Tech Summit on Artificial Intelligence: Consumer Facing Applications

April 2024
Office of Technology
US Federal Trade Commission

Table of Contents

Overview

On January 25, 2024, the FTC held a Tech Summit on Artificial Intelligence. The event page, with the full 4.5 hour recording of the event, is available here.

In the third panel, we hosted the following panelists:

- **Atur Desai**, Deputy Chief Technologist for Law and Strategy, U.S. Consumer Financial Protection Bureau
- **Karen Hao**, award-winning journalist covering the impacts of artificial intelligence on society and a contributing writer for The Atlantic
- **Conrad Kramer**, Co-Founder and CTO of Software Applications Incorporated, a new startup building consumer software using AI
- **Ben Winters**, Senior Counsel at EPIC, and leads EPIC's AI and Human Rights Project

Panel Summary: The panelists discussed norms of tech product design and deployment as products are being released to hundreds of millions of users with *known* harms and without incentives for companies to mitigate risks upfront. In addition, panelists mentioned that end-user AI applications can create harmful outcomes that stem from data collection, sharing, use, and monetization tactics, discriminatory algorithms, and security practices. Finally, panelists shared that companies may be employing marketing tactics such as ill-defined "AI Safety" or "Privacy Enhancing" labels to falsely build trust with consumers.

Why a Quote Book? The voices of people on the ground can sometimes be lost in discussions involving dense technical, policy, or legal language. While the benefits or risks of new technologies are being debated by policymakers, these individuals—investigative journalists, startup founders, and consumer advocates--experience the effects of innovation in real-time.

The FTC recognizes that this is not a representative sample of the entire population, and we strive to continue to listen and engage with a variety of perspectives. The goal of the quote book solely aims to reflect and compile quotes from the participants aggregated into common themes. This summary aims to be a resource, to see various perspectives on topics.

Factors to Build a Model

- “The best models are currently available for purchase or for rent from the larger companies, versus the open-source models are a little bit lagging behind on quality.” - Conrad Kramer
- “The other trade-off to consider is cost. And so, [with] open source models... the data is free or to get the model is free, but to run it [...] you have to pay for compute to run the model. And so the cost scales from just paying for computation, all the way up to paying for computation and for a model developer to build and test the model.” - Conrad Kramer
- “...Quality can sometimes depend on which data the model is trained on. And because we don't really know, for example, for the closed source models, which data is being used to train them, you actually just have to guess and check. [...] Versus the open source models, you actually in most cases have visibility into the entire dataset, and so you can actually see what is being used to train the model, and you can actually use that knowledge to build a better product. And so, there are a lot of trade-offs there, I'd say, with models.” - Conrad Kramer

AI Benefits to Consumers

Life improvements

- “I'm really excited about just the potential for all these products to improve people's lives.” - Conrad Kramer

Unlock creativity

- “Consumers are also excited about the possibility to integrate some of these tools into their lives, and automate or help them unlock their creativity, like talking with ChatGPT to get inspiration and ideas.” - Karen Hao
- “Using Stable Diffusion to generate concept work that can then help them figure out where they want to go, whether it's an architecture, building that they're designing, or something like a poster that they're designing.” - Karen Hao

Educational engagement

- “I've also seen excitement with parents, and using these tools to engage with their kids on educational and interactive story time.” - Karen Hao

Reduce redundancy

- “A lot of you interacting with a computer is filling out forms, or doing things that are otherwise rote or repetitive. I'm really excited to hopefully graduate from that era of computing, where we're not doing these rote, repetitive things. We can focus on the more human things.” - Conrad Kramer

AI Risks to Consumers

Deceptive marketing

- “The biggest issue that consumers face is this lack of transparency, which is a recurring theme throughout the day today. The two biggest sources of that lack of transparency, I think have been ambiguous or deceptive marketing, and then also obfuscation.” - Karen Hao
- “Discussions of AI are often accompanied by a lot of marketing or hype surrounding how novel or revolutionary it is. But in reality, complex models have been used in consumer financial markets for a long time. For example, in credit underwriting and credit scoring. Modern deployments of AI are of course increasingly complex and powerful, and rely on incredible amounts of data, but complex models have fundamentally been around in the markets we oversee for a while.” - Atur Desai

Hallucinations

- “[Hallucinations]: Because these models are trained on a lot of data, and then they're ultimately generating more data through statistical correlations, they're not actually extracting specific pieces of information for you from the web. It's a probabilistic completion of either pixels or text, or now we're getting into video, probabilistic video completions.” - Karen Hao

Mistakes in critical, high-stakes contexts

- “So you could definitely foresee a consumer wanting to upload an image of an MRI scan for example, or an MRI report at length and say to ChatGPT, ‘Please summarize this for me in lay language.’ And what they found was they asked a bunch of radiologists to evaluate the summaries that ChatGPT was giving them, and many, many, many instances, the summary was just completely wrong in a way that would be harmful to the patient. So in one particularly egregious example, there was an MRI scan of a growing brain tumor, and ChatGPT said, ‘This brain does not seem to be damaged.’” - Karen Hao
- “And of course, there was that infamous case of a lawyer who then used OpenAI's technology to try to figure out whether he could get some assistive help on his legal research, and it ended up fabricating everything.” - Karen Hao
- Criminal accusations: “this has been a problem with predictive AI models, where someone might've gotten falsely arrested by a facial recognition algorithm and they didn't know that it was a facial recognition algorithm at work.” - Karen Hao

Lack of awareness of supply chain inputs

- “There's the AI model developers, and then there are the consumer-facing companies that are taking the models and integrating it into a consumer facing product. And one of the challenges now is these supply chains have become so convoluted that consumers don't actually know ultimately what is the underlying model that they are interfacing with.” - Karen Hao

- “And from my perspective, as an investigative journalist, it is really, really complicated and it takes me a lot of time to and unspool all of the different ingredients, all of the different vendors, all of the different challenges of these tools. So as a consumer, it feels really impossible.” - Karen Hao
- “So labeling on privacy is a problem, but also labeling on privacy, privacy for me comes down to the most important question when you're using any product. Where is the data? Is it on a computer that you own, or is it on a computer that someone else owns? And first of all, even knowing that is challenging with some of these products.” - Ben Winters
- “Companies can actually send their data to another company. For example, to do analytics, and then that company could be doing training with that data. There's already a supply chain problem with data acquisition, and we actually saw some of that with the General Data Privacy Regulation (GDPR), where there's actually some transparency regulations where all of the sub processors for all the data companies have to be listed. Which I think is great progress, but I still think that from a consumer perspective, it's fairly opaque of what is this company allowed to do with my data.” - Ben Winters

Social harms

- “Social harms, which are often a little bit less tangible, like the impact on the environment, the fracturing and stressing of the information ecosystem that the availability of these text generation tools has.” - Ben Winters
- “The impact on elections, the impact on that competition ecosystem. And then there are also individual harms.” - Ben Winters

Data privacy

- “So that is the data theft, the data security, the victims of non-consensual intimate imagery that people can create with these available tools. And so that's one binary way of thinking about it.” - Ben Winters
- “... increased opaque data collection. In addition to scanning and scraping the internet, there are these exploitative turns on the relationships that companies have with users for years.” - Ben Winters

Data security

- “The concept of data minimization. The use, the building, all of this stuff is really difficult for data security. The more data you take in, the more vulnerable you are to data breaches. Just period, especially when there's no reason for it.” - Ben Winters

Harassment

- “[H]arassment, impersonation and extortion. This is a really big problem when you think about non-consensual intimate imagery, otherwise known as revenge porn. But that also comes up with potentially intimate images of children. It also just comes up when you have someone using the voice of Barack Obama, and then connecting that to a robocaller and telling voters that they shouldn't vote, or they should vote on the wrong day or something to that effect." - Ben Winters

Discrimination

- "The discrimination problem that we see on all sorts of automated systems... there's been a lot of studies on this that generative AI systems specifically really entrench discriminatory stereotypes that we've seen for a long time. You type in 'doctor,' you're going to see a white guy. You type in 'homemaker,' you're going to see a woman. It is not advancing anything, it is keeping us stuck in the past." - Ben Winters

Looking forward: How to approach AI consumer product and service development

Existing laws apply

- "Stated simply, there's no AI or fancy technology exception to the laws that CFPB enforces. The fact that you're using a complicated AI model, or that you may not understand why your model is reaching the conclusions it is reaching does not diminish your legal obligations under our laws or consumers' rights." - Atur Desai
- "... at the end of the day, if using a technologically complex model means that a company cannot comply with its obligations under federal consumer financial laws? They really shouldn't be using that model." - Atur Desai
- "Breaking the law should not be a company's competitive advantage. So I think as a first principle as we start to think about this, companies really should adhere to their obligations under the law. If a company can't comply with laws like federal consumer financial laws because their technology is too complex or otherwise? Then they really shouldn't be using that technology." Atur Desai

Integrating technologist expertise

- "One thing that is important is that we ensure that we have people with diverse perspectives and skill sets in the room, and this is a focus area for the CFPB. In 2022, we started our technologist program. And what this specifically means is that we began a program to tightly embed and integrate folks with technical expertise within our supervision and enforcement teams. These are data scientists, AI ML experts, design experts amongst other technical staff. So CFPB is putting a focus on making sure that we're building these interdisciplinary teams, so we're not just approaching problems from the perspective of lawyers, or economists or other professionals, but rounding it out with technologists who have deep knowledge of the markets that we're overseeing." - Atur Desai

Regulation & Law Enforcement

- "There is a place for legislators and regulators to force that, there are good mechanisms like audits and impact assessments." - Ben Winters

- “The other laws still exist. We have civil rights laws, consumer protection laws, fair competition laws, and while we do need a comprehensive baseline privacy law, we need laws that ban specific, really just unconscionable uses of AI. We can, a little bit, little by little, tweak and improve the status quo with the laws that are on the books.”
  - Conrad Kramer

AI safety and other labels

- "...when we start talking about AI safety in the public domain, safety has a totally different definition than public domain. And so now it's become a really clever marketing trick for companies to lean into the common interpretation of the term, which is that... It is related to privacy, security, fairness and the economic impacts of AI or its military implications, and that is a really big disconnect that ultimately allows companies to continue doing a lot of things that are not necessarily great for the consumer in the long run.” - Karen Hao
- “... a lot of other startups share this responsibility, and I think further that doing the minimum or doing what is required is one approach, but I think startups that take this seriously and actually innovate ways to give privacy to users and to build safer models, I think, will ultimately succeed.” - Conrad Kramer

More transparency and information

- “So I think just one thing is just to try to empower consumers, regulators, legislators, writers, that you can understand it and push back about it.” - Ben Winters
- “...really question what companies say and how they message things to us, not only in terms like AI safety or in the other kind of marketing that they use, but also in the way that they frame what is good for us, like the idea of deploy now and iterate later.” - Karen Hao

More governance

- “...Open AI launched ChatGPT within two to three weeks, on a whim of a decision, based on competitive pressures, and then suddenly, it bursts forth and we're all living in this new era and we all have to grapple with it, I don't feel like any of us had any kind of agency, any kind of democratic governance over that decision.” - Karen Hao