Beware of AI Hype & Harm

By Lisa D. Dance, UX Consultant/Founder, ServiceEase

I originally launched this series of LinkedIn posts on AI on March 15, 2023 (The Ides of March) as a reference to Shakespeare's Julius Caesar receiving the warning "Beware of the Ides of March" before he was assassinated on that very day.

Big Money Deprioritizes Safety

"Beware of the Ideas of March" from Shakespeare's Julius Caesar in high school always stuck with me. It's meant to be a caution about people intending to do you harm. On this Ides of March, I thought it was appropriate to look at ways we all need to develop a new mindset on AI. Let's be clear AI is already implemented in many ways (chatbots, recommender for movies, articles or restaurants or predictive models in healthcare, credit, hiring, child services, the judicial system, and more. Everyday life stuff … large and small, but isn't regulated enough to protect people or the environment. I'll discuss the first one today and others over the next few days.

Big Money Deprioritizes Safety: There's lots of money involved in AI from the cost of development all the way through to the potential money to be made by the companies involved. The rush to gain an advantage makes for less cautious approaches to AI.

Consider how the rush releases of Microsoft's Bing AI and Google's Bard showcased these chatbots insisting incorrect information as fact. The factual mistake by Bard at its demo cost Google $100 billion in market value.[1] Microsoft laying off its Ethics and Society Team within its AI Team doesn't show AI ethics concern while it rushes ahead with Bing AI.[2]

o Yes, this is capitalism at work, but capitalism as currently practiced is has historical income equality… so big money shifts matter in who will gain the most and who will lose from AI.

(1) https://lnkd.in/eYUAkd5i
(2) https://lnkd.in/ey27vrek
#ai #aiethics #dataprivacy #ethicaldesign

Historical Data=Historical Bias on Blast

Instead of blindly rushing to AI utopia, let's adopt a new mindset on AI. Today, let's discuss #2 Historical Data = Historical Problems on Blast from "Beware of AI Hype & Harm" (below): - AI models are based on historical data with all its flaws (bias, inaccuracies, misinformation, delusions, limited representation, and more). Think of historical as both the recent past (ex. yesterday or last month) to "history" history (ex. the 1950s or 1800s). While companies use both computers and humans to remove some bias in the data for

these models, bias still shows through like when Lensa images that sexualized women and anglicized features.[1] The speed of AI systems amplifies information meaning the sins of the past can be repeated on blast.

- Some might say humans have the same flaws, but there are important differences: the scale and speed of AI as well as AI models' ability to not forget that past. As the "Combating Automation Bias" article by ForHumanity clearly points out AI doesn't allow for the very human characteristic of changing course or overcoming your past, you are what the data says you are (aka predicts). Isn't the ability to change at the core of who we are or want to be as humans? Should AI through large language models be able to stop that? [2]

- Another important aspect is that the data used to train LLMs (large language models) aren't 100% clear but are partly based on non-representative sources particularly the internet. Think of how the internet is dominated by some voices more than others through manipulation and misinformation. So, people who are already marginalized are marginalized at scale through the use of these models which was famously forewarned in 'On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?" paper.[3]

Have you considered these aspects of using AI or mitigated for them? #ai #data #bias #largelanguagemodels #aiethics
(1) https://lnkd.in/emFWZ2hE
(2) https://lnkd.in/ehSXhkR4
(3) https://lnkd.in/e547XgKb

Are We Unpaid Workers in the AI Value Chain?

These large language and image to text models like ChatGPT & Lensa AI are trained on large amounts of data scraped from books, webpages, and other source. We didn't give consent to use some of the data and companies are promoting AI Utopia (where all hard tasks can be automated) to entice us to make these AI tools better. Consider these issues:

- Unauthorized Use of Images: Consider the case of one woman who found private medical photos of her face were used in a LIAON dataset used to train Stable Diffusion and Google Imagen. As a copy of her release shows, she only authorized the use of her photos in her file only and not shown to anyone.

Beware of AI Hype & Harm

By Lisa D. Dance, UX Consultant/Founder, ServiceEase

(1) Copyrights: Several artists in a class action suit and Getty Images separately have sued Stable AI, the companies behind a popular AI image generator, for copyright infringement by scraping their copyrighted images from the internet for their datasets. Some images produced from its models have the Getty Images' watermark on them. These lawsuits raise new questions about the legality of this.

(2) Collecting Biometric Data: Lensa AI faces a new lawsuit over collecting facial data (biometrics) through its image scraping without consent under Illinois' 2008 Biometrics Information and Privacy Act.

(3) Underpaid and Traumatized: According to a Time article, workers tasked with labeling graphic depictions of violence and abuse were paid as little as $2 hour for nine-hour shifts in Kenya. This would help OpenAI be more marketable because it was less toxic. Workers called dealing with this toxic content "torture" and despite promises of "wellness counselors" they either unhelpful or not available as promised.

(4) Free Work: Last, but not least when we use these models, we provide more data for them to train on. From our initial asks through all our refinements needed to produce a helpful answer, we are modeling language even when the chatbots responses are wrong. This helps train the model which improves its performance and increases its value in the marketplace.
- Are our rights protected in the AI value chain?
- Do we want to be workers in the AI value chain?
- Are we getting enough benefit from the AI value chain to work for free?

Who Will Be Ultimately Responsible?

Despite the current Wild West release of new AI systems and the lack of comprehensive federal legislation in the US, regulation on AI is ahead and companies that design, use or deploy AI should keep up to date on laws and prepare for compliance.

The EU is set to finalize the "AI Act", proposed Regulation Laying Down Harmonized Rules on Artificial Intelligence, in 2023. The AI Act "will govern anyone who provides a product or service that uses AI. The Act will cover systems that can generate output such as content, predictions, recommendations, or decisions influencing environments." It covers private companies and the public sector, and identifies high risk areas such as critical infrastructure, law enforcement, or education which will have strict controls and transparency requirements.[1]

Beware of AI Hype & Harm

By Lisa D. Dance, UX Consultant/Founder, ServiceEase

New York City's Local Law 144, which is set to go into effect in April 2023, requires HR departments to test their AI recruitment tools for bias, and defines situations when companies must tell applicants they're using the tools. While an important step, advocates are concerned the bill has been watered down through lobbying efforts by AI companies.[2]

California, Colorado, Maryland, Connecticut, and Illinois are among the states working on AI and data privacy legislation. Most of the bills identify areas of consequential decisions that use AI (ex. Housing, employment, financial matters, etc.) and requiring governance, transparency, and making algorithmic assessments public.[3]

The White House released its "Blueprint for an AI Bill of Rights" in October 2022, which lists "a set of five principles and associated practices to help guide the design, use, and deployment of automated systems to protect the rights of the American public." that include:[4]

- Safe and Effective Systems
- Algorithmic Discrimination Protections
- Data Privacy
- Notice and Explanation
- Human Alternatives, Consideration, and Fallback

The FTC has provided guidance on AI including a February 2023 warning to companies to "Keep your AI claims in check". It highlighted areas of AI claims in advertising that the FTC will be looking at:[5]

- Are you exaggerating what your AI product can do?
- Are you promising that your AI product does something better than a non-AI product?
- Are you aware of the risks?
- Does the product actually use AI at all?
- Is your organization prepared to both use AI and be complaint with applicable laws?

(1) https://www.reuters.com/technology/what-is-european-union-ai-act-2023-03-22/
(2) https://www.fastcompany.com/90856421/nyc-is-about-to-regulate-ai-in-hiring-critics-say-the-new-law-doesnt-do-much
(3) https://www.brookings.edu/blog/techtank/2023/03/22/how-california-and-other-states-are-tackling-ai-legislation/

Beware of AI Hype & Harm

By Lisa D. Dance, UX Consultant/Founder, ServiceEase

(4) https://www.whitehouse.gov/ostp/ai-bill-of-rights/what-is-the-blueprint-for-an-ai-bill-of-rights/
(5) https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check

New Mindset for AI (Always Investigate)

The PR push, news stories, influencer posts, and lobbying efforts promising freedom from tiresome tasks, future medical breakthroughs, and no jobs left for humans want us to adopt AI and other technologies without question. Instead, we need to Develop and Maintain a New Mindset for AI to Always Investigate claims.

- In the name of innovation, some want to burden individuals with enduring, policing, and reporting AI issues despite known harms like hallucinations, harmful content, amplifying stereotypes, bias, misinformation and disinformation, privacy violations, economic impacts, and more.[1] Instead, we need governments to firmly establish the responsibility and liability around AI lies with the developers and deployers of AI technology through robust regulation and enforcement.

- Since AI, like social media, can be a tool for misinformation, we should Always Investigate claims. Here are some of the questions we should consider:

    1. Is AI needed for this purpose?
    2. Is the AI claim true? Is the result desirable? Could it harm people?
    3. Are the people or companies making the claim credible? Do they provide documentation or sources?
    4. What is their motivation? Ex. Money, influence, clicks, engagement, misinformation, amusement, etc.
    5. Where does the data come from? Do they have permission to use it? Is the data robust and accurate?
    6. Is my data protected when I use it?
    7. Does the AI model or algorithm produce biased outcomes?
    8. What laws apply to this use of AI? Ex. Employment, Housing, and Banking Laws
    9. Am I providing free data and labor when I interact with these tools? Is this a fair exchange?
    10. Are workers being exploited to improve the technology? Ex. Underpaid workers in the Global South labeling toxic content to help improve the model.

Beware of AI Hype & Harm

By Lisa D. Dance, UX Consultant/Founder, ServiceEase

I'm not sure what to think about the "Open Letter calling for a pause on AI" released today. Is it simply about deep concern, an effort to influence potential regulation or an attempt to misdirect the narrative around AI?[2] Who knows?

- Instead, I will continue to plug into a broader and more diverse community researching and/or working with #AI and AI Ethics that includes AIethicist.org, Algorithmic Justice League, Distributed AI Research Institute (DAIR), Fight for Our Future, ForHumanity, and ProPublica[3] and support appropriate and robust regulation that protects humans today and in the future.

(1) https://cdn.openai.com/papers/gpt-4-system-card.pdf
(2) https://www.vice.com/en/article/qjvppm/the-open-letter-to-stop-dangerous-ai-race-is-a-huge-mess
(3) https://www.aiethicist.org/ai-organizations