative AI context. In the case that broad definitions are used, give the FTC clear direction to consider context and the technology's use during rule making.

Consider what meaningful transparency means for the public versus researchers/auditors versus regulators. Is there information about how generative AI tools are trained and tested (red teamed) that could be made avilible to the public or researchers? Balance these goals with risks to privacy and security. This will require engaging multiple expert communities that are sometimes siloed.

DATA PROTECTION

Challenges bills aim to address:

When considering personal information and generative AI, the notable risks are a) a generative AI tool reveals (generates) output containing personal information, b) the prompts entered by the users can be used to infer sensitive information, similar to traditional search queries and c) personal information is processed in a way that discriminates against or otherwise harms a user.

Progress made by existing proposals:

The interaction between data protection/privacy laws and generative AI is perhaps the most challenging to assess because the proposal's definitions of covered data, personal data, public data, anonymous data, third party (data broker) and service provider determine if a standalone generative AI tool is covered by the text and what obligations apply. Additionally, the public currently only has high level information regarding exactly what data has been used to train and test these models (see need for transparency above). To determine if the bills listed below cover generative AI tools, I looked closely at these definitions and considered the following categories of data: device IDs, user prompts (that can be argued are reasonably linkable to a user), inferences made from public data and/or anonymized data.

The proposals below will likely capture the data practices of most generative AI tools, but obligations such as deletion rights are murky and likely to be context specific. To the extent a generative AI tool can truly separate user prompts from the user (no collection of device ID) they may be able to escape coverage entirely of these provisions depending on the exact language of the text.

Some of the proposals also include provisions such as duty of care (requires covered entities take reasonable measures to reduce harm) and obligations to uphold civil rights that will likely extend to generative AI tools. These provisions will require companies building these tools to carefully consider and test the outputs generated by their technology (the ways these tools process covered data/personal data).

American Data Privacy Protection Act (ADPPA) (H.R. 8152)

Rep. Pallone (D-NJ), Rep. McMorris Rodgers (R-WA), Rep. Schakowsky (D-IL), Rep. Bilirakis (R-FL)

Outlines a comprehensive set of obligations for covered entities and protections for consumers including data minimization. Companies building generative AI tools would be considered covered entities and would have a range of obligations under the bill.

Clarifies that covered data would include *"any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive covered data with respect to an individual."* Therefore, to the extent public data is used to train a generative AI tool, and that tool reveals sensitive data about an individual, that output is protected.

Additionally, Sec 207 would clarify that a generative AI tool *"may not collect, process, or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability."*

Similar to the Algorithm Accountability Act, depending on the size of the generative AI platform, the company may have to conduct algorithm impact assessments that outline the steps the company *"has taken or will take to mitigate potential harms from the covered algorithm to an individual or group of individuals, including related to—*

(I) covered minors;

(II) making or facilitating advertising for, or determining access to, or restrictions on the use of housing, education, employment, healthcare, insurance, or credit opportunities;

(III) determining access to, or restrictions on the use of, any place of public accommodation, particularly as such harms relate to the protected characteristics of individuals, including race, color, religion, national origin, sex, or disability;

(IV) disparate impact on the basis of individuals' race, color, religion, national origin, sex, or disability status; or

(V) disparate impact on the basis of individuals' political party registration status."

To the extent that a generative AI tool uses data that is "licensed" or otherwise non-public they would potentially be considered a "third party" or a "third party collecting agency" and would be implicated by several provisions of the bill.

The bill also outlines mandates for data deletion and portability and includes important text acknowledging that exemptions may be needed for some technologies.

Consumer Online Privacy Rights Act (COPRA) (S.3195)

Sen. Cantwell (D-WA)

Outlines a comprehensive set of obligations for covered entities and protections for consumers.

The covered entity definition will likely include generative AI tools both because they collect user prompt data and because the training data while presumably "public data," if it is combined to display personal information it would be captured in the "limitation" for "publicly available information" which does not include "information derived from publicly available information."

As a covered entity, generative AI tools would have a duty of care similar to that described in the Data Care Act, but slightly broader: *"A covered entity shall not— (1) engage in a deceptive data practice or a harmful data practice…" where, "The term "deceptive data practice" means an act or practice involving the processing or transfer of covered data in a manner that constitutes a deceptive act or practice in violation of section 5(a)(1) of the Federal Trade Commission Act"* and the term *"harmful data practice means the processing or transfer of covered data in a manner that causes or is likely to cause any of the following: (A) Financial, physical, or reputational injury to an individual. (B) Physical or other offensive intrusion upon the solitude or seclusion of an individual or the individual's private affairs or concerns, where such intrusion would be offensive to a reasonable person. (C) Other substantial injury to an individual."*

The bill includes civil rights protections:

"A covered entity shall not process or transfer covered data on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability—

(A) for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for a housing, employment, credit, or education opportunity, in a manner that unlawfully discriminates against or otherwise makes the opportunity unavailable to the individual or class of individuals; or

(Continued on next page)

(*B) in a manner that unlawfully segregates, discriminates against, or otherwise makes unavailable to the individual or class of individuals the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation."*

The bill also requires algorithmic decision-making impact assessments:

"a covered entity engaged in algorithmic decision-making, or in assisting others in algorithmic decision-making for the purpose of processing or transferring covered data, solely or in part to make or facilitate advertising for housing, education, employment or credit opportunities, or an eligibility determination for housing, education, employment or credit opportunities or determining access to, or restrictions on the use of, any place of public accommodation, must annually conduct an impact assessment of such algorithmic decision-making that—

(A) describes and evaluates the development of the covered entity's algorithmic decision-making processes including the design and training data used to develop the algorithmic decision-making process, how the algorithmic decision-making process was tested for accuracy, fairness, bias and discrimination; and

(B) assesses whether the algorithmic decision-making system produces discriminatory results on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability."

Under the bill, covered entities have a range of other duties and obligations.

Information Transparency and Personal Data Control Act (H.R.1816)

Rep. DelBene (D-WA)

Outlines conditions under which controllers offer consumers opt-in and opt-out options for data collection. Generative AI tools that collect "sensitive personal information" would be considered a controller.

Most generative AI tools will likely collect "sensitive personal information" because prompt data is covered by the following:

"(xvi) web browsing history, application usage history, and the functional equivalent of either that is data described in this subparagraph that is not aggregated data."

There are carve outs for de-identified information and publicly available information that may limit a generative AI tool's responsibilities.

Data Care Act (S.919)

Sen. Schatz (D-HI)

Mandates online services abide by a *duty of care and duty of loyalty*.

Most generative AI tools would be covered by the definition of “online service provider” because they collect what the bill refers to as “individual identifying data.”

This means they would be held to a *“duty of care”*

“An online service provider shall—

(A) reasonably secure individual identifying data from unauthorized access; and

(B) subject to subsection (d), promptly inform an end user of any breach of the duty described in subparagraph (A) of this paragraph with respect to sensitive data of that end user.”

And a “duty of loyalty”

“An online service provider may not use individual identifying data, or data derived from individual identifying data, in any way that—

(A) will benefit the online service provider to the detriment of an end user; and

(B) (i) will result in reasonably foreseeable and material physical or financial harm to an end user; or

(ii) would be unexpected and highly offensive to a reasonable end user.”

My best interpretation is that a prompt entered into a generative AI tool would count as “individual identifying data” and therefore could not be used “in reasonably foreseeable and material physical or financial harm to an end user” meaning potential output of say a chatbot that met this level of harm would be prohibited.

Social Media Privacy Protection and Consumer Rights Act (S. 1667)

Sen. Klobuchar (D-MN), Sen. Kennedy (R-LA)

Mandates online platforms implement certain privacy protections pertaining to transparency and terms of service, access rights, and actions when a violation of privacy occurs.

This bill uses the following definition of "online platform" and would likely capture most generative AI tools although the "and" may mean that generative AI tools are only covered if the courts determine they are "a search engine."

"The term "online platform"—

(A) means any public-facing website, web application, or digital application (including a mobile application); ***and***

(B) includes a social network, an ad network, a mobile operating system, a search engine, an email service, or an internet access service."

Balancing the Rights Of Web Surfers Equally and Responsibly Act of 2021 (S.113) (H.R.4659)

Sen. Blackburn (R-TN)

Requires "edge services" obtain opt-in approval from a user to use, disclose, or permit access to the sensitive user information of the user.

The term "edge service" means a service provided over the internet— *"(i) for which the provider requires the user to subscribe or establish an account in order to use the service; (ii) that the user purchases from the provider of the service without a subscription or account; (iii) by which a program searches for and identifies items in a database that correspond to keywords or characters specified by the user, used especially for finding particular sites on the world wide web; or (iv) by which the user divulges sensitive user information; and (B) includes a service described in subparagraph (A) that is provided through a software program, including a mobile application.*

Sensitive user information includes any of the following: *(A) Financial information. (B) Health information. (C) Information pertaining to children under the age of 13. (D) Social Security number. (E) Precise geolocation information. (F) Content of communications. (G) Web browsing history, history of usage of a software program (including a mobile application), and the functional equivalents of either."* The "functional equivalents" of browsing history would likely cover user prompts into a generative AI tool.

Consumer Data Privacy and Security Act of 2021 (S.1494)

Sen. Moran (R-KS)

Outlines a comprehensive set of obligations for covered entities and protections for consumers.

Companies building generative AI tools would likely be considered covered entities because they *"alone, or jointly with others, determine the purpose and means of collecting or processing personal data"* where "personal data" means *"information that identifies or is linked or reasonably linkable to a specific individual."* which is likely to include prompt data linked to an account.

The proposal does exclude "publicly available information" from the definition of personal data where "*The term "publicly available information" means any information that a covered entity or service provider has a reasonable basis to believe is lawfully made available to the general public from– (i) a Federal, State, or local government record; (ii) widely distributed media; or (iii) a disclosure to the general public that is made voluntarily by an individual, or required to be made by a Federal, State, or local law."* In the case that the inferences made by the generative AI tool are made with publicly available information that sensitive information may fall outside the bounds of this bill.

Generative AI tools or technologies that incorporate generative AI tools covered by this bill will also be required to provide data access, portability, ability to correct and erase. Due to the publicly available information exclusion, it is unclear if a provider of a generative AI tool would be required to provide erasure rights in the case of information (true or false) generated about an individual.

Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act or the SAFE DATA Act (S.2499)

Sen. Wicker (R-MS), Sen. Blackburn (R-TN)

Outlines a comprehensive set of obligations for covered entities and protections for consumers.

This is a comprehensive data protection proposal and most companies building generative AI tools would likely be considered covered entities because they "*collect, process, or transfer covered data; and determines the purposes and means of such collection, processing, or transfer,"* where covered data is *"linked or reasonably linkable to an individual."* which is likely to include user prompt data linked to an account.

This proposal does exclude "publicly available information" from the definition of personal data where *"the term "publicly available information" means any information that a covered entity has a reasonable basis to believe—(I) has been lawfully made available to the general public from Federal, State, or local government records;(II) is widely available to the general public, including information from—(aa) a telephone book or online directory;(bb) television, internet, or radio content or programming; or(cc) the news media or a website that is lawfully available to the general public on an unrestricted basis (for purposes of this subclause a website is not restricted solely because there is a fee or log-in requirement associated with accessing the website); or (III) is a disclosure to the general public that is required to be made by Federal, State, or local law."* This definition quite clearly includes any data posted publicly on a social media site or online forum regardless of sensitivity.

Generative AI tools or technologies that incorporate generative AI tools covered by this bill will also be required to provide *"access to, and correction, deletion, and portability of, covered data."* It is unclear if a provider of a generative AI tool would be required to provide erasure rights in the case of information (true or false) generated about an individual.

Protecting the Information of our Vulnerable Children and Youth Act (Kids PRIVCY) (H.R. 4801)

Rep. Castor (D-FL)

Amends the Children's Online Privacy Protection Act of 1998. Includes a full set of product design and data protection obligations.

A generative AI tool that processes covered information (*"means any information, linked or reasonably linkable to a specific teenager [under age 18] or child, or specific consumer device of a teenager or child"*) and is *"directed to children"* (*"targeted to or attractive to children"*) would likely be a children's service.

Operators of a *children's service* have several obligations under the bill related to data minimization, transparency, consent, retention of data, sharing of data with third parties, rights to access, correct, delete covered information.

Additionally, the bill outlines *"prohibited practices with respect to teenagers and children"* which includes:

"(i) process any covered information in a manner that is inconsistent with what a reasonable teenager or parent of a child would expect in the context of a particular transaction or the teenager's or parent's relationship with such operator, or seek to obtain verifiable consent for such processing;

(ii) process any covered information in a manner that is harmful or has been shown to be detrimental to the well-being of children or teenagers;

(iii) process covered information for the purpose of providing for targeted personalized advertising or engage in other marketing to a specific child or teenager or group of children or teenagers based on—

(I) using the covered information, online behavior, or group identifiers of such child or teenager or of the children or teenagers in such group; or

(II) using the covered information or online behavior of children or teenagers who share characteristics with such child or teenager or with the children or teenagers in such group, including income level or protected characteristics or proxies thereof;

(Continued on next page)

(iv) condition the participation of a child or teenager in a game, sweepstakes, or other contest on consenting to the processing of more covered information than is necessary for such child or teenager to participate;

(v) engage in cross-device tracking of a child or teenager unless the child or teenager is logged-in to a specific service, for the sole purpose of facilitating the primary purpose of the good or service or a specific feature thereof;

(vi) engage in algorithmic processes that discriminate on the basis of race, age, gender, ability, or other protected characteristics;

(vii) disclose biometric information;

(viii) disclose geolocation information; or

(ix) collect geolocation information by default or without making it clear to a user when geolocation tracking is in effect"

Point (ii) suggests that generative AI tools are responsible for their outputs in response to a child's prompt. Point (vii) includes "biometric information" which the bill does not define but in other bills includes voice prints and facial mapping, generative AI tools would be prohibited from disclosing (which likely includes generating) this information.

Children and Teens' Online Privacy Protection Act (S.1628)

Sen. Markey (D-MA), Sen. Cassidy (R-LA)

Amends the Children's Online Privacy Protection Act of 1998.

Generative AI tools that are *"directed to children or minors"* (under age 17) as demonstrated by a set of criteria related to the marketing and appearance of the tool or because the tool is *"used or reasonably likely to be used by children or minors."* (this last part will likely capture many of the generative AI tools out right now because of use in school work) would be subject to data collection and processing provisions related to "personal information."

"The term "personal information" means individually identifiable information about an individual collected online, including-(A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph."

Clean Slate for Kids Online Act of 2021 (S.1423)

Sen. Durbin (D-IL), Sen. Markey (D-MA), Sen. Blumenthal (D-CT), Sen. Hirono (D-HI)

Provides deletion rights for personal information regarding children 13 or under.

This bill would require *"the operator of any website or online service directed to children"* to give *"individual over the age of 13, or a legal guardian of an individual over the age of 13 acting with the knowledge and consent of the individual,"* the ability to request and delete *"all personal information in the possession of the operator that was collected from or about the individual when the individual was a child notwithstanding any parental consent that may have been provided when the individual was a child;"* where personal information has the definition in Section 1302 of the Children's Online Privacy Protection Act of 1998 (below)

Personal information as defined in COPPA:

The term "personal information" means individually identifiable information about an individual collected online, including-

(A) a first and last name;

(B) a home or other physical address including street name and name of a city or town;

(C) an e-mail address;

(D) a telephone number;

(E) a Social Security number;

(F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or

(G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph."

First, it is interesting to note that the definition of personal information in COPPA does not have a carve out for public data, in fact in order to host an ICS for children, the operator is responsible for deleting "all individually identifiable information from postings by children before they are made public, and deletes such information from the operator's records."[3]

[3] Federal Register / Vol. 78, No. 12 / Thursday, January 17, 2013 / Rules and Regulations (https://www.ftc.gov/system/files/2012-31341.pdf)

Regarding a generative AI tool's training data, there should not be any public data posted by a child (assuming websites have been following COPPA) however it is possible that a generative AI tool used data posted by adults that would contain personal information belonging to a child and as an operator under this law may need to process deletion requests. If this bill intends to include any and all personal information belonging to children under 13 including in training data sets based on public information published by an adult, this text would benefit from clarity.

To the extent a generative AI tool is "directed to children" they would also likely be responsible for deleting any user prompts stored from the young users under this proposal.

Note: There are several sector specific data protection bills (health data, student data, etc) that would likely be relevant to generative AI tools but are outside the scope of this list.

Considerations for lawmakers moving forward:

Should the outputs of generative AI tools, even those trained with anonymous and/or public data be considered covered information (subject to various obligation in the legislation)? If so, be sure the definitions of covered data account for this output.

To the extent the proposal includes deletion rights (for adults or children), do they extend to a generative AI tool's training data (especially if training data is considered public information and/or anonymous)? In the case that an application is built on top of an existing generative AI tool, would the deletion requirements flow to the creator of the underlying generative AI tool or is the provider exempt based on definitions of *service provider*?

Does the *duty of care* language cover the concerns posed by generative AI tools? To the extent the process of generating harmful content is covered by a duty of care what is the impact on free expression and access to information? How should *duties of care* be enforced?

PRODUCT DESIGN CONSIDERATIONS

Challenges bills aim to address:

Generative AI tools like other online experiences can include design features aimed at keeping users on the platform for longer or otherwise manipulate users in harmful ways.

Progress made by existing proposals:

Many lawmakers have begun to view digital platform regulation from the viewpoint of protecting consumers from faulty product design and/or business models. Members of Congress have proposed prohibitions on targeted advertising, dark patterns or manipulative interfaces (endless scroll, auto play, badges, etc) and have outlined requirements for parental controls. The proposals below mostly target platforms that are understood to be protected from product liability cases under Section 230 of the Communication Decency Act, although many of the proposals below do not directly rely on the definition of Interactive Computer Service (ICS) defined in Section 230, meaning generative AI tools may be covered regardless of whether courts consider generative AI tools to be ICS.

Banning Surveillance Advertising Act (H.R.6416) (S.3520)

Rep. Eshoo (D-CA), Sen. Booker (D-NJ)

Bans targeted advertising.

To the extent a generative AI tool uses *"personal information with respect to the dissemination of the advertisement."* they would be banned from targeted advertising and allowed only to use contextual advertising.

"The term "target" means, with respect to the dissemination of an advertisement, to perform or cause to be performed any computational process designed to select an individual, connected device, or group of individuals or connected devices to which to disseminate the advertisement based on personal information pertaining to the individual or connected device or to the individuals or connected devices that make up the group."

Deceptive Experiences to Online Users Reduction (DETOUR) Act (H.R.6083) (S.3330)

Rep. Blunt Rochester (D-DE), Rep. Gonzalez (R-OH), Sen. Warner (D-VA), Sen. Fischer (R-NE)

Prohibits certain manipulative user interfaces.

Large online services defined as *"a website or a service, other than an internet access service, that is made available to the public over the internet, including a social network, a search engine, or an email service."* and has *"more than 100,000,000 authenticated users of an online service in any 30-day period"*

It would be unlawful for large online services:

"(1) to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision making, or choice to obtain consent or user data;

(2) to subdivide or segment consumers of online services into groups for the purposes of behavioral or psychological experiment or research of users of an online service, except with the informed consent of each user involved; or

(3) to design, modify, or manipulate a user interface on a website or online service, or portion thereof, that is directed to an individual under the age of 13, with the purpose or substantial effect of causing, increasing, or encouraging compulsive usage, inclusive of video auto-play functions initiated without the consent of a user."

Kids Online Safety Act (KOSA) (S.3663)*

*Also listed in risk assessment & transparency

Sen. Blumenthal (D-CT), Sen. Blackburn (R-TN)

Outlines a duty of care, mandates certain product design features and parental controls.

The provisions in this bill are tied to covered platforms where the *"term "covered platform" means a social media service, social network, video game, messaging application, video streaming service, educational service, or an online platform that connects to the internet and that is used, or is reasonably likely to be used, by a minor."*

"An online platform that connects to the internet" would likely cover most generative AI tools.

(Continued on next page)

Includes a duty of care that would impact the design and testing of generative AI tools:

"(a) Best interests.—A covered platform shall act in the best interests of a minor that uses the platform's products or services, as described in subsection (b).

(b) Prevention of harm to minors.—In acting in the best interests of minors, a covered platform shall take reasonable measures in its design and operation of products and services to prevent and mitigate—

(1) mental health disorders or associated behaviors, including the promotion or exacerbation of self-harm, suicide, eating disorders, and substance use disorders;

(2) patterns of use that indicate or encourage addiction-like behaviors;

(3) physical violence, online bullying, and harassment of a minor;

(4) sexual exploitation, including enticement, grooming, sex trafficking, and sexual abuse of minors and trafficking of online child sexual abuse material;

(5) promotion and marketing of narcotic drugs (as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802)), tobacco products, gambling, or alcohol; and

(6) predatory, unfair, or deceptive marketing practices, or other financial harms."

Additionally, platforms must design safeguards for minors and parental tools:

"a) Safeguards for minors.—

(1) IN GENERAL.—A covered platform shall provide a minor with readily-accessible and easy-to-use safeguards to, as applicable—

(A) limit the ability of other individuals to contact or find a minor, in particular individuals aged 17 or over with no relationship to the minor;

(B) prevent other users, whether registered or not, from viewing the minor's personal data collected by or shared on the covered platform, in particular restricting public access to personal data;

(C) limit features that increase, sustain, or extend use of the covered platform by a minor, such as automatic playing of media, rewards for time spent on the platform, notifications, and other features that result in compulsive usage of the covered platform by a minor;

(Continued on next page)

(D) control algorithmic recommendation systems that use a minor's personal data, including the right to—

(i) opt out of such algorithmic recommendation systems; or

(ii) limit types or categories of recommendations from such systems;

(E) delete the minor's account and delete their personal data;

(F) restrict the sharing of the geolocation of a minor and provide notice regarding the tracking of a minor's geolocation; and

(G) limit the amount of time spent by a minor on the covered platform.

b) Parental tools.—

(1) TOOLS.—A covered platform shall provide readily-accessible and easy-to-use tools for parents to supervise the use of the covered platform by a minor.

(2) REQUIREMENTS.—The tools provided by a covered platform shall include—

(A) the ability to control privacy and account settings, including the safeguards established [above];

(B) the ability to restrict purchases and financial transactions by a minor, where applicable;

(C) the ability to track metrics of total time spent on the platform; and

(D) control options that allow parents to address the harms described in [harm to minors section]"

Kids Internet Design and Safety Act (KIDS Act) (S.2918) (H.R.5439)

Sen. Markey (D-MA), Rep. Castor (D-FL)

Prohibits certain interface elements within online platforms directed to children.

Most generative AI tools would meet the definition of an online platform.

To the extent generative AI tools are *"directed to children"* they would face a *"prohibition on certain interface elements."* Notably this would include *"(iv) Any interface element or setting that unfairly encourages a covered user, due to their age or inexperience, to share personal information, submit content, or spend more time engaging with the platform."*

Additionally, the text includes language that would make it unlawful for an online platform directed to children to use an:

"algorithmic process that amplifies, promotes, or encourages covered users' consumption of videos and other forms of content that—

(A) are of a non-educational nature (as determined by the Commission); and

(B) involve—

(i) sexual material;

(ii) promotion of physical or emotional violence or activities that can reasonably be assumed to result in physical or emotional harm, including self-harm, use of weapons, and bullying;

(iii) activities that are unlawful for covered users to engage in or the promotion of such activities; or

(iv) wholly commercial content that is not reasonably recognizable as such to a covered user."

(Continued on next page)

"Where the term "algorithmic process" means a computational process, including one derived from machine learning or other artificial intelligence techniques, that processes personal information or other data for the purpose of determining the order or manner that a set of information is provided to a user of an online platform, including the provision of commercial content, the display of social media posts, or any other method of automated decision making, content selection, content recommendation, or content amplification."

The phrase *"determining the order or manner that a set of information is provided to a user of an online platform"* suggests many generative AI tools would be covered. It is less clear to me if a response from a generative AI tool to a user's prompt would qualify as *"algorithmic process that amplifies, promotes, or encourages covered users' consumption of videos and other forms of content."*

Nudging Users to Drive Good Experiences on Social Media Act" or the "Social Media NUDGE Act" (S.3608)

Sen. Klobuchar (D-MN), Sen. Lummis (R-WY)

Directs the National Science Foundation (NSF) to work with the National Academy of Sciences, Engineering, and Medicine (NASEM) to conduct a study to identify "content-neutral interventions" aimed at reducing the spread of "harms related to algorithmic amplification and social media addiction" on covered platforms.

Covered platforms include *"any public-facing website, desktop application, or mobile application that—*

(A) is operated for commercial purposes;

(B) provides a forum for user-generated content;

(C) is constructed such that the core functionality of the website or application is to facilitate interaction between users and user-generated content; and

(D) has more than 20,000,000 monthly active users in the United States for a majority of the months in the previous 12-month period."

This definition will likely not cover standalone generative AI tools but would cover social media platforms that integrate generative AI or spread content created by generative AI.

Directs the FTC to conduct rule making on how covered platforms should apply the findings from the study.

"Promoting Rights and Online Speech Protections to Ensure Every Consumer is Heard Act" or the "PRO-SPEECH Act". (S. 2031)

Sen. Wicker (R-MS)

Outlaws internet platforms from preventing access to lawful content.

Generative AI tools would likely be considered an internet platform under this bill because they *"enables a user to initiate a search query for particular information using the internet and…[are] capable of returning at least 1 search result unaffiliated with the owner or operator of the search engine."*

The bill states that an internet platform may not *"Block or otherwise prevent a user or entity from accessing any lawful content, application, service, or device that does not interfere with the internet platform's functionality or pose a data privacy or data security risk to a user."* along with other outlawed practices. This type of language would mean that developers of generative AI tools may have to think about the types of prompts they block/discourage and may have to consider if those restrictions prevent the user's access to lawful content.

The bill also includes transparency requirements *"an internet platform shall disclose, on a publicly available and easily accessible website, accurate information regarding the platform management practices, performance characteristics, and commercial terms of service of its app store, cloud computing service, operating system, search engine, or social media network sufficient to enable a reasonable user to make an informed choice regarding the purchase or use of such service and to develop, market, and maintain a product or service on the internet platform."*

Note: there are many bills that amend Section 230, in the case that a generative AI tool is deemed an Interactive Computer Service by the courts, these bills would be relevant. [4] Additionally, bills that amend Section 230 may also impact the way social media companies treat content created by generative AI tools.

[4] Anand, M., Jeevanjee, K., Johnson, D., Jurecic, Q., Lim, B., Ly, I., Perault, M., Reed, E., Ruddock, J., Schmeling, T., Vattikonda, N., Worthington, B., Wilson, N., & Zhou, J. (2021, March 23). All the Ways Congress Wants to Change Section 230. Slate. https://slate.com/technology/2021/03/section-230-reform-legislative-tracker.html

Considerations for lawmakers moving forward:

What types of manipulation from generative AI tools are embedded in the user interface and/or business model? What types of manipulation come from the content or responses provided by the generative AI tool? Are the policy levers to address these the same?

If design limitations are addressing harms to children, will the different product goals require different underlying statistical models for children and adults or can concerns be addressed in other ways?

COMPETITION IN DIGITAL MARKETS

Challenges bills aim to address:

Generative AI tools require vast amounts of data storage and computational power which are currently only offered as-a-service by a handful of companies in the US: Amazon, Microsoft and Google.[5] These companies are also owners and investors in the exact generative AI tools built using their infrastructure creating conflicts of interest and barriers to entry.

Progress made by existing proposals:

In the 116th Congress, the House Judiciary led an investigation into digital markets. The results of that investigation informed a collection of bipartisan legislation introduced in the 117th Congress.[6] Some of the proposals focus broadly on oxygenating the digital market space by providing antitrust regulators more resources to bring cases and scrutinize mergers, while others specifically prohibit anti-competitive practices. Below, I highlight a few proposals that would have clear implications for companies deploying generative AI tools today.

[5] US House Judiciary Committee. (2020). Investigation of competition in digital markets: Majority staff report and recommendations. Subcommittee on Antitrust, Commercial, and Administrative Law Committee on the Judiciary, US House of Representatives: Washington. (see Cloud Computing Chapter, Voice Assistants Chapter, and Amazon Web Services Chapter)

[6]Feiner, L. (2021, June 11). Lawmakers unveil major bipartisan antitrust reforms that could reshape Amazon, Apple, Facebook and Google. CNBC. https://www.cnbc.com/2021/06/11/amazon-apple-facebook-and-google-targeted-in-bipartisan-antitrust-reform-bills.html

American Choice and Innovation Online Act (S.2992) (H.R.3816)

Sen. Klobuchar (D-MN), Sen. Grassley (R-IA), Rep. Cicilline (D-NJ), Rep. Gooden (R-TX)

This bill only covers very large companies for which market cap is a key metric (and has been fluctuating over the last few years), for the sake of analyzing generative AI, I am assuming Amazon, Google and Microsoft are covered platforms.

Makes a series of anti competitive discrimination unlawful including:

"(1) preference the products, services, or lines of business of the covered platform operator over those of another business user on the covered platform in a manner that would materially harm competition;

(2) limit the ability of the products, services, or lines of business of another business user to compete on the covered platform relative to the products, services, or lines of business of the covered platform operator in a manner that would materially harm competition;

(3) discriminate in the application or enforcement of the terms of service of the covered platform among similarly situated business users in a manner that would materially harm competition;

(4) materially restrict, impede, or unreasonably delay the capacity of a business user to access or interoperate with the same platform, operating system, or hardware or software features that are available to the products, services, or lines of business of the covered platform operator that compete or would compete with products or services offered by business users on the covered platform;

(5) condition access to the covered platform or preferred status or placement on the covered platform on the purchase or use of other products or services offered by the covered platform operator that are not part of or intrinsic to the covered platform;

(6) use nonpublic data that are obtained from or generated on the covered platform by the activities of a business user or by the interaction of a covered platform user with the products or services of a business user to offer, or support the offering of, the products or services of the covered platform operator that compete or would compete with products or services offered by business users on the covered platform;

(Continued on next page)

(7) materially restrict or impede a business user from accessing data generated on the covered platform by the activities of the business user, or through an interaction of a covered platform user with the products or services of the business user, such as by establishing contractual or technical restrictions that prevent the portability by the business user to other systems or applications of the data of the business user;

(8) materially restrict or impede covered platform users from uninstalling software applications that have been preinstalled on the covered platform or changing default settings that direct or steer covered platform users to products or services offered by the covered platform operator, unless necessary—

…(9) in connection with any covered platform user interface, including search or ranking functionality offered by the covered platform, treat the products, services, or lines of business of the covered platform operator more favorably relative to those of another business user than under standards mandating the neutral, fair, and nondiscriminatory treatment of all business users;"

The provisions **could** be interpreted by the courts to outlaw situations such as:

- A user enters a prompt into Bing's generative AI chatbot ("what video games should I play this weekend") that is trained to disproportionately respond with games produced by Activision Blizzard (This is an example of a Microsoft product preferencing another line of business)
- Applications using Bard are designed to work twice as fast on Android operating system
- A startup company building a generative AI tool uses AWS infrastructure, AWS can not intentionally slow service for the startup or use the metadata generated by the startup's use of AWS to compete against it, etc

Ending Platform Monopolies Act (H.R.3825)

Rep. Jayapal (D-WA), Rep. Gooden (R-TX)

This bill only covers very large companies for which market cap is a key metric (and has been fluctuating over the last few years), for the sake of analyzing generative AI, I am assuming Amazon, Google and Microsoft are covered.

Makes it illegal for these companies to give rise to a conflict of interest:

"it shall be unlawful for a covered platform operator to own, control, or have a beneficial interest in a line of business other than the covered platform that—

(1) utilizes the covered platform for the sale or provision of products or services;

(2) offers a product or service that the covered platform requires a business user to purchase or utilize as a condition for access to the covered platform, or as a condition for preferred status or placement of a business user's product or services on the covered platform; or

(3) gives rise to a conflict of interest.

(b) Conflict of interest.—For purposes of this section, the term "conflict of interest" includes the conflict of interest that arises when—

(1) a covered platform operator owns or controls a line of business, other than the covered platform; and

(2) the covered platform's ownership or control of that line of business creates the incentive and ability for the covered platform to—

(A) advantage the covered platform operator's own products, services, or lines of business on the covered platform over those of a competing business or a business that constitutes nascent or potential competition to the covered platform operator; or

(B) exclude from, or disadvantage, the products, services, or lines of business on the covered platform of a competing business or a business that constitutes nascent or potential competition to the covered platform operator."

Given that data storage and compute power is a primary input into generative AI tools, and that the companies covered by this bill build generative AI and compete against other companies building generative AI tools, cloud computing business lines (AWS, Google Cloud, Azure), at a minimum, would likely need to be structurally separated from the parent companies.

Considerations for lawmakers moving forward:

These bills create additional tools for the existing anti-competitive conduct regulatory toolbox, the considerations for generative AI tools are similar to other digital technologies: what specifics/details need to be explicitly outlined in the legal text versus left to specific case interpretation?

How do public investments in shared computing infrastructure such as the proposed National Artificial Intelligence Research Resource (NAIRR)[7] address issues related to concentrated power in the storage and compute market? Where would additional market power concerns remain?

[7] Strengthening and Democratizing the U.S. Artificial Intelligence Innovation Ecosystem: An Implementation Plan for a National Artificial Intelligence Research Resource. (2023). National Artificial Intelligence Research Resource Task Force.