DATA BOILER TECHNOLOGIES, LLC

BIG DATA | BIG PICTURE | BIG OPPORTUNITIES

*We see big to continuously boil down the essential improvements until you achieve sustainable growth!*

✉ info@databoiler.com databoiler.com

*30 January 2026*

*via Electronic Mail (policy-ai@fca.org.uk)*

Mr. David Geale – Executive Director for Payments and Digital Finance
Ms. Jessica Rusu – Chief Data, Information and Intelligence Officer
Dr. Henrike Mueller – AI Strategy Team Manager, Advanced Analytics

**AI Policy, Financial Conduct Authority**
12 Endeavour Square, London E20 1JN

**Re: Current and future uses of Artificial Intelligence (AI) + financial services regulatory framework**[1]

Dear Director Geale, Ms. Rusu, Dr. Mueller and fellows at the FCA AI Lab,

On behalf of Data Boiler Technologies, I am pleased to provide the U.K. Financial Conduct Authority (FCA) – AI Lab with our comments on the current and future uses of AI related to the financial services' regulatory framework. As an inventor of patented solutions (Europe, US, Canada, Singapore, Japan, Australia) in signal processing, ensemble learning, trade analytics, time-lock cryptography, etc., we are among the first to pin point the true '*AI Risks*'[2] (= downfall of humanity, including but not limited to the possibility of AI taking down the energy grid). A key takeaway:

Respect human's creativity and ingenuity – Enhance Copyright Laws to aligns AI rights and obligations

1. What AI use cases are you considering or exploring in your firm/organisation? What do transformative AI use cases look like in the next 5 to 10 years?

   The typical AI use cases include: (a) usage of GenAI and natural language processing tools to extract and summarize information from multiple sources for investment research; (b) Robo-advisory; (c) automating the regulatory research and compliance process; (d) big data credit models; (e) automating repetitive back-office tasks for operational efficiency; (f) chatbots for client services, etc. We are aware that some are experimenting with how machine learning can improve their portfolio management model in further optimizing asset allocation and rebalancing processes. Elites market makers, high-frequency trading firms, quant funds, multilateral trading facilities are using advanced AI/ machine learning for algorithmic trading, identifying toxic versus natural liquidity, adverse selection detection, etc.

   For us at Data Boiler, we focus on real time detection of anomalies and suspicious patterns that can be indicative trade irregularities. Our patented solutions that crossover between music and trade provide more accurate detection of onset signals / trade irregularities at accelerated speed and are more tolerable to unsynchronized clocks/ timestamp issues + more. It addresses the inherent problem of data imprecision (50± milliseconds timestamp tolerance)[3] and reduces false positives/ negatives. It is the ONLY solution to address IOSCO – CR12/ 2012[4] challenges to effective market surveillance. It works similarly to music plagiarism detection but for market and risk monitoring.

   We believe pattern recognition should NOT be the privilege of those elite firms who have the money for AI. We envisage development of a 'sound library'[5] that would accelerate algo development lifecycle and foster creative discovery of unknown unknowns. New ways to do trading analytics with a community library of known lessons to encourage participation. It would grow the overall pie, make the market safer, and promote fairness.[6]

[1] https://www.fca.org.uk/ai-input-zone
[2] https://www.linkedin.com/pulse/ai-risks-downfall-humanity-kelvin-to-yhzge/
[3] https://tabbforum.com/opinions/is-clock-synch-the-cats-fatal-flaw/
[4] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD389.pdf
[5] https://www.databoiler.com/index_htm_files/DataBoiler%20SoundLibrary.pdf
[6] https://www.databoiler.com/index_htm_files/DataBoiler%20BIG%20OPP.pdf

We foresee and concur that AI will move beyond summarizing research to act as a 'lab assistant' to generate hypotheses, control experiments via apps, and collaborate with human technologists. In the next 5 to 10 years, autonomous operations, agentic maintenance, and micro-workshops would flourish with a trend towards mass customization, hyper-personalized services. The current chatbot interfaces will evolve into Agentic AI—specialized digital employees that proactively anticipate needs.

2. Are there any barriers to adopting these use cases currently, or in the future?

On June 12, 2025, the US Securities and Exchange Commission (SEC) has formally withdrawn the problematic proposal from the last administration about "*Predictive Data Analytics*"[7] that was detrimental to AI innovation. Per our 2023 submitted comments to the SEC,[8] we argued that "*the scope is overly broad and would become a tollgate every time an investment firms procures new technology, they will have to first consult a law or consulting firm – result in, the 'non-TECH bureaucrats' regulating the 'TECH professionals' and corruption.*" The UK FCA AI Lab should observe and heed from this lesson.

3. Is current financial services regulation sufficient to support small firms to embrace the benefits of AI in a safe and responsible way, or does it need to evolve?

Per our comment letter to the US White House Office of Science and Technology Policy,[9] "*the foundation of a responsible AI is NOT about how good one person can articulate or reveal the secret ingredients of an AI to others. Unfortunately, many existing financial regulations are based on big law or consulting firms help their elite clients to brag about their policies and procedures to pursue enforcement, rather than reviewing real substance in improving controls. The related compliance burdens are ways for Elites to suppress smaller competitors who cannot afford to pay the big law or consulting firms. In case something bad happened, Elites leverage on the clout of big law or consulting firms to shoulder the blame. Small AI firms should allow to compete with larger counterparts. We despise policies exacerbating gap between the 'Haves' and 'Have-Nots'.*" We and other small AI developers would require diplomatic support before we consider setting ourselves abroad in sensitive TECH such as AI.

4. What specific changes or additions to the current regulatory regime, or areas of further clarification/guidance, do you think are needed?

One cannot jump to the 'How' when the 'What' has NOT been properly defined. Despite the EU being the first to come up with their AI Act, there is NO first mover advantage in rule making. It is better late than never if we can get it right when framing the regulatory solutions to the problems in the AI space.

AI is NO ordinary '*machine-based systems*' or '*automations*,' but a '*cognitive system*' capable of '*learning*' to continuously improve the Functioning of a Computer / to any Other Technology or Technical Field (e.g. a GPS Satellite system is NOT AI, but traffic predictions and personalized recommendations are). By referring to AI as '*cognitive*,' the focus is on the system's internal (mental like) processes, rather than SOLELY on external behaviors and consequences.

Learning per the '*Dog Salivating Theory*'[10] that nurtures voluntary behavior by pairing external conditioned stimulus to associate two or more phenomena, such technique alone does NOT constitute it as AI. Computational techniques that

[7] https://www.sec.gov/files/rules/proposed/2023/34-97990.pdf
[8] https://www.databoiler.com/index_htm_files/DataBoiler%20SEC%2020231010%20Predictive%20Analytics.pdf
[9] https://www.databoiler.com/index_htm_files/DataBoiler%20WHOSTP%2020251027R.pdf
[10] https://cavcanine.com/classical-conditioning/

mimic pet training in itself are insufficient or unlikely to pose an existential threat to humanity, except exploitation of Dopamine for addictive behaviors. Also, the presence or absence of '*operant conditions*'[11] could merely be automation in itself to modify voluntary behavior through external consequences (reacting to the laws) of reward and punishment. Without combining it with other internal (mental like) computational techniques, such systems should NOT be considered as AI.

CAPTCHA[12] – a security test that uses a '*Turing test*'[13] to differentiate between humans and bots is NOT AI in itself. However, Google reCAPTCHA system is part of an AI that consists of internal processes (e.g. keylogging[14] to track and analyze user interactions, such as mouse movement and typing patterns) to determine if a user is human. Keylogging without a user's consent could be invasive to privacy; hence it should be a regulated activity. Another computing activity that should be regulated is – the use of AI to help bots bypass CAPTCHA[15] or the like security test, except when used for ethical hacking.

A crawler or web scraper that automatically extracts data from an external environment (web) is NOT inherently an AI. When combining crawler's function with internal processes involving intelligent data analysis to enhance the data collection with contextual understanding (rather than just the keywords search), then such system is an AI.

A scanner or camera to surveil the public area outside of private property is NOT an AI. Adding a sophisticated system that has internal processes to control one or orchestrate multiple surveillance camera(s) to enhance the monitoring with contextual awareness (e.g. facial recognition to analyze identity) is an AI. We despise heavy-handed government policies to brutally force AI firms to censor / filtering so-called '*unsafe behaviors / outputs*' or require adversarial training to ban or reveal what authoritarian may constitute as *'vulnerabilities.'*

We are thankful for the US Vice President JD Vance remarks[16] at the AI Action Summit, in particular *"AI must remain free from ideological bias, and that American AI will not be co-opted into a tool for authoritarian censorship."* It helps address civic concerns over massive government surveillance.[17] NOTE: '*Ideological bias*' is a human bias driven by political or social belief. Whereas '*bias*' in many domains – especially competitive ones like defense or finance – **bias is not just inevitable, it is essential** to: prioritize certain outcomes (e.g. speed over accuracy, stealth over transparency), reflect strategic performance (e.g. risk tolerance, adversary modeling), and/or to exploit asymmetries (e.g. alpha in trading, deception in war).

There are different AI machine learning algorithms, some use cognitive reasoning for multi-step strategic plans (e.g. chess game) where *"bias"* is essential. Others use non-reasoning (or generative) models which excel at fast, pattern-based tasks like content generation or chatbots where consensus building and/or optimization for the most commonly accepted response (consistency in reproducibility of outcomes) is prioritized. One size does not fit all.

Bias can be '*conscious*' and/or '*unconscious*.' A cognitive system does NOT have to be conscious. Neuroscientists believe consciousness could be a distributed process that does not depend on a singular '*self*.' Unconscious bias can

[11] https://psychcentral.com/health/operant-conditioning
[12] https://en.wikipedia.org/wiki/CAPTCHA
[13] https://www.techtarget.com/searchenterpriseai/definition/Turing-test
[14] https://en.wikipedia.org/wiki/Keystroke_logging
[15] https://www.sciencefocus.com/future-technology/ai-vs-captcha
[16] https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-artificial-intelligence-action-summit-paris-france
[17] https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/ethics.html

inflict harm amid unintentional – negligence. Cognitive systems with no recommendations[18] should NOT escape AI responsibilities. '*Bias*' depends on social norm.[19] Social norms evolve overtime.

*'Signal amplification'* is an absolute necessity in sequencing technologies. It enables detection, ensures accuracy via redundancy, and is particularly useful when working with limited input material. However, amplification inherently introduces '*technical bias'* into sequencing data – a known and acknowledged challenge, but it may be better than the inability to generate any data at all.

Trade surveillance processes should *objectively* check if a trade has the effect of altering the worth of a target. It is a *red flag* of market manipulation if the trade caused a '*bias'* in market mechanism. The challenge is how to distinguish between a *systematic technical bias* or human-made *artifact* in data, from *natural evolutionary bias or selection.* Content preference[20] and context bias[21] are highly dependent on the specific use case or application, i.e. largely *subjective* and situational.

'Normalization' is the statistical data smoothing process that meant to address '*bias*.' Yet, whenever one applies computational methods to the data, the relationship between the true '*signal'* and the technical '*noise'* is inherently altered. There is a trade-off in gaining clarity of signal at the potential cost of introducing subtle '*new biases*' or *suppressing* real, but weak, '*signals*.' Strive for the most timely, accurate, relevant, and complete data where possible to avoid excessive manipulation in normalization for the best sequencing results. Unfortunately, the consolidated tape without time-lock encryption to make market data available securely in synchronized time[22] causes '*initial bias*' that exacerbates the gap between subscribers of proprietary feeds and the public consolidated tape.

Hallucination is considered an output that is out of norms. Hallucinations are like dreams (a state of consciousness that one's '*awareness'* of external environments may be out of synch), except dreams may be more vivid / emotion than hallucinations. The five human senses are less active during dreams. When AI sensory attenuation primarily focuses on language or visual images, it undermines other sensory inputs, such as sound, touch, smell and taste, etc.

AI is often being mythologized by humans as all-knowing. People expect instant gratification. Yet, AIs are like *replicas* of humans. There will be occasions of *'I don't know'*, irrelevant fluff being generated, stuttering, or words could not catch up with thoughts. The ability to form and process complex thoughts is distinct from the ability to articulate fluently and coherently. Improve context awareness, better adversary training, use of ensemble learning,[23] and multimodality[24] all contribute to reducing AI hallucinations but cost extra time, effort, and may introduce noise.

Unlike *data* extraction that can be *timely*, *accurate* and *complete* if one is willing to pay extra, *intelligence* may never be 100%. I.e. AI *prediction* or *advice* seldom possess all attributes simultaneously due to in inherent constraints, such as information asymmetry, the tension between speed and quality, cognitive limitations, and the dynamic nature of reality.

Do NOT lambast AI for its hallucinations. Humans often fail to think critically, unable to synthesize information from various sources for evaluating information to find deeper meaning, and lack adaptability and creativity. Yet, humans

[18] https://www.baeldung.com/cs/cognitive-computing-vs-ai
[19] https://en.wikipedia.org/wiki/Social_norm
[20] https://academic.oup.com/joc/article/73/5/463/7190600
[21] https://academic.oup.com/jrsssa/article/185/Supplement_2/S620/7069513
[22] https://www.linkedin.com/pulse/market-data-available-securely-synchronized-time-kelvin-to/
[23] https://www.researchgate.net/publication/381994127_Ensemble_Deep_Learning_and_Machine_Learning_Applications_Opportunities_Challenges_and_Future_Directions
[24] https://www.sdu.dk/en/forskning/cmc/key-terms/multimodality

like to dream and imagine. Should cognitive systems be allowed to dream – a possible indicator of Artificial General Intelligence?[25] AI hallucinations may discover **unknown unknowns** which were previously nonsensical to human. To better understand nuances and enhance AI performance, policy makers should incentivize the industry to turn '*unknowns*' into '*knowns.*'

Lesson from the US – the last administration inappropriately assumed or interpreted '*AI bias*' as systematic and repeatable error in a computer system that creates unfair outcomes, such as disadvantaging a particular gender or race. This contradicts with the current US administration's merit-based policy (EO 14173)[26] that dismantles Diversity, Equity and Inclusion (DEI) initiatives. Trying to *'neutralize'* biases in pursuit of consensus or fairness can dilute a country's strategic advantage, especially when foreign adversaries are not playing by the same rules.

The EU AI Act mandates development of a Code of Practice on General-Purpose AI is problematic. Best practice sharing is not wrong. Concern is – how they would consider *"the Code's design and build coherence where needed"*? Regurgitating GRC tools as AI compliance is the wrong approach. *"Coherence"* limits creativity. Differentiation is what drives innovation. The EU Digital Markets Act aims to ensure *"fair competition and practices among large online 'gatekeeper' platforms like search engines and app store"* is nothing but a protectionism policy. Invoke Antitrust laws may suffice.

China released their *'AI Safety Governance Framework 2.0'* (CN-AISGF2).[27] Their cybersecurity law,[28] computer crime criminal law (Articles 285-287),[29] and Personal Information Protection Law[30] are their broader policies that prioritize their national security and state control. CN-AISGF2 looks undeniably comprehensive as we compared it against the 2022 version of the US NIST-AIRMF (see pages 9-10 of our comment letter).[31] Their usage of familiar GRC best practices make it appealing for foreign jurisdictions to adopt it. The US NIST-AIRMF playbook and related guidelines if blindly continuing the oversimplified '*Govern*' in center of '*Map, Measure, and Manage*' (GMMM) path may end-up similar to CN-AISGF2.

In order for the UK together with the US to exert influence on Global AI policies, the UK and US AI regulatory regime should center the focus on the identified key AI risks (energy; addictive, herd and/or polarized behaviors / destroy humans' abilities to think independently; censorship; hyper optimization; insurgent / unhealthy competition) to mitigate the downfall of humanity.[2] Policy Makers should consider the Asimov's Three Laws[32] and Zeroth (Forth) Law[33] for AI. The ISO 23894 Risk, ISO 42001 management system, and ISO 38507 governance frameworks should be redirected accordingly.

Another lesson from the US – the US Department of Justice's Computer Fraud and Abuse Act (CFAA)[34] has a narrower statute if compared to other jurisdictions.[35] CFAA is meant to target external hackers' unauthorized access and

[25] https://en.wikipedia.org/wiki/Artificial_general_intelligence
[26] https://public-inspection.federalregister.gov/2025-02097.pdf
[27] https://www.cac.gov.cn/2025-09/15/c_1759653448369123.htm
[28] https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/
[29] https://www.warnathgroup.com/wp-content/uploads/2015/03/China-Criminal-Code.pdf
[30] https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/
[31] https://www.databoiler.com/index_htm_files/DataBoiler WHOSTP 20251027R.pdf
[32] https://en.wikipedia.org/wiki/Three_Laws_of_Robotics
[33] https://www.streetdirectory.com/travel_guide/120083/technology/the_fourth_law_of_robotics.html
[34] https://www.justice.gov/jm/jm-9-48000-computer-fraud
[35] https://digitalcommons.harrisburgu.edu/cgi/viewcontent.cgi?article=1006&context=other-works

damage; it does NOT impute liability to internal workers who disregard a use policy. Bypassing code would constitute a cybercrime ONLY if the code is a '*real barrier*'[36] as opposed to a '*speed bump*.' '*Function creep*'[37] is concern we identified with the US FINRA Consolidated Audit Trail (CAT) system.[38] Adverse scenarios[39] with government and bank systems have happened with serve consequences.

The original inventor may never come up with an exhaustive list of usage purposes or anticipate the possible repurpose of his/her technology. It is unjust to require AI firms to *"establish comprehensive and explicit enumeration of AI systems' context of business use and expectations."* Do not expect examiners to truly understand every bit of "*contextual factors may interact with AI lifecycle actions*", for they are rule and law enforcers not technologists. Free enterprise should NOT be obligated to reveal the secret ingredient of their technologies, unless it is being identified with evidence for suspicious crime.

There are already long lists of data / information security standards and technical safeguarding requirements, such as UK GDPR & Data Protection Act 2018 (DPA 2018), NIS2 Directive/Regulations (Network and Information Systems), Cyber Essentials / Cyber Essentials Plus, Data Security and Protection Toolkit (DSPT), Product Security and Telecommunications Infrastructure Act 2022, Privacy and Electronic Communications Regulations (PECR), Data Protection Impact Assessments (DPIAs), UK SOX, etc. Amid there could be risks "*emerge from the interplay between technical development decisions and how a system is used, who operates it, and the social context into which it is deployed*", it is applicable to all technologies, not just AI. Rights to revoke a user agreement with a standard provision, such as *"no illicit or manipulative use of technology"* may suffice.

Based on the preceding analysis, we recommend adopting the following definition of AI—or a similar variant—for adoption by the UK, US, and the international community:

> *"Covered AI technologies refer to cognitive systems (beyond learning from pairing a neutral stimulus that becomes a conditioned stimulus), comprised of memory AND topology of known lessons, that learn from regularities and irregularities of pattern(s) / knowns and unknowns / models/ simulations, AND*
>
> *the system's internal process EITHER comprises of multi-steps reasoning (understand in a way that mimics humans; NOT merely extracting signals to generate alerts; NOT unconscious thinking) OR capable of generating datum uniquely different from a plagiarized copy, that*
>
> *manipulates or presents at least an abstracted phenomenon (person or avatar, thing or computer-generated element, or real or virtual event that is hypothetical or observed to exist or happen in a distanced past, real-time, or irrespective of space-time) in a metaverse, real, or virtual environment*
>
> *autonomously OR follow commands/ instructions, to generate expectations, make-believe, or assert that certain selected or perceived phenomenon is or will occur / available for use (regardless of the system internalizes, consumes, or makes feed(s) / datum available to its users in a domain, a dark web, or any iteration of the internet or intranet), AND through action (including provision of customized or generic recommendation that reinforces, strengthen or weaken an ideology) OR inaction to stimulate the thought processes of at least an individual human OR the operations of a machine."*

[36] https://columbialawreview.org/wp-content/uploads/2016/05/Orin-S.-Kerr.pdf
[37] https://www.lawinsider.com/dictionary/function-creep
[38] https://www.databoiler.com/index_htm_files/DataBoiler SEC CAT 20210503.pdf
[39] https://en.wikipedia.org/wiki/Edward_Snowden ; https://en.wikipedia.org/wiki/2015%E2%80%932016_SWIFT_banking_hack

Feel free to contact us with any questions. Please keep us posted where our expertise might be helpful.

Sincerely,

***Kelvin To***

Founder and President

**Data Boiler Technologies, LLC**

This letter is also available at: https://www.DataBoiler.com/index_htm_files/DataBoiler%20FCA%2020260130%20AILab.pdf

Cc: Ms. Sarah Pritchard – Executive Director, Markets and International, FCA
Mr. Stephen Hanks – Manager, Markets Policy Division, FCA
Mr. Stéphane Malrait – Non-Executive Director, FCA
Ms. Lucy Rigby KC MP – Economic Secretary, HM Treasury