212° 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 https://www.databoiler.com

March 15, 2025

via Electronic Mail (ostp-ai-rfi@nitrd.gov)

Mr. Faisal D'Souza, Technical Coordinator
National Science Foundation (NSF)
Networking and Information Technology Research and Development (NITRD)
National Coordination Office (NCO) 2415 Eisenhower Avenue, Alexandria, VA 22314

Re: Development of an Artificial Intelligence (AI) Action Plan - 2025-02305 (90 FR 9088)[1]

Dear Mr. D'Souza,

On behalf of Data Boiler Technologies, I am pleased to provide the NSF - NITRD NCO with our comments on the captioned release to "Request for Information on the Development of an Artificial Intelligence (AI) Action Plan", thereafter, refers as the "AI Plan". As an inventor of patented solutions (US, Canada, Singapore, Japan and recently approved in Australia and EPO) in signal processing, ensemble learning, trade analytics, time-lock cryptography, etc., I understand why policy makers around the world are scrambling to regulate Big-TECH,[2] and Artificial Intelligence (AI). Deepfake imposter scams are driving a new wave of fraud.[3] Disinformation and privacy issues[4] should be a concern for society and government. Amid the AI Act[5] in the EU is the world's first AI law to ensure better conditions for the development and use of this innovative technology, it failed to address the true AI risks while subjectively put non-Europe based innovators at a disadvantage.

Per our 2023 submitted comments[6] to the US Securities and Exchanges Commission (SEC), AI users should be aware that there are different machine learning models. Some are "Black Boxes" that lack good interpretability. The SEC proposal regarding Predictive Data Analytics (PDA)[7] is detrimental to innovation. If it was to pin-point these "Black Boxes" and favor our approach which includes taxonomy and customizable parameters that provides appropriate 'contexts' to the AI predictions or analysis and ensuring 'fit-for-purpose', then certain guidance to alert the AI users would make sense. However, if that SEC proposal is adopted as drafted, 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 corruptions.

I am perturbed by those who do NOT understand AI using *"AI Risks"* in an attempt to sell existing Governance Risk, Compliance (GRC), Business Continuity, Resiliency, Cybersecurity, Privacy, and non-discriminatory tools, and then regurgitate them as the *"Foundations of a responsible AI risk management framework"*. Prescribing the wrong framework undermines true AI risks and may inadvertently exacerbate the risks to humankind. Please allow me to explain why AI risks can be the downfall of humanity.

AI enables computers and machines to simulate human intelligence. Human intelligence[8] is the *"mental quality that consists of the abilities to learn from experience, adopt to new situations, understand and handle abstract concepts, and use knowledge to manipulate one's environment."* Automated intelligence and generic predictive data analytics are

[1] https://www.federalregister.gov/documents/2025/02/06/2025-02305/request-for-information-on-the-development-of-an-artificial-intelligence-ai-action-plan
[2] https://www.brookings.edu/articles/a-focused-federal-agency-is-necessary-to-oversee-big-tech/
[3] www.bloomberg.com/news/articles/2023-08-21/money-scams-deepfakes-ai-will-drive-10-trillion-in-financial-fraud-and-crime
[4] https://time.com/5872868/big-tech-regulated-here-is-4-ways/
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
[6] https://www.databoiler.com/index_htm_files/DataBoiler%20SEC%2020231010%20Predictive%20Analytics.pdf
[7] https://www.sec.gov/files/rules/proposed/2023/34-97990.pdf
[8] https://www.britannica.com/science/human-intelligence-psychology

outside scope if the computer or machine is NOT performing functions to *"simulate the mental quality of humans"*. However, AI does NOT need to be autonomous to be within scope. Confining AI risks to covering only Artificial General Intelligence (AGI) would be too narrow of a scope.

The existing definition of AI under 15 U.S.C. § 9401(3)[9] is problematic. Which modern technologies are not *"machine-based system"*? Amid the available of subject matter eligibility guidance and AI related updates[10] explains how the US Patent and Trademark Office (USPTO) personnel including patent examiners should evaluate claims for patent subject matter eligibility under 35 U.S.C. 101, USPTO scrutiny of AI related applications is overly subjective based on individual examiners' personal preference or prejudice. Per this 2024 issuing spotting chart by USPTO,[11] policy makers should appalled by the cumbersome and bureaucratic requirements that hinders the development of AI in the US.

Also, how autonomous AI agents may fall within or outside scope of *"a given set of human-defined objectives"*? The part about *"make predictions, recommendations or decisions influencing real or virtual environments"* under the existing AI definition is worst. It seems to encompass all modern and age-old technologies. Would the following scenarios fall within scope: (a) Capital Asset Pricing Model, an age-old widely used method to OPTIMIZE the risk and portfolio return; (b) Black-Scholes, Value-at-Risk, or other risk management approaches, which CORRELATION assumptions can break (these techniques are commonly used by market participants and applicable to all options and derivative trading); (c) private companies following the US Treasury Department Office of Finance Research in using Agent-Based Models[12] for ANALYZING threats to financial stability; private companies following the SEC's example[13] in engaging Academia to use Machine Learning models to research or prove if there is alpha in odd-Lot, depth-of-book data, + other PDA to determine the optimal tick size, etc.

If (a) and (b) are within scope of 'Covered technology', then too many firms will be required to comply. How will financial regulators have the resources to review all related written policies and procedures? Would it be a "check-the-box" type of review, which big law / consulting firms on behalf of their Elites clients would prepare a "standard compliance template" for the evaluation of compliance when in fact it is a delusional diplomacy. For (b), how frequently (every 3 months or annually) should firms access if correlation assumptions may break or not? Why is there different treatment for private use of AI machine learning by private companies or citizens versus government officials if (c) and (d) are within scope? Would research or the SEC example in (d) constitute as prohibited INTERACTIONS? Would there be exemption(s) for Academia? What claimed to be a "principle-based rule" may indeed generate more questions than answers.

AI Risks = Downfall of Humanity

To truly understand AI risks, one should first make reference to the Asimov's Three Laws:[14] "*machines* [1] *may not injure a human being, or through inaction, allow a human to come to harm;* [2] *must obey the orders given it by human beings except where such order would conflict with the Frist Law;* [3] *must protect its own existence as long as such protection does not conflict with the First or Second Law*", plus the later introduced "Zeroth (Forth) Law".[15] Accordingly, Asimov's

[9] https://www.law.cornell.edu/definitions/uscode.php?height=800&def_id=15-USC-1491829989-625142935&term_occur=999&term_src=title:15:chapter:119:subchapter:I:section:9415
[10] https://www.uspto.gov/sites/default/files/documents/OCE-DH_AdjustingtoAlice.pdf; https://www.federalregister.gov/documents/2024/07/17/2024-15377/2024-guidance-update-on-patent-subject-matter-eligibility-including-on-artificial-intelligence
[11] https://www.uspto.gov/sites/default/files/documents/2024-AI-SMEUpdateExamples47-49.pdf
[12] https://www.financialresearch.gov/working-papers/files/OFR_Working_Paper_No3_ABM_Bookstaber_Final.pdf
[13] https://youtu.be/s9gdfxCoIq4
[14] https://en.wikipedia.org/wiki/Three_Laws_of_Robotics
[15] https://www.streetdirectory.com/travel_guide/120083/technology/the_fourth_law_of_robotics.html

second and third laws depend on the first law about individual safety of a human. Due to ethical complexity, the Zeroth law emphasized on the broader humanity rather than individual. A bright-line test to AI risk is therefore, whether the disobedience, action, or inaction of AI would impair the livelihood of human(s), exacerbate the downfall of humanity, or pose existential threats to human(s).

Humankind should develop an urgency towards learning and adapting to an AI-filled environment where humans can master over it. In my 2024 article published on GARP Risk Intelligence and other media,[16] I highlighted the following list of AI risk examples:

- AI drains significant energy, analogy to mining crypto, that it could potentially bring down the energy grid. Underwater cooling[17] and other innovative approaches[18] are ways to deal with unprecedented demand of data centers[19] given the growth of AI Yet, the efficiency of AI should be embedded in its design. Finding a needle in a haystack to rely on a "black box" neural network deep learning from a gigantic, centralized data vault, such as the FINRA Consolidated Audit Trail[20] is highly inefficient. Decentralized/ Federated learning and analysis directly from data sources is a much better approach from cybersecurity, privacy, and resources saving perspectives.
- AI molding people into machines or 'couch potatoes' is another threat. Reinforcement model,[21] optimize AD algorithm,[22] and/or learning methods[23] that lead to addictive, herd and/or polarized behaviors should be closely scrutinized. If we are against human slavery, then we should watch out for Authoritarians trying to use AI to exploit or destroy humans' abilities to think independently. Indeed, there are civic concerns[24] about massive government surveillance.
- AI can recall every bit of big data to optimize and rationalize everything for a speedy and accurate decision, no average human being can match up. The irony is, if AI mimics the human brains like the Nobel Winner – Daniel Kahneman's Prospect Theory[25] (book: Thinking, fast and slow),[26] where *"division of labor between System 1* (fast, intuitive, and automatic) *and System 2* (slow, effortful, and logical) *minimizes effort and optimizes performance"*, then would AI have the same fallacies influenced by *"loss aversion, certainty, and isolation effect"*? AI has driven modern society towards the risk of hyper optimization. Do we want consistency and act rationally every time to undermine humans' unique ability to think laterally and/or selectively forget about things? These mental qualities reflect our human imperfections, while the last defense against AI relies on Eureka derives from usefulness of the useless knowledge.[27] So, before you wish AI to give consistent and rational answers (output reliance), or not, be careful.

---

[16] https://www.garp.org/risk-intelligence/technology/extreme-manageable-risks-ai-240517 ; https://www.tradersmagazine.com/am/a-i-risks-downfall-of-humanity/ ; https://www.benzinga.com/opinion/24/04/38441152/a-i-risks-downfall-of-humanity ; https://www.linkedin.com/pulse/ai-risks-downfall-humanity-kelvin-to-yhzge/

[17] https://news.microsoft.com/source/features/sustainability/project-natick-underwater-datacenter/

[18] https://www.techrepublic.com/pictures/photos-20-innovative-data-centers-that-gives-us-a-glimpse-of-the-future-of-computing/

[19] https://www.us.jll.com/en/newsroom/growth-of-ai-creates-unprecedented-demand-for-global-data-centers

[20] https://www.linkedin.com/pulse/cat-outdated-design-since-2012-kelvin-to/

[21] https://arxiv.org/pdf/2302.01470v1

[22] https://www.searchenginejournal.com/google-ads-audit-optimize-thatppcguy-spa/509185/

[23] https://medium.com/ai-artistry/maximizing-rewards-with-policy-gradient-methods-and-monte-carlo-reinforcement-learning-part-46f2fd852cf0

[24] https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/ethics.html

[25] https://en.wikipedia.org/wiki/Prospect_theory

[26] https://www.amazon.com/Thinking-Fast-Slow-Daniel-Kahneman/dp/0374533555

[27] https://www.ias.edu/sites/default/files/library/UsefulnessHarpers.pdf

- AI exacerbates the 21st century challenges, include: a rebellious move by an insurgent with a war chest to orchestrate a market wide shake-up, and foreign adversaries wanting to see the US engage in unhealthy competition to possibly erode the US's prominent market position. Many may claim to be 'Nomad' when they represent the 'Corpo'. While 'Street Kid' may not be the underserved and the most vulnerable that people stereotyped. In the cyberpunk era, be mindful of the gap and realize that an inverse relation between DeFi and CeFi.[28] Rather than punishing all tech innovations, the ability to delineate good and bad actors is essential to mitigate this risk.

- AI is like the News media. *"There are multiple versions of truth. The news, while attempting to inform, often selectively highlights certain aspects rather than recording everything in its entirety"* (acclaimed author Alain de Botton's book: The News: A User's Manual).[29] "Bias" is an interesting topic, amidst different AI models have different tradeoff between tractability versus realism. This empirical research[30] by the US Treasury O.C.C. and the Rensselaer Polytechnical Institute and University College Dublin about *"machine learning model complexity in capturing the information processing costs that lead to information asymmetry in financial markets"* is worth reading. It is NOT about over/ under-representation of a population cohort, whilst majority of data consumed by AI is inherently biased towards English and precluding other languages. Nemil Dalal argued that *"today's biggest threat to democracy isn't fake news* [Hallucination] *—it's selective facts."*[31] A group of academia has launched a Data Provenance Initiative[32] to address concerns about legal and ethical risks face by practitioners in the AI community. What constitutes Fair, Reasonable, and Non-Discriminatory? I recommend assessing the divergence between private rights and social costs.[33]

Improving Trust Amid Race in Technologies

TECH advancements and increased interconnectedness offer many benefits to society. Whilst it poses new Cybersecurity risks and privacy threats. The world becomes chaotic when authentication techniques cannot discern what to trust or untrust. To foster healthy AI development, let revisit the historical developments of internet safety and envisage what is next in improving Trust amid the race in various AI technologies.

Public Key Infrastructure (PKI) was originally invented by the British intelligence agency in the early 1970s as a centralized Certificate Authority (CA)[34] based system. CAs are prone to hackers' Man-in-the-Middle attacks.[35] Instead of relying on CAs, Decentralized Public Key Infrastructure (DPKI) has key-value storage in a decentralized form for better security. Pretty Good Privacy (PGP) is a decentralized "web of trust"[36] system developed by Phil Zimmermann long before the existence of Blockchain/ Distributed Ledger Technology (DLT). PGP is the common encryption standard in today's market.

The internet highway is a "Public" space. It is dominated by Google and other Big TECHs, as well as many Hackers and Foreign Adversaries. PGP is no longer effective in the convoluted World Wide Web. According to NIST and NCCoE,[37] *"The proliferation of cloud computing, mobile device use, and the Internet of Things has dissolved conventional network boundaries."* Users of internet applications may opt-in/ opt-out of sharing. Organizations are only now catching up in

[28] https://www.databoiler.com/index_htm_files/DataBoiler Treasury Digital Assets 202208.pdf
[29] https://www.amazon.com/News-Users-Manual-Alain-Botton/dp/0307379124
[30] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4763575
[31] https://qz.com/1130094/todays-biggest-threat-to-democracy-isnt-fake-news-its-selective-facts
[32] https://arxiv.org/pdf/2310.16787.pdf
[33] https://iea.org.uk/wp-content/uploads/2016/07/THE MYTH OF SOCIAL COST.pdf
[34] https://en.wikipedia.org/wiki/Certificate_authority
[35] https://en.wikipedia.org/wiki/Man-in-the-middle_attack
[36] https://en.wikipedia.org/wiki/Web_of_trust
[37] https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf

deployment of cybersecurity best practices. All of these do not change the fact that the internet highway is NOT a space for "Quiet Enjoyment" (QE)[38] – a right of an occupant to enjoy and use premises in peace and without interference.

There are limitations of Privacy Enhancing Techniques.[39] By "joining" (daisy chain/ mesh) multiple digital trails and metadata using AI, biometric recognition, geolocation and/or other technologies, Personal Identifiable Information and confidential data could be unveiled. Law enforcement agents may use such techniques to pinpoint wrongdoers. All giving rise to civic concerns[24] about Massive Government Surveillance agencies and systems. In addition, disinformation,[40] headline cases of non-compliance, tech companies' failure,[41] and/or other controversies[42] have shaken peoples' trust on technology.

While people love the convenience of physical token-less security screening tools using biometrics, such as CLEAR - NextGen Identity+, for digital identity to access secured areas (airport) and digital online space (LinkedIn verification), there are a few security incidents[43] with the firm. Facial recognition is everywhere, and anyone's biometrics information may already be collected by different machine learning libraries that are susceptible to attack or misuse.

Security controls should be embedded in the design of any systems.[44] Minimize data-in-motion.[45] 'Data-in-use' is more vulnerable than 'at-rest.' The more users/ devices access data, the greater the risk hackers may alter/ add/ insert/ use (or reuse) the data abusively. If putting these principles in a broader context of architectural design of the Internet, the concept of having Metaverse[46] makes sense. Crafting out private QE spaces from the public internet highway would better delineate: (1) the Authenticity of the People, (2) In-Door Places, and the (3) Ontology of Things.

According to the World Economic Forum, "Zero Trust"[47] is *"a shift in the security approach on how to dynamically and holistically establish trust with an unknown, whether a human being or a machine"*. That being said, Authenticity Institute summarized 10 reasons for why PKI (or DPKI) has yet to be widely adopted.[48] We agree there are significant gaps in the awareness and know-how in the appropriate implementation of Zero Trust Architecture. Yet, we believe "Establishment Pushback" being the prominent factor hindering a paradigm shift.

The point is – technology is only one-third of the race in improving trust. People accustomed to data breach class action settlements. Governance may play a small part in inducing change. Using the US Government confiscated cryptocurrencies from illicit activities to showcase the "trust" issues,[49] the biggest challenge faced by the regulators is, the entire flow mixes-in legitimate Distributed Ledger Technologies (DLT) initiatives with potential bad actors / foreign adversaries that hide under the guise of DeFi / De-dollarization movements.[50] Authenticating who is who, who is doing what, where and when via the PKI or DPKI Metaverse is good, but insufficient. 21st century's challenges or "chaos" include: content

---

[38] https://www.amazon.com/Quiet-Enjoyment-Security-Privacy-Networks/dp/1931248125
[39] https://www3.weforum.org/docs/WEF_Next_Gen_Data_Sharing_Financial_Services.pdf
[40] https://news.stanford.edu/2022/04/13/know-disinformation-address/
[41] https://www.fsb.org/wp-content/uploads/P281123.pdf
[42] https://fortune.com/2023/11/27/openai-board-dysfunction-right-choice-defeat-battle-ai-profits-ethics-contest-tech-leadership-ann-skeet/
[43] https://www.cbsnews.com/news/tsa-clear-secure-screening-passenger-ammo/ ; https://www.politico.com/news/2023/08/07/transpo-clear-tsa-00110124
[44] https://www.linkedin.com/pulse/cat-through-z-security-privacy-requirements-kelvin-to/
[45] https://www.databoiler.com/index_htm_files/DataBoilerInMotion.pdf
[46] https://en.wikipedia.org/wiki/Metaverse
[47] https://www3.weforum.org/docs/WEF_The_Zero_Trust_Model_in_Cybersecurity_2022.pdf
[48] https://youtu.be/xdvfvBzZduo?si=DEpNfZw0_Ylg1GEL
[49] https://docs.ie.edu/cgc/research/cryptocurrencies/CGC-Cryptocurrencies-and-the-Future-of-Money-Executive-Report.pdf
[50] https://www.linkedin.com/pulse/have-you-seen-quantum-cat-after-digital-asset-crash-kelvin-to

moderation versus censorship,[51] rogues hop around, "Street Kids" uprise with MEME stock phenomenon, digital "Nomads" could care less about ethics, "Corpos" rent seeks in the Cyberpunk era, and/or allegedly cahoots activities.

Regardless of the present Internet space or Metaverse, weeding out misbehavior, creating fair, reasonable and non-discriminatory mechanisms to align rights with obligations, and management of private rights with divergence of social costs[33] are top priorities. People demand for high quality "furnished" conditions of QE space. I.e., guarantee that chaos is not happening. Also, people want frictionless transitions from the legacy web/ social media platforms to Web3 at presumably "FREE" or justifiable return on investment.[52]

It is a tall order. No denial that Zero Trust is an important "TECH Bandage" to curb bot attacks before a complete overhaul of the web from a philosophical perspective. However, it works in COUNTER of people's SOCIAL NEEDS. Democratize AI rather than held in the hands of a few elites. Web3 defense builders should not perceive Big TECHs as the biggest societal threats. Authoritarians, insurgents, and human sloppiness are indeed the common "enemies." Healthy AI development requires different TECH participants to be united while maintaining positive tensions in the technology arms race. Trust will be earned over time if we can reduce chaos and shape a safer and fair environment for all!

Volatility and AI Hallucinations – from Challenges to Opportunities:

A token limitation may be the one weakness of Large Language Model. AI can deploy countless 'agents' to avert hackers. Can a "virus" to overflow the system be used as a last resort method to stop AI upon a conflict with Asimov's first, second, or forth law? Or should every AI be mandated a kill-switch/ circuit breaker to fulfill Asimov's third law? Stephen Hawking warns AI could end humankind.[53] It takes unconventional wisdom for a Eureka moment amid the race between AI and humans. Embrace difficult challenges would help us to learn, unlearn, and relearn[54] in the 21st century to prevent a downfall of humanity and address AI risks.

People poking holes in the initial results of AI, which they are rightly to do so. Yet, the performance of AI improves over time and AI hallucinations may discover unknown unknowns which were previously nonsensical to human. It's a paradigm shift to go from suspicions to opportunistic about newfound onset signals / liquidity among chaos/ market dynamics.

The key technical challenges people face when integrating AI is people not realizing the various pros and cons with different machine learning models. Blindly goes with neural network, deep learning black boxes, then go about craving for evermore data to feed the models. Much resource is devoted to sourcing alternate data, while too much data and inherent problem of data imprecision causing it to take forever to achieve 'golden-source'. Then, they'll be jiggling to insert or delete nodes for tunning/ data corrections (e.g. Support Vector Machine requires labeled data), while not knowing valuable insights may inadvertently be removed from the dataset. In turn, inexactitude in trade sequencing caused analytic results based on vector measurement or visualized heat-maps to be erroneous (false +/-).

It is optimal if onset signals could be detected without the additional alternate data because there are cost-benefits in finding relevant needles in a haystack. Integrating AI all boils down to the analysis. Do NOT fall for the hype of data management. Picking the right machine learning models (robust to missing data and outliers) and data science methods (trivially parallelized) would accelerate the training of computers for good predictive power. A good decision made now and pursued aggressively is substantially superior to a perfect decision made too late.

---

[51] https://www.brookings.edu/events/online-safety-and-digital-content-oversight/
[52] https://en.wikipedia.org/wiki/Web3
[53] https://www.bbc.com/news/technology-30290540
[54] https://www.nsca.org/learn-unlearn-relearn-becoming-change-ready/

✉ info@databoiler.com https://www.databoiler.com

In order for the US to continue leading the World in AI, a machine learning library is key. The library serves as anchored reference of known lessons, for benchmark comparison. Recognizing patterns (regularities), identifying risks (irregularities), and discovering hidden models (unknowns) – whoever has the bigger machine learning library and more accurate lessons will control the "who gets what" (i.e., most impactful).

Conclusions and Other remarks:

1. It is inevitable that markets will be driven increasingly by AI algorithms.[55] AI risks is an engineering problem require an engineering approach to solve. The last administration indiscriminately discourages all PDA developments rather than rewarding the development and use of innovative PDA to prevent frauds, curb conflicts or abuses. SEC Cybersecurity rule[56] requiring public companies to heighten related governance controls and disclosure is another example of burdensome policies that only benefit the big law or consulting firms. Victims of Cybersecurity incidents need government's help, rather than being penalized twice when they performed all reasonable defend steps.

   The faulted definition of AI under 15 U.S.C. § 9401(3) or the EU AI Act created unnecessary bureaucracy, favored subjective judgements, and is counter-productive to the goals of advancing the interests of U.S. consumers and businesses. The right focus and priority to regulate misuse of AI and/or other technologies should be to curb fraudulent activities. US Government Agencies has extensive powers under existing authority to tackle fraud. The last administration missed the right target, or it is a mismatch to civic concerns[24] about disinformation and privacy issues.

2. It should and always is the responsibility of the regulators to review if there are misuse of AI or conflicts resulted in exploitation behaviors in the markets and take appropriate actions to prosecute wrongdoing. The former administration slacks off its own responsibility and put the burden to decipher wrongdoing on tech practitioners and users of AI (or their delegated law / consulting firms) to self-assess is unjust. It is in essence a 'self-regulation' regime, to that we disagree. Yet, government gathering of, and the more people know about these AI secret ingredients, the higher risk (e.g. function creep)[57] there will be for the society. Take the Consolidated Audit Trail (CAT)[58] project – the world's largest financial database as an example. The SEC asked FINRA CAT to comply with an outdated[59] NIST's CISP revision 4 of SP800-53 standard.[60] Irony is that several government agencies providing AI cybersecurity guidelines[61] or rules[56] for public to follow have themselves been hacked.[62] Hackers do not necessarily come from outside, e.g., the Edward Snowden case embarrassed the Central Intelligence Agency.[63]

3. If without the appropriate "contexts" of HOW certain AI activities should be prohibited versus permissible under WHAT "circumstances", it is impossible for any TECH practitioners and users of AI to fulfill regulatory to identify the "WHEN" a *"firm uses a covered technology that takes into consideration an interest of the firm or its associated persons"* that constitute as an existence of a "misuse, conflict, or exploitation".

---

[55] https://www.linkedin.com/pulse/from-latency-ai-algo-driven-capital-markets-kelvin-to-xu5te
[56] https://www.sec.gov/news/press-release/2023-139
[57] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547903
[58] https://www.databoiler.com/index_htm_files/DataBoiler SEC CAT 20210503.pdf
[59] https://www.sec.gov/rules/proposed/2020/34-89632.pdf
[60] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
[61] https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf
[62] https://www.marketwatch.com/story/treasury-department-reportedly-breached-by-hackers-01607895145; https://www.nbcnews.com/tech/security/us-govenment-agencies-hacked-cyberattack-moveit-rcna89525 ; https://cybernews.com/news/lockbit-ransomware-us-federal-reserve-published/
[63] https://www.britannica.com/biography/Edward-Snowden

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 should blames. Please be reminded of Société Générale (SocGen) $7.2 billion loss in 2008,[64] Rogue trader - Jérôme Kerviel bought into the top boss - Daniel Bouton's lip service about SocGen's internal control strengths, even stating the followings during his testimony: *"The techniques I used aren't at all sophisticated and any control that's properly carried out should have caught it."*[65]

4. There are more effective ways to guard against misuse of TECH or to curb "black box" algorithms causing market chaos, market manipulation, or conflicts. They are: (i) follow our suggestions to overhaul the outdated design of CAT;[66] (ii) require market data Available SECURELY in Synchronized time using Time-Lock Encryption;[67] (iii) align rights and obligations with Copyright Licensing mechanism[68] – by putting a value on Intellectual Property (IP), e.g. quotes and trades composition, and requiring "streaming platforms" (trading venues) to provide a "catalog" (disclosure), proper considerations will be given to eliminate conflict of interest, as well as ensuring efficiency in deployment of resources, rather than engaging in non-productive fights that destroy value.[69]

The Bipartisan House Task Force Report on AI[70] highlighted that *"there is no universal definition of AI. If Congress chooses to preempt state AI laws, then the preempting legislation should precisely define AI in a manner that represents the intended scope of preemption."* We acknowledge the Federal Reserve Governor Bowman's comments about regulators should *"not adopt a one-size-fits-all approach as we consider the future role of AI in the financial system."*[71] Given the problems with the existing definition of AI as cited in earlier section of this letter, 15 U.S.C. § 9401(3) must be revised amid the difficulty to do so. We recommend the "AI Plan" to adopt the following in compliance with the President Trump signed Executive Order 14179 (Removing Barriers to American Leadership in Artificial Intelligence):[72]

a. 15 U.S.C. § 9401(3) revision should follow Asimov's Three Laws[14] and the later introduced Zeroth (Forth) Law.[15] Also, America should have an energy policy to prevent AI or other Big TECH from bring down the energy grid. This is a much simpler and effective approach to preventing humanity's downfall – addressing the true AI risks, than imposing *"excessive regulation of the AI sector,* [which] *could kill a transformative industry just as it's taking off."*

b. To *"make every effort to encourage pro-growth AI policies"*, policy makers should consider the appropriate divergence between private rights and social costs.[33] AI copyright lawsuits continue to be on the rise,[73] streamlining copyright laws and relaxing USPTO 35 U.S.C. 101 help protect essential IP rights and encourage innovations. When accessing the

[64] http://www.businessinsider.com/how-jerome-kerviel-lost-72-billion-2016-5
[65] http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/5241263/Societe-Generale-chairman-Daniel-Bouton-to-step-down.html
[66] https://www.linkedin.com/pulse/hr-block-analogy-cat-combating-fraud-kelvin-to/
[67] https://www.linkedin.com/pulse/market-data-available-securely-synchronized-time-kelvin-to/
[68] https://www.databoiler.com/index_htm_files/DataBoiler%20BIG%20OPP.pdf
[69] https://www.databoiler.com/index_htm_files/DataBoiler%20Copyright%20Licensing.pdf
[70] https://republicans-science.house.gov/_cache/files/a/a/aa2ee12f-8f0c-46a3-8ff8-8e4215d6a72b/6676530F7A30F243A24E254F6858233A.ai-task-force-report-final.pdf
[71] https://www.federalreserve.gov/newsevents/speech/bowman20241122a.htm
[72] https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence
[73] https://www.wired.com/story/ai-copyright-case-tracker/

Values of Composing IP[74] to determine who gets what,[75] we advocate for learning from the music industry's licensing framework. It has over a half century of litigation experience to align rights and obligations globally. It helped music reach a wider audience and grow the overall pie.

AI should remain widely accessible to the American public rather than being controlled by a few elites, the democratization of affordable AI is essential. For that, Department of Justice should tighten enforcement of antitrust laws. AI innovations should be merit-based, irrespective of a company's size. Federal subsidizations and encourage private fundings to support small business to, not only adopting AI but also innovating in AI to challenge the status quo of Big TECH. For Big TECH, they should bear social responsibility in contributing to a National machine learning library of known lessons to discover discovery of unknown unknowns. By then, it will *"ensure that American AI technology continues to be the gold standard worldwide and we are the partner of choice for others -- foreign countries and certainly businesses -- as they expand their own use of AI."*

c. A complete overhaul of the web to ensure quiet enjoyment[38] of private citizens. Vice President JD Vance remarks[76] 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"* help address civic concerns over massive government surveillance.[24] The public has long suffered from spams and privacy invasions and other chaos, Americans deserve frictionless transitions from the legacy web/ social media platforms.

d. Establish a special task force to deter bad actors / foreign adversaries in using AI or hide under the guise of DeFi / De-dollarization movements[50] that attack America. This task force should encompass humanity and engineering talents where they will learn, unlearn, and relearn,[54] from for example the Prospect Theory[25] and the usefulness of the useless knowledge,[27] in developing efficient and effective engineering approach to address related AI risks.

We hope Policy Makers can work constructively together with us to address the 21st Century's problems, such as: insurgent in Cyberpunk Era, misuse of TECH by "Big Corpo" to exploit others, etc. Feel free to contact us with any questions and 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%20NSFOSTPNITRDNCO%2020250315.pdf

[74] https://minnesota.publicradio.org/tools/current-utilities/images/music_rights_final_v7.pdf
[75] https://www.amazon.com/Who-Gets-What_And-Why-Matchmaking/dp/1501238159
[76] https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-artificial-intelligence-action-summit-paris-france