Center for AI and Digital Policy

"Request for Information and Comment on Financial Institutions'

Use of Artificial Intelligence, including Machine Learning"

DEPARTMENT OF THE TREASURY Office of the Comptroller of the Currency

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

FEDERAL DEPOSIT INSURANCE CORPORATION

BUREAU OF CONSUMER FINANCIAL PROTECTION

NATIONAL CREDIT UNION ADMINISTRATION

OCC-2020-0049

The Center for AI and Digital Policy (CAIDP) welcomes this request for information and comment on the use of artificial intelligence (AI). The CAIDP is a non-profit organization that advises governments and international organization regarding artificial intelligence (AI) and digital policy. Our report *Artificial Intelligence and Democratic Values* ranked 30 countries on their regulatory framework governing AI. One of the key recommendations that we made was the "countries should ensure public participation in AI policymaking."[1] With regards to the questions that you have posed we have chosen to provide our expertise on questions 12, 14, and 17.

What are the risks that AI can be biased and/or result in discrimination on prohibited bases? Are there effective ways to reduce risk of discrimination, whether during development, validation, revision, and/or use? What are some of the barriers to or limitations of those methods?

Artificial Intelligence (AI)-based systems are employed in various sensitive domains and have recently become more prominent in decision-making processes across the public and private sectors. Consequently, they enable beneficial as well as nefarious activities. For example, AI systems can approve or deny job applications, medical treatment, or loans from bank, recommend specific movies, or articles to read. These systems can also make biased decisions.

[1] CAIDP, Artificial Intelligence and Democratic Values at 4 (Recommendations) (the "CAIDP Report"), https://caidp.dukakis.org/aisci-2020/

The sources of such decisions vary. Generally speaking, human cognitive biases[2] and lack of complete data can seep into AI systems and result into discriminatory decisions. Often, biased decisions of these systems occur in the data set that train AI tools. They often replicate social problems such as racist and gender-related biases. Amazon's a hiring algorithmic system[3] is a famous example. This system concerns algorithms that can make autonomous decisions of job applications. The Amazon system was systematically biased against black female applications, relying on historical data which favors white males in job market. Consequently, such scenarios can have severe negative effects on human rights. This in turn results in creating disadvantaged communities in the society.

In our recent publications *Artificial Intelligence and Democratic Values*,[4] a comprehensive report on the AI policies and practices in 30 countries, CAIDP explained that bias can exist at every stage of the development and deployment of AI systems.[5] To prevent such practices, we recommended that "AI actors should, based on their roles, the context, and their ability to act, apply a systematic risk management approach to each phase of the AI system lifecycle on a continuous basis to address risks related to AI systems, including privacy, digital security, safety and bias."[6] Moreover, we recommend the following steps to tackle the challenges resulting from AI systems: 1) understanding bias, 2) mitigating bias, and 3) allocating responsibility. As for the first point, we recommend a clear and comprehensive understanding of the source of bias and in which particular part of the decision-making process and in what forms has the bias occurred. Secondly, we recommend that technical and non-technical experts are involved in the development of these system. Finally, the last point concerns, we recommend "The Right to a Human Determination," which "reaffirms that individuals and not machines are responsible for automated decision-making."[7]

Concerning the barriers/limitation of these methods, the primary concern is algorithmic opacity in automated decision-making systems. Once opacity replaces transparency, individuals concerned face difficulties to challenge the decisions of these systems. Both for regulatory oversight and consumer protection, *financial institutions should be required to maintain AI systems that are transparent, provable, explainable, verifiable, and subject to third party auditing, A consumer of a financial service that is based on an AI-derived output should have the opportunity to meaningfully contest an adverse decision.*

[2] Several studies discussed this problem, see for example, Moss-Racusin, Corinne A., et al (2012). Science faculty's subtle gender biases favor male students. Proceedings of the National Academy of Sciences 109.41: 16474-16479

[3] Reuters, *Amazon scraps secret AI recruiting tool that showed bias against women*, October 2018

[4] Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values* ("CAIDP Report") (CAIDP 2020), https://caidp.dukakis.org/aisci-2020/

[5] See Defender of Rights, *Algorithms: preventing automated discrimination* n. 19 (May 2020), https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/synth-algos-ennum-16.07.20.pdf.

[6] CAIDP Report 326

[7] CAIDP Report 335

Please describe any particular challenges or impediments financial institutions face in using AI developed or provided by third parties and a description of how financial institutions manage the associated risks. Please provide detail on any challenges or impediments. How do those challenges or impediments vary by financial institution size and complexity?

A study from 2020 outlined that the two key areas in which financial institutions utilized AI was in Sales and Marketing and Risk[8]. With financial institutions often lacking the expertise third party companies are often employed to develop the AI systems used in their various departments. There are several risks that may arise from this. This first one is that data breach may exist with the use of third-party applications. Secondly lack of control over methods utilized by the third-party applications may result in violation of existing legal and regulatory frameworks . The third issue concerns explainability and interpretability of third-party AI systems.

The essential ingredients driving AI driven applications utilized by financial institutions is data. Leaving this is in the hands of a third party poses significant risks. To demonstrate this one of the most well-known examples would be the Marriot data breach. When Marriott acquired Starwood unbeknownst to them third party actors had gained access to their reservation system platform which then resulted in a data breach leaking individual private information including credit card details[9]. This directly resulted in more that 5% decrease in Marriott's share price[10] as well as £18.4 million fine by the UK Information Commissioner for violation of General Data Protection Rules.[11] The breach of sensitive personal data is an ongoing risk for financial institutions that should be considered. Any data breach utilizing AI techniques or enabled by third parties may also have implications for share price and liability.

One solution could be to require financial institutions to appoint an in-house Data Protection Officer. The GDPR mandated this for financial institutions holding data for European Residents.[12] In the US however there is no such obligation except for undertakings regulated by HIPAA.[13] Larger financial institutions with a presence in Europe already have to fulfill this obligation however applying the requirements to all jurisdictions utilizing third party AI based

[8] Suparna Biswas et al., AI-bank of the future: Can banks meet the AI challenge?, (10 May. 2021), https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge#

[9] Tiffany Newsome, The Marriott/Starwood Data Breach: Why Third-Party Risk Management is Critical During M&A, (May 1, 2021), https://www.prevalent.net/blog/the-marriott-starwood-data-breach-why-third-party-risk-management-is-critical-during-m-a/

[10] Id.

[11] Information Commisioner Office, ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure, (May 3. 2021), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/

[12] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679,Art. 38.

[13] DLA Piper: *Data Protection Laws of the World: United States,* (May 3, 2021) https://www.dlapiperdataprotection.com/index.html

applications would be strong step forward. Furthermore, for smaller financial institutions not already compliant with the GDPR this would mitigate the risk for data breaches domestically.

Another potential risk is the use of third party AI techniques for loan applications and credit approval systems, including violations of the Equally Credit Opportunity Act (ECOA) and the Fair Housing Act and other federal statutes. The third party's aim may be to provide a system which maximizes the financial institutions profits. Third parties often utilize external consumer data in their AI application. An example of external consumer data use was when New York State Department of Financial Services sent out a warning letter to insurer utilizing algorithms in underwriting life insurance]. The New York State agency found that insurers were using homeownership data and higher education qualification among others.[14] The Department found that this was in direction violation of Articles 26 and 42 of the state Insurance Law.[15] This is a clear case that shows the risk in the use of third-party application that may not comply with regulatory obligations. This challenge will present itself in both large and small financial institutions. It is important to note that in large financial institutions this will play a larger role as the number of products they offer are far greater in number.

A solution to this could be a contractual clause in the service level agreement which obliges the third-party provider or developer to provide timely transparency reports with regards to the sets of data that their using and the parameters. In the CAIDP report *Artificial Intelligence and Democratic Values*, we said that "Countries must guarantee fairness, accountability, and transparency in all AI systems."[16] This principle should be applied to financial institutions uniformly to mitigate any potential governance issues. This issue of fairness, accountability, and transparency has been globally recognized. The Monetary Authority of Singapore has also outlined this in their report regarding the use of AI in Singapore's Financial Sector.[17] That report specifically targeted the governance and principles that (Artificial Intelligence and Data Analytics) AIDA firms could use.

We commend the *Third Relationships: Risk Management Guidance and the Interagency Fair Lending Examination Procedure* that the Office of the Comptroller of the Currency has provided. However, we urge you to update the Guidance to reflect the developments that have occurred with the use of AI in financial institutions.

[14] New York State Department of Financial Services, (May 8, 2021), Insurance Circular Letter No. 1 (2019) RE: Use of External Consumer Data and Information Sources in Underwriting for Life Insurance, https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2019_01

[15] Id.

[16] CAIDP Report at 4 (Recommendations)

[17] Monetary Authority of Singapore, (May 9,2021), Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector,mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf

The third issue that we recognized was regarding explainablity and interpretability of AI systems.[18] This problem may be more amplified in smaller financial institutions. Often smaller financial institutions may not possess the resources and expertise to assess and evaluate the process through which the third-party AI application are providing the results. Governor Lael Brainard identified this issue as the "black box problem"[19] where the process to understand the results from the data being input is often "obscured." The result of this is that should there be a miscalculation it may have large consequences should it go unnoticed. *The simple solution is "algorithmic transparency."*

To the extent not already discussed, please identify any benefits or risks to financial institutions' customers or prospective customers from the use of AI by those financial institutions. Please provide any suggestions on how to maximize benefits or address any identified risks.

Another key area where AI could be used extensively in the financial services sector is in anti-money laundering (AML). The cost of AML compliance is the US is approximately $23.5 billion per year.[20] We would like to note that Senator Mark Warren introduced the Illicit Cash Act which promotes the creation of a Financial Technology Task Force.[21] An interdisciplinary task force would be key in targeting terrorism financing and threats to national security. Given the recent rise in the uses of cryptocurrency financial institutions needs to adapt to be able to track illicit transactions. Furthermore, the use of AI may prove to be a more scalable operation. *It is important though that human oversight in present in the use of AI in the AML sectors. In our report one of the recommendations was that there be "robust mechanisms or independent oversight of AI systems."[22]*

A specific area of AML where AI/ML could be utilized would be in vetting individuals who are listed have sanctions against them or have been blacklisted by the US government. Manually going through these lists may prove to be a cumbersome and time-consuming task which may result in errors. This would be useful for large financial institutions who are operating in multiple countries and have comply with KYC/AML regulations of these jurisdictions.

The third risk of AI that needs to be highlighted is the use of natural language processing (NLP) in the financial markets. NLP refers to the use of "utilizing textual data improve modeling

[18] Artificial Intelligence/Machine Learning Risk & Security Working Group (AIRS), (May 8, 2021), Artificial Intelligence Risk & Governance, https://ai.wharton.upenn.edu/artificial-intelligence-risk-governance/#_ftn7

[19] Lael Brainard, (May 10, 2021), Supporting Responsible Use of AI and Equitable Outcomes in Financial Services, https://www.federalreserve.gov/newsevents/speech/files/brainard20210112a.pdf

[20] World Economic Forum, *How AI is transforming the fight against money laundering* (Jan. 17, 2019), https://www.weforum.org/agenda/2019/01/how-ai-can-knock-the-starch-out-of-money-laundering/

[21] Text - S.2563 - 116th Congress (2019-2020): ILLICIT CASH Act, S.2563, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/senate-bill/2563/text.

[22] CAIDP Report at 4 (Recommendations)

of the financial market dynamics."[23] Nowadays due to the growth in media and social media outlets such as Twitter in Facebook this has become a widespread practice among financial institutions to forecast the outcome of various trading models.

In a recent study, researchers found that datasets consisting of the same news articles led to "herd behavior" and often ignored the outliers. By ignoring the outliers and solely relying on the sentiment ascertained from the majority this could lead to "splash crash" across many asset classes. *We believe that there needs to a stricter form of regulation that can tackle these deep learning models which could be the impetus for further financial crises.*[24]

A second issue is the need to verify the source of data used in NLP. While news API such as Bloomberg and Reuter charge customers for information and undergo editorial review, social medial platforms are often the first report any major events that may affect the financial markets. One of the main problems is the absence of verification to ascertain the validity of the statements being made on social media platforms. While steps have been taken to prevent the spread of false narratives in ML context the categorization between opinion and facts may become harder to ascertain. There is an additional risk that AI-based techniques, such as GPT-3, may play a larger role in the creation of news articles, as this will allow media organizations to generate advertising revenue at very low cost.[25] *For this reason, we recommend that there be mandatory strict human oversight process.*

As a final step to we would like to direct your attention to use the OECD AI Principles[26], which the United States had endorsed, specifically the second and fourth principle:

> 2. *AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society.*
>
> 4. *AI systems must function in a robust, secure and safe way throughout their lifetimes, and potential risks should be continually assessed and managed.*

Both these principles should be adhered in the use of AI in the financial markets and the federal agencies should ensure this through their regulatory actions.

[23] Xing, Frank Z., et al. "Natural Language Based Financial Forecasting: A Survey." Artificial Intelligence Review, vol. 50, no. 1, June 2018, pp. 49–73.
[24] Vicari, M., Gaspari, M. Analysis of news sentiments using natural language processing and deep learning. *AI & Soc* (2020). https://doi.org/10.1007/s00146-020-01111-x
[25] James Vincent, *OpenAI's text-generating system GPT-3 is now spewing out 4.5 billion words a day: Robot-generated writing looks set to be the next big thing,* The Verge (Mar. 29, 2021), https://www.theverge.com/2021/3/29/22356180/openai-gpt-3-text-generation-words-day
[26] OECD, Forty-two countries adopt new OECD Principles on Artificial Intelligence, (May 22, 2019), https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm

Thank you for your consideration of our views.

Marc Rotenberg, President
Center for AI and Digital Policy

Max Birla
Georgetown LLM student
CAIDP Research Group

Lucas Laurentius Olivier Cardiell
European University Institute, PhD candidate
CAIDP Research Group