Future Proofing Data & Tech Ecosystems: Preparing for Federal Action

Stacey Rolland
Senior Vice President, Emerging Technologies and Data Policy
June 2021

www.forbes-tate.com

Regulatory Uncertainty

- **Emerging technologies, big data, and algorithm-based business practices** have created **gray spaces** within multiple regulatory frameworks – the spaces Congress and federal agencies are now navigating and seeking to clarify.
- Data privacy has been under the national spotlight, but there are other areas of regulatory attention that impact the **larger data ecosystem**.
- Today, we'll look at where legislative and regulatory attention is focused and where it might go.
- We'll also talk about affirmative steps companies can take today to successfully meet future regulatory requirements.
- Ultimately, as you're planning and implementing policies and governance within your data ecosystem, there are **things you can do now** to future proof your company for the regulatory regimes to come.

Legislative Proposals to Regulate Emerging Technologies and Data Ecosystems

E.U.: Proposal for a Regulation on a European Approach for AI

U.S.: Algorithmic Accountability Act
Senators Wyden (D-OR) and Booker (D-NJ)
(Rep Clarke (D-NY)

U.S.: Algorithmic Fairness Act
Senator Coons (D-DE)

First Legislative Efforts to Regulate AI and Data Ecosystems

Most early legislation in the U.S. is focused on *investments* and growing the AI workforce and calling for readiness/national strategy on AI

Unlike with data privacy legislation, legislative efforts to *regulate* emerging technologies, algorithms, and data ecosystems have been not based solely on establishing broad principles or creating consumer rights but take a **prescriptive risk-based** approach

First Legislative Efforts to Regulate AI and Data Ecosystems

- **E.U.: Proposal for a Regulation on a European Approach for Artificial Intelligence**
  - Affects companies whose AI systems, decisions, or outputs would impact EU citizens

- **U.S.: First legislative efforts to regulate AI:**
  - Algorithmic Accountability Act
  - Algorithmic Fairness Act

While these legislative proposals are just that, proposals, they can tell us a lot about the direction of regulatory expectations in the larger data ecosystem.

These legislative proposals have in common: Risk-Based Approach

1. **Documentation**
2. **Audit Trails**
3. **Assessments**

LEGISLATIVE EFFORTS

Common Requirement	E.U.: Proposal for a Regulation on a European Approach for AI	U.S.: Algorithmic Accountability Act	U.S.: Algorithmic Fairness Act
Purpose	Create first ever legal framework on AI to address the risks of AI and **position Europe to play a leading role** globally in development of secure, trustworthy, and ethical AI	**Requires assessments** of high-risk automated decision-making systems, such as AI and ML	Prevent companies from acting on algorithmic eligibility determinations **deemed unfair** by FTC's unfairness standard
Regulation of High-Risk AI	**Bans AI** that: 1. Uses subliminal techniques to manipulate behavior that causes or is likely to cause physical or psychological harm; 2. Exploits vulnerabilities of a group due to their age or disability 3. Government-conducted social scoring. High-risk AI systems fall within specific **use** categories: 1. Biometric identification 2. Critical infrastructure 3. Education and vocational training 4. Employment, workers management, and access to self-employment 5. Access to essential private and public services 6. Law enforcement 7. Migration, asylum, and border control 8. Administration of justice and democratic processes	High-risk defined broadly within **risk** categories: 1. Poses significant **risk to privacy or security** or results in/contributes to **inaccurate, unfair, biased, or discriminatory decisions** 2. Makes or facilitates human **decision-making** based on systematic and extensive **evaluations of consumers** 3. Involves **personal info of significant number** of consumers regarding race, religion, health, gender, gender identity, criminal convictions or arrests 4. Systematically **monitors** public places 5. Other criteria set by FTC	N/A

LEGISLATIVE EFFORTS

Common Requirement	E.U.: Proposal for a Regulation on a European Approach for AI	U.S.: Algorithmic Accountability Act	U.S.: Algorithmic Fairness Act
Assessments: • **Identify and analyze risk** • **Adopt and detail risk mitigation and controls** • **Manage data and assess for assumptions, suitability, bias, and gaps**	Risk management system assessment with continuous iterative process through entire lifecycle of high-risk AI system must: 1. Identify and analyze risks 2. Adopt risk management measures, mitigation, and controls 3. Test risk management measures prior to market Data Governance: Training, validation and testing data must have appropriate data governance and management of design, collection, preparation, assumptions, suitability, biases, gaps, and how they're addressed.	Assessments must: 1. Describe the system in detail 2. Assess the relative costs and benefits of the system 3. Determine the risks to the privacy and security of personal information 4. Explain the steps taken to minimize those risks, if discovered Data Governance: Training data must be assessed "for impacts on accuracy, fairness, bias, discrimination, privacy, and security" and must include, among other things, a description of the duration for which the system stores personal information and results, what information about the system is available to consumers, the extent to which consumers have access to the results of the system and may correct or object to its results.	N/A
Documentation / Audit Trail: • **Maintain detailed documentation of system/algorithm development, training, and performance.**	Maintain technical documentation on how high-risk AI systems were developed and how they perform over time. Retain for 10 years.	N/A	Create an audit trail for each algorithmic eligibility determination about a consumer, preserving records about the data and methodology used to make the determination, how the algorithm was created and trained, and the ultimate decision rendered.

Federal Agencies Are Taking An Active Approach

Federal Trade Commission

Consumer Financial Protection Bureau

Other Financial Services Agencies

Federal Trade Commission (FTC)

FTC has the authority to enforce multiple regulatory areas, including unfair or deceptive acts or practices in or affecting commerce, under Section 5 of the FTC Act.

On April 19, the FTC provided **new guidance** on the commercial use of AI and the steps companies must take to ensure AI does not exhibit bias:

- FTC intends to use its full authorities (Section 5, FCRA, ECOA) to regulate data gaps, algorithm design flaws, and transparency.
- AI developers should control for discriminatory outcomes of algorithms, retest over time, provide transparency, and seek help from independent sources to evaluate for potential bias they might have missed.
- Companies should disclose potential gaps in data sets used in AI systems.
- Companies must disclose to users how they use consumer data.

FTC: "Hold yourself accountable – or be ready for the FTC to do it for you."

FTC Settlement with Everalbum, Inc.

In January, the FTC reached a settlement in an enforcement action with photo app Everalbum, Inc. alleging they deceived users about their use of facial recognition.

The FTC ordered Everalbum to delete not only the biometric data but ***also the models and algorithms trained on it.***

Things to look out for from the FTC include:

1. Expect larger and more frequent **fines** and **greater coordination** with the Consumer Financial Protection Bureau and other agencies.
2. Legislation may provide **expanded regulatory authority** for the FTC.
3. The FTC may start to **stretch their interpretation** of unfair and deceptive practices in the coming years.

Watch This Space: Financial Services

When it comes to what the future of regulation in emerging technologies and data ecosystem, look at financial services for a path forward.

With its mature regulatory regime, the financial services sector will help lay the groundwork for how the United States tackles any future national strategy on emerging technologies and data ecosystems and how the U.S. approaches harmonizing policies across the country and the globe.

Today, the attention of financial services regulators is focused on a number of fronts and foundations are being set for upcoming rulemaking and guidance.

Consumer Financial Protection Bureau (CFPB)

In June 2020, the Supreme Court held the CFPB Director could be fired at-will, which converted the CFPB from an independent agency into an **executive agency**. A Biden White House is likely to leverage the CFPB to serve its **policy agenda**.

The CFPB Director nominee is **Rohit Chopra**, a current FTC Commissioner and close ally of Senator Elizabeth Warren.

What we might expect from CFPB:

- Greater **use of enforcement** and other authorities
- Attention on **unfairness and deception** of consumers during COVID, fair lending (student loans, mortgages, etc), **innovation**, fintech, open banking, and data security
- Increased use of **guidance**
- Potential **inflation of penalties**
- Greater **cooperation** with other agencies and state attorneys general

Overall, CFPB emphasizes that business practices, no matter how rigorous, must be documented and exist within some risk management framework.

CFPB: Rulemaking in Section 1033 of the Dodd-Frank Act

- Section 1033 is the most detailed federal discussion to date on **data rights**, **data access**, and the downstream effects of **data flows**.
- In October 2020, CFPB released an Advance Notice of Proposed Rulemaking (ANPR) on Section 1033 of the Dodd-Frank Act regarding **authorized data access standards and practices**.
- CFPB is considering regulating how consumers can **access their data** via *direct access* through their financial institution's online servicing portal or mobile app vs. through *authorization* in which the consumer allows a third party (data aggregator) to access their financial account data.
- The CFPB rulemaking could have **far-reaching implications** for how consumers, banks, and non-bank fintechs access and share data.

CFPB: Section 1033 Questions

Issue	Question
Benefits and Costs of Consumer Data Access	What are the costs and benefits of authorized data access versus direct access to consumers and data holders and to competition and innovation?
Competitive Incentives and Existing Market Dynamics	What competitive incentives currently exist in the market and how should the Bureau's rulemaking account for existing market dynamics while promoting further competition?
Industry Standard-Setting vs. Regulatory Standards	Should the CFPB expect broad-based standard-setting work by the industry to enable and facilitate authorized data access and encourage, rather than impede, competition and innovation? Should the Bureau let the standard-setting play out before deciding whether to prescribe specific standards?
Access Scope	Who should be "an agent, trustee, or representative" that can exercise access rights on behalf of a consumer and should different processes apply when third parties access data on behalf of a consumer?
Consumer Control and Privacy	Do consumers understand the actual movement, use, and storage of their data?
Data Security and Accuracy	Do existing legal requirements or market incentives effectively mitigate data security and accuracy risks or should the rulemaking do so?

CFPB: Section 1033

Comments on the ANPR raise an array of significant issues that are also relevant to other data ecosystems:

- Restrictions on **data use**
- Downstream **liability** (when data shared with 4th+ parties)
- **Conflicts** with other regulations
- Whether **third+ parties** accessing data should be held to the same regulatory requirements as data holders in data security and use - and contribute to data security costs of data holders.

The next opportunity to comment on Section 1033 will be the Notice of Proposed Rulemaking (NPR).

Other Financial Services Agencies Looking at AI

On March 29, 2021, the Federal Reserve, CFPB, Federal Deposit Insurance Corporation (FDIC) and National Credit Union Administration (NCUA) released a Request for Information (RFI) seeking information on **how financial institutions are using AI and managing AI risks** with the goal of ensuring the financial system has a regulatory framework that enables innovation in a safe and responsible way.

The deadline for public comment has been extended to **July 1.**

Watch this space for future regulatory guidance.

How You Can Future Proof:
Internal and External Engagement

Future Proofing

With policymakers beginning to act, it is time for companies to move beyond their wait-and-see approach and start thinking about a regulatory strategy and government engagement.

Major aspects these proposals and approaches have in common:
assessments, audit trails, documentation.

Even if future guidance comes in the form of a principles-based approach, **it behooves companies to take a more risk-based approach**. Having even a basic risk and control framework and clear documentation will better set you up to meet requirements even in a principles-base regulatory environment.

Internal Engagement

Employers must already be aware of the potential for disparate treatment or impact claims under equal employment opportunity laws like Title VII and the Americans with Disabilities Act (ADA)...

...but companies should prepare now for **increased government oversight** of AI and **enhanced customer expectations** regarding the lawful and ethical use of AI.

Internal Engagement

To prepare effectively, companies should:

- **Document key decision-making** through the data ecosystem.
- Begin creating **risk, impact, and data security assessments** that ensure accountability, risk identification, controls, and effective challenge.
- Implement an **audit system** for regularly checking data, algorithms, systems, procedures, and frameworks for unintended inputs and results.
- Make sure there **aren't hidden incentives** within your organization to greenlight decisions that have risks that haven't been thoroughly assessed (create a culture that supports speaking up).

Internal Engagement

- Develop **training programs** for those engaged in AI development and data processing to raise awareness of the inherent biases in data. Train anyone who is part of the entire data ecosystem.

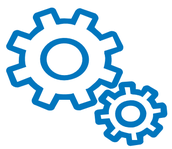
- The FTC already put you on notice: Make sure the claims your company is making are **true**. This might seem like table stakes, but the financial and reputational risk of an FTC fine based on deceptive practices is significant. Data policy and governance are complicated and words matter.

- Increase **transparency** to consumers regarding data and AI use.

- Ensure you have **accountable executives** directly engaged in procedures empowered to investigate and rectify bias and security risks in AI systems. Solicit buy-in and support from other teams/executives. Consult with outside experts on best practices and additional risk mitigation strategies.

External Engagement

Companies are increasingly calling for **clarity** in the form of regulatory guidance to ensure the sustainability of their emerging technology systems and to build trust among their target customers.



Policymakers are seeking to **work together** with companies to better understand their technologies and to work in partnership to create workable solutions to industry problems, protect citizens, and encourage innovation.

Companies across all sectors should build **relationships** and **partner** with policymakers.

Companies that foster positive working relationships with policymakers and partner to craft definitions and shape approaches to the future of their industry will have a **significant competitive advantage**.

Conclusion

Ultimately, your companies are investing significant resources into using and protecting valuable data. Just because there aren't clear guidelines from the federal government today, doesn't mean there won't be regulatory requirements in the coming years.

1. In the future, regulators will expect to see documentation of the decision-making processes and risk mitigation you are going through today.

2. Look to engage with the federal government to educate them about your innovations and help shape the regulatory environment and market in which you're operating.

Partnering with Policymakers > Waiting to see what happens and having to quickly adjust

FORBES | TATE
PARTNERS

CONTACT

Stacey Rolland
202.422.2271
srolland@forbes-tate.com

ADDRESS

777 6th Street NW
8th Floor
Washington, DC 20001