The Developing Regulatory Framework for AI

D. Reed Freeman, Jr.
Partner, ArentFox Schiff
Reed.Freeman@afslaw.com

Eva Pulliam
Partner, ArentFox Schiff
Eva.Pulliam@afslaw.com

Sheila Colclasure
Global Digital Responsibilty Chief, Interpublic Group
Sheila.Colclasure@interpublic.com

Agenda

- Key Publications and Events in the U.S. (So Far)
- Key Topics
- Looking Ahead: State Legislation, Rulemaking, and the EU AI Act

Introduction

5CB94378.html

https://www.youtube.com/watch?v=jYTsZHd49Jo&t=3s

You Won't Believe What Obama Says In This Video! 😉 - YouTube

Part I: Key Publications and Events

- Various bodies within the executive branch of the U.S. federal government are working, both independently and collectively, to promulgate standards and guidelines for the development and use of artificial intelligence and machine learning technologies.

- Executive Orders related to artificial intelligence create a foundation for a "coordinated federal government strategy" on AI, including guiding principles.

Dept. of Defense / CIA Activity on AI

- **February 24, 2020: the DoD published <u>Department of Defense (DOD) AI Ethical Principles</u>**
  - Focus on preventing bias, promoting fairness, transparency, safety and security, and ability to disengage or deactivate deployed systems that demonstrate unintended behavior.

- **June 2020: the Intelligence Community published an AI Ethics <u>Principles</u> and <u>Framework</u>**
  - Focus on initial and ongoing testing to identify foreseeable risks, avoid lawful information collection respecting individual rights and liberties, incorporate human judgment and human accountability, mitigate bias.

Blueprint for an AI Bill of Rights

- In October, 2022, the Biden Administration published the <u>Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People</u>

- The Blueprint is intended to support the development of policies and practices that protect civil rights and promote democratic values in the building, deployment, and governance of automated systems.

Biden Administration Blueprint for an AI Bill of Rights

The Blueprint consists of five key Principles:

1) **Safe and Effective Systems:** Pre-deployment testing, risk identification and mitigation, ongoing monitoring

2) **Algorithmic Discrimination Protections:** Unjustified different treatment or impacts disfavoring people based on a protected characteristic; disparity testing

Blueprint for an AI Bill of Rights

3) **Data Privacy:** Focus on consent, privacy settings by default, training data sets, enhanced protections for sensitive data, worker protections from surveillance

4) **Notice and Explanation** that you're interacting with an automated system

5) **Human Alternatives, Consideration, and Fallback: Ability** to opt-out, where appropriate, and have access to a person who can quickly consider and remedy problems you encounter.

Biden Administration Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

– October 30, 2023

1) **Safety:**

- Share safety red team testing information with U.S. Government where foundational models affect national security (including economic security) or public health
- NIST to develop red team standards
- Watermarking to prevent fraud and deception using AI
- Continue to deploy AI to make networks more cyber-resiliant

Biden Administration Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

2) **Privacy**
   - Renewed call for Federal Privacy legislation
   - Focus on preserving privacy of training data
   - Federal agencies to evaluate effectiveness of privacy-preserving techniques in AI systems

3) **Civil Rights**
   - Guidance to avoid discrimination in housing, healthcare, and justice
   - DOJ to prosecute algorithmic discrimination resulting in civil rights violations

Biden Administration Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

3) Jobs

- Develop principles and best practices to address issues of workplace surveillance, bias, and job displacement cause by AI
- Study effect of AI on labor markets

4) Innovation and Competition

- Encourage FTC to keep markets competitive and protect small businesses
- Promote immigration for highly skilled employees

Biden Administration Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

5) Advance American leadership on International Frameworks and Standards on AI

6) USG to use AI to work better for Americans

Further Agency Publications and Developments Related to AI in 2023

- **January 2023**: NIST published Artificial Intelligence Risk Management Framework (AI RMF 1.0)
  - Reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair, with bias managed.

- **April 25, 2023**: Four federal agencies (CFPB, DOJ Civil Rights Division, EEOC, and FTC) released a joint statement on enforcement efforts against discrimination and bias in automated systems

- **July and September 2023**: Seven private sector technology companies met at the White House and voluntarily committed to manage the risks posed by artificial intelligence
  - Safe, secure, information sharing regarding AI risks, build public trust through transparency (watermarking), mitigating bias, promoting privacy, and directing AI systems to solve biggest societal challenges

- **August 9, 2023**: the White House announced an AI Cyber Challenge at the Black Hat USA Conference, a leading hacking conference in Las Vegas.

FTC Activity Related to AI

The FTC published two key reports, as well as several blog posts on AI.

Its 2016 report, "Big Data: A tool for Inclusion or Exclusion?, warns companies that big data analytics could result in bias or other harm to consumers.

Applicable laws: FCRA, ECOA, FTC Act

Operators of big data algorithms should focus on four high-level issues:
- Representative data sets
- Data models that account for bias
- Accurate predictions based on big data
- Consider ethical and fairness concerns

FTC Activity Related to AI

– On June 16, 2022, the FTC published a report to Congress, "Combatting Online Harms Through Innovation."

- Details the FTC's concerns that AI tools can be inaccurate, biased, and discriminatory by design.

- Concludes that AI is not the solution to the spread of harmful online content; new technology can be both helpful and dangerous.

- These themes are mirrored in the Blueprint for an AI Bill of Rights.

Part II: Special Topics -- Advertising

– The use of AI in the creation and marketing of products and services raises concerns related to <u>deceptive trade practices</u>.

– Examples:
  – Representing digital items as human-created, when in fact created by AI
  – Representing or implying the sale of all rights, when conveying only a limited license
  – Representing authenticity, when in fact AI-generated (e.g., voice in music)

Topic: Advertising

- Companies should keep in mind:

    - Do customers understand the material terms and conditions of what they are buying?
    - When offering a generative AI product, are you disclosing to what extent the training data includes copyrighted or otherwise protected material?

- The <u>FTC has warned companies</u> and advertisers to ensure statements made to consumers are truthful, supported, and do not "overpromise what your algorithm or AI-based tool can deliver."

- This is one of the key areas of concern for the FTC in its current investigation into OpenAI

Topic: Privacy

- The first two EOs (February, 2019 and December, 2020) discussed the need for the US to foster confidence in AI technologies but also to protect civil liberties, including privacy

- White House Blueprint for an AI Bill of Rights includes privacy as one of its five key principles

Topic: Privacy

– Privacy is one of the key areas of concern for the FTC in its current investigation into OpenAI (focus on <u>inputs</u>: training data sets and data scraping *and* <u>outputs</u>: accuracy of information regarding individuals)

– The companies who met at the White House in July, 2023 identified prioritizing research on societal risks including protecting privacy as part of their voluntary commitment.

– State comprehensive privacy laws in California and Colorado address "dark patterns" which will be a topic of future regulation by the California Privacy Protection Agency.

Topic: Privacy

Privacy Litigation

- Plaintiffs allege that OpenAI, Microsoft, and their respective affiliates violated the privacy rights of millions of internet users through the large-scale scraping of their personal data from social media, blog posts, and other websites, and using those data to train machine learning models.

- Plaintiffs assert that the defendants violated the Computer Fraud and Abuse Act (CFAA) by intentionally accessing protected computers without authorization and obtaining information through ChatGPT plug-ins integrated across various platforms and websites.

- *This is a sweeping new privacy theory, and could result in a market for "privacy-safe" data sets.*

- NOTE that the October 30 EO also focuses on protecting the privacy of training data

Topic: Cybersecurity

- One unintended consequence of the rush to release new AI systems: "Democratizing" cybersecurity harms

- Two basic types of issues:
    - Hacking techniques more accessible
    - AI going rogue and not following instructions, creating vulnerabilities and chaos

Topic: Cybersecurity

– The FTC has shown it is committed to addressing data security issues in its <u>investigation</u> into OpenAI.

– Following on numerous prior enforcement actions related to inadequate security protections of consumer's personal information, <u>the CID</u> asks about OpenAI's data security and the data security of the LLMs when made available through an API or plugin.

- Users' account information and chat history available to others
- User controls and how messaged
- "Prompt injection" attacks: Unauthorized attempts to bypass filters or manipulate an LLM using prompts that cause the model to ignore previous instructions or to perform actions unintended by its developers
- Addressing reasonable foreseeable risks: Asks for OpenAI policies and procedures used to assess risks to users' personal information in connection with API integrations and plugins and restrictions imposed on third parties use of user data.

– October 30 EO warns of cybersecurity risks but also benefits us using AI to improve cybersecurity

Topic: Intellectual Property Issues

– The process of training AI tools comes with <u>IP infringement risks</u>.

– Content produced without significant human control and input is <u>not copyrightable under U.S. law</u>, raising the question of who owns works created using generative AI tools, and who has the right to use these works?

Topic: Intellectual Property Issues

Intellectual Property Litigation

– Recent lawsuits comprise three putative class action complaints filed by authors:

- Software code owners have filed class actions against GitHub, *Microsoft*, and *Open AI*, involving the software code development AI models, namely, OpenAI's Codex and GitHub's Copilot.
  - Plaintiffs claim that the AI models were trained on a large corpus of software-related data, including copyrighted materials offered under specific open-source licenses.
  - Coders allege that the training and operation of the AI models not only violate their IP rights, but also breach the terms of the applicable software license agreements.
  - Authors have filed at least two complaints against OpenAI LP (owner of ChatGPT) and related entities and a third against Meta.
    - Allegation: Training data sets contained copyrighted material; outputs are dependent on them

Artificial Intelligence

Friday, September 29, 2023

Inside: • **Leading the News** • **Analysis** • **Companies**

IBM Joins Microsoft, Adobe in Protecting AI Customers From Suits

Customers of IBM's business-focused artificial intelligence model watsonx will be indemnified against copyright and other intellectual property infringement claims, the company announced Thursday, following similar moves from Microsoft and Adobe.

The initiative underscores the AI industry's growing recognition of the potential legal risks that come with obtaining large volumes of training data—much of which can be under copyright—without permission. IBM primarily markets watsonx as an AI platform for other businesses, unlike consumer-facing products such as OpenAI Inc.'s ChatGPT or StabilityAI Ltd.'s Stable Diffusion.

IBM also published information about the training methodology for its Granite model series, and the company noted it selectively blocks "websites known to disseminate pirated information," including the controversial Books3 dataset which authors claim contains hundreds of thousands of pirated books. Other major AI companies have faced a slew of recent copyright infringement suits from authors, coders, and visual artists. **Read More**

Leading the News

Nvidia Linked to Dawn Raid by French Competition Regulators

Topic: Employment Issues

– Employers are increasingly using AI systems to advertise jobs, target job applicants, and make hiring and other employment decisions. Employers can be exposed to liability if they exclude or disparately impact protected groups via the use of this technology in employment-related decision making.

– The EEOC is focusing on employment decisions in which companies use technology that may violate employment law.

– In April, EEOC Chair Charlotte A. Burrows further emphasized this interest in a **joint statement** with leaders of the US Department of Justice (DOJ), the Federal Trade Commission (FTC), and the Consumer Financial Protection Bureau (CFPB)

Topic: Bias

– AI technology can create and reinforce biases based on how the tool is built, especially with respect to what data is used to train the algorithm. This has been a repeated, primary focus of the agencies working on regulating AI.

– President Biden's EO in February, 2023 focused on "further advancing racial equality and support for underserved communities through the federal government."

– October 30 EO focuses of limiting harm caused by discrimination and bias in housing, healthcare, and justice, directs the DOJ to investigate and prosecute

– The Blueprint for an AI Bill of Rights also focuses on the risk of unlawful discrimination

Topic: Bias

– On April 25, 2023, four federal agencies (CFPB, DOJ Civil Rights Division, EEOC, and FTC) released a joint statement on enforcement efforts against discrimination and bias in automated systems.

– The agencies reaffirmed that their enforcement authority applies to automated systems.

– The agencies agree that automated systems may contribute to unlawful discrimination and otherwise violate federal law.

Topic: Fair Credit Reporting Act

– The Fair Credit Reporting Act addresses automated decision making; financial services companies have been applying these laws to machine-based credit underwriting models for decades.

– The FTC has provided some guidance on notices that may be required when AI-based tools are used to make decisions:

  – *"If you make automated decisions based on information from a third-party vendor, you may be required to provide the consumer with an "adverse action" notice.*

Topic: Competition / Antitrust

– The FTC has raised competition concerns with respect to the development and use of AI technologies in the commercial environment.

  – In their article "Generative AI Raises Competition Concerns" (June 29, 2023), they discuss how the FTC's Bureau of Competition, working closely with the Office of Technology, and is focused on "ensuring open and fair competition, including at key inflection points as technologies develop."

Topic: Understandability and Transparency

– Transparency and understandability with respect to AI refers to the ability for regular people to see how an AI model works and understand how it makes decisions.

– October 30 EO calls for AI watermarking to protect consumers from fraud and deception in use of AI

– Transparency also relates to individuals understanding that the product, service, or information they are receiving is being provided by an automated system.

  – This connects to our earlier discussion related to advertising, and the FTC's concerns about deceptive trade practices.

Topic: Accuracy and Reliability

- The accuracy and reliability of AI-generated content is of primary concern to regulators and has been raised by the FTC in their investigation into OpenAI.

- In the CID, the FTC stated it seeks information on complaints or reports that LLMs generate statements about individuals that are false, misleading, disparaging, or harmful, any procedures for addressing these complaints/ reports, and any policies/ procedures for excluding those outputs.

- Ultimately asking: Do the LLMs operate "unfairly" under Sec. 5 of the FTC Act by causing harm when conveying misleading or false information about individuals.

Looking Ahead

California

Through its privacy legislation and Privacy Protection Agency, the state is developing rules and regulations related to the development and use of automated technologies including AI.

- On February 10, 2023, the CPPA published an invitation for preliminary comments on its second round of CPRA rulemaking related to three areas: cybersecurity audits, risk assessments, and automated decision-making. The Agency asked a series of questions aimed at gathering more information from all potential stakeholders on how to craft these regulations.

- On September 8, 2023, the CPPA Board met and discussed rulemaking activities surrounding draft risk assessment regulations

Compare: EU AI Act

– The <u>EU AI Act</u> takes a risk-based approach including restrictions based on how dangerous lawmakers predict an AI application could be.

- – Bans tools lawmakers deem "unacceptable" (e.g., systems for law enforcement to predict criminal behavior based on analytics).
- – Introduces limits on technology considered "high risk" (e.g., tools influencing voters/elections or recommendation algorithms used on social media platforms).
- – Companies would be obligated to label, or watermark AI-generated content to prevent spreading falsehoods.

US Legislative Efforts

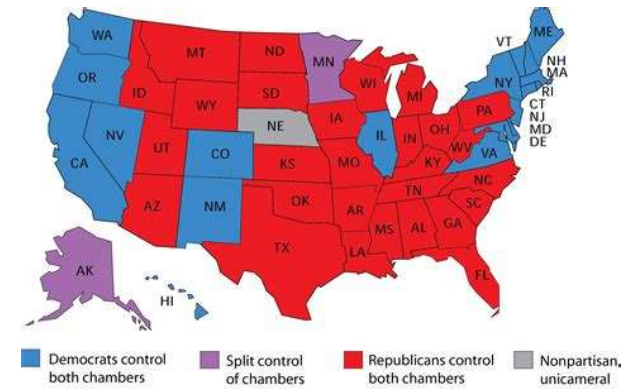Congress is currently working on a series of proposed bills related to AI.

– Sen. Schumer is leading a bipartisan group to craft AI legislative framework; said Congress is months away from considering any proposed laws.

– Sens. Josh Hawley and R. Blumenthal (on June 14, 2023) proposed a bill to ensure that the immunity online companies have under Section 230 of the CDA doesn't extend to claims based on GenAI.

– 18 US State attorneys general are focused on the importance of accountability and transparency. The AGs have called for the National Telecommunications and Information Administration to develop a "risk-based approach" to regulation of AI like that of the EU AI Act. The state AGs also want to make sure they have concurrent enforcement authority

Bipartisan Framework for U.S. AI Act

– A Top-Down Legislative and Regulatory Approach

– Establish a Licensing Regime administered by an Independent Oversight Body

– Ensure Legal Accountability for Harms -- PRA

– Defend National Security and International Competition

– Promote Transparency

– Protect Consumers and Kids

Democrats control both chambers · Split control of chambers · Republicans control both chambers · Nonpartisan, unicameral

State AI Laws and Proposed Bills

- Ten states have <u>laws going into effect in 2023</u> which include AI regulations.

- Several states proposed task forces to investigate AI.

- Several states proposed bills in the current legislative session.

Of note is <u>New York City's AI in employment bill</u> which provides rules for using "automated employment decision tools" in employment decision-making.

Conclusion: Where We Are Now

– There is a large body of law that exists now and that regulates AI
  – Consumers generally: FTC Act (Deception, Unfairness), state UDAP law
    – Advertising, privacy, data security
  – Credit context: ECOA
  – Data for credit, employment or insurance decisions: FCRA
  – Employment context: Civil rights laws
  – Business context: Intellectual property law, product liability law
– Issues specific to AI:
  – Transparency, human alternative / intervention, safety, accuracy, reliability

Conclusion: Looking Ahead

– Pending legislation chances
  – Targeted (e.g., NY AI in employment)
  – Comprehensive (e.g., Schumer model; Blumenthal / Hawley model
– In the meantime…
  – Interesting market developments: Microsoft, Adobe, IBM indemnifying users for copyright violations. Is more like this coming? The market seems to be calling for it. (E.g., privacy-safe training datasets)

Thank You!

Questions & Contact Information

D. Reed Freeman, Jr.
Reed.Freeman@afslaw.com

Eva Pulliam
Eva.Pulliam@afslaw.com

Sheila Colclasure
Sheila.Colclasure@interpublic.com