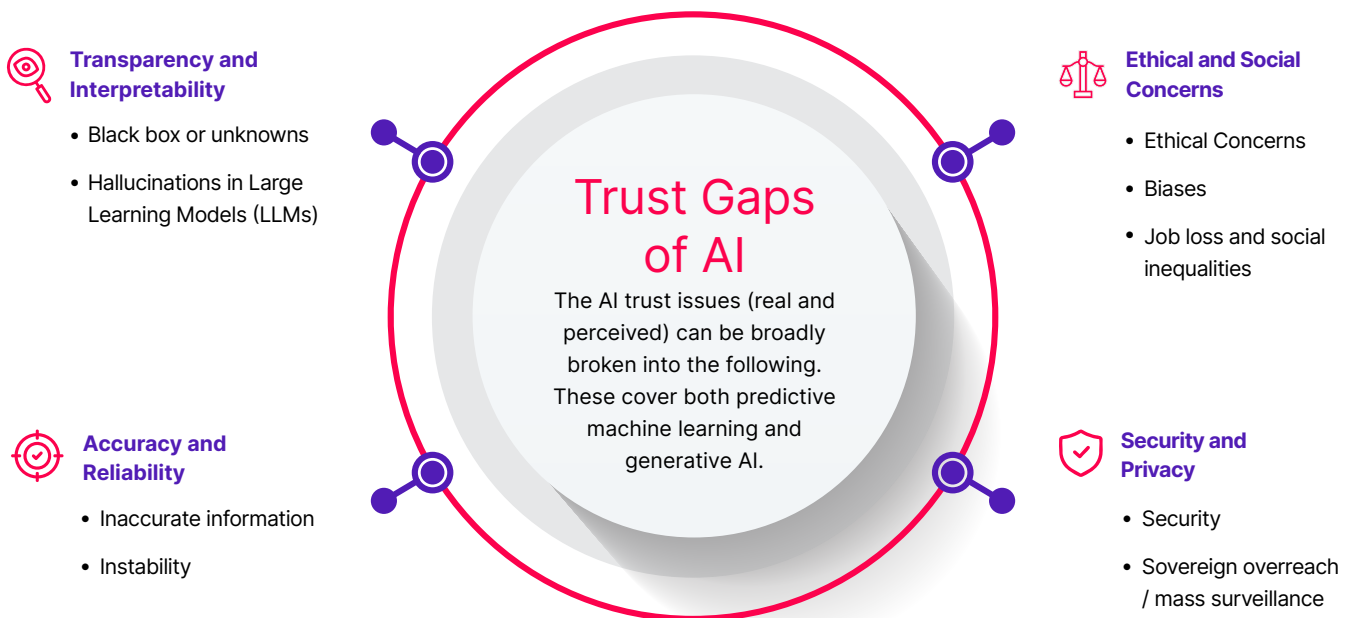November 2024

AI AIDE

Building Trust in the Age of AI

glance

Introduction

AI has been a transformative force in our world for decades, enhancing everyday life through automated decision-making technologies, robotic systems, and more. AI is transforming the way we live, work, and interact, offering remarkable potential for innovation and efficiency. While AI simply refers to systems capable of learning, adapting, and improving over time, in machine learning models using large datasets, copyright issues may arise in the training of AI as well as in the use of content generated by AI. Therefore, while adoption of AI is imperative to reap the benefits of its transformative and productive offerings, it has also become imperative to delve much deeper as AI proliferates every step of digital life at an unprecedented pace, and the corresponding legal frameworks, industry practices, and privacy approach must evolve to be in tandem. As AI's influence grows, so do concerns about its ethical implications, transparency, and the protection of personal data.

As a privacy-first organization, privacy is at the heart and centre of all our products. We extrapolate the concept of **Privacy by Design (PbD)** to **Ethical AI by Design (EaiD)** in recognition that trust and transparency are fundamental to the adoption and success of AI enabled technologies.

This document outlines our strategic approach to fostering trust in AI through rigorous ethical standards, robust data protection measures, and a transparent AI governance framework. We believe that ethical AI is not just a choice; it's a responsibility; therefore, EaiD must be applied at inception and monitored through the lifecycle of AI-driven propositions.

Transparency and Interpretability

- Black box or unknowns
- Hallucinations in Large Learning Models (LLMs)

Accuracy and Reliability

- Inaccurate information
- Instability

Trust Gaps of AI

The AI trust issues (real and perceived) can be broadly broken into the following. These cover both predictive machine learning and generative AI.

Ethical and Social Concerns

- Ethical Concerns
- Biases
- Job loss and social inequalities

Security and Privacy

- Security
- Sovereign overreach / mass surveillance

Addressing Trust Gaps through Risk Management

To address these gaps and ensure responsible use of AI, it is essential to implement a comprehensive risk management strategy that categorize(s) AI systems based on their risk levels and applies targeted mitigation measures accordingly.

Our Approach to AI – Trust Gap Risk Management

To address the trust gaps relevant to our businesses, our current approach to AI risk management broadly relies on the recommendations from the **White House Executive Order on AI (Order)** and the **European Union Artificial Intelligence Act (EU AI Act)**. The Order and the EU AI Act have many overlapping recommendations which have been incorporated within our guiding principles of product development. Besides the foregoing, we look at global laws and regulations for constant guidance and intend to abreast with their requirements, as they evolve.

The Order among other standards require, strengthening privacy-preserving research and technologies, development of standards / tools to help ensure that AI systems are safe, secure, and trustworthy, protection against AI-enabled fraud or deception, establishment of suitable cyber security measures to develop AI tools to find and fix vulnerabilities in critical software, other relevant measures to ensure security.

The EU AI Act categorizes AI systems into **different risk levels—unacceptable, high, limited, and minimal risk**. We are aware of the evolving legislative landscape around AI and privacy and ensure our EaiD and PbD framework(s) are nimble in nature to accommodate any additional requirements while implementing comprehensive best practices. Additionally, **the EU AI Act defines specific roles for the "providers" and "deployers"**. The term 'provider' in the EU AI Act covers entities that build base AI systems, whereas the term 'deployer' applies to entities that deploy AI systems built by providers for enabling certain AI-based technologies.

Colorado is the first state in the U.S. to enact a comprehensive law relating to the development and deployment of primarily high-risk artificial intelligence (AI) systems and adopts a risk-based approach to AI regulation that shares some similarities with the EU AI Act.

As a 'deployer' of AI enabled propositions, Glance's offerings typically use "general purpose" AI models (those which can be applied to a wide range of purposes without being limited to a specific function). For illustrative purposes, please see our AI Looks proposition below which only attempts to create AI generated images of the users in imaginative avatars. These models typically fall within limited or minimal risk category as they are applied in the contexts such as entertainment, commerce and content discovery. While the risk levels associated with these models are generally lower, we endeavour to ensure responsible deployment and ongoing risk management.

User accepts TnC and Privacy Policy at/before the collection of Personal Data
(Sample Screens for Illustration Purposes)
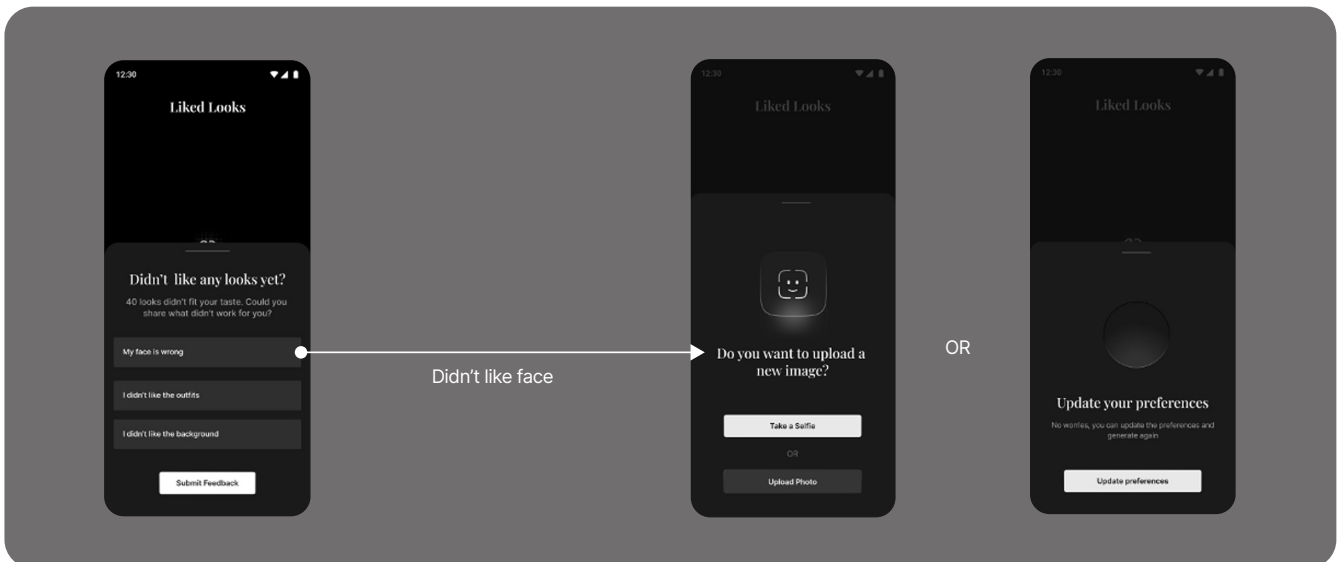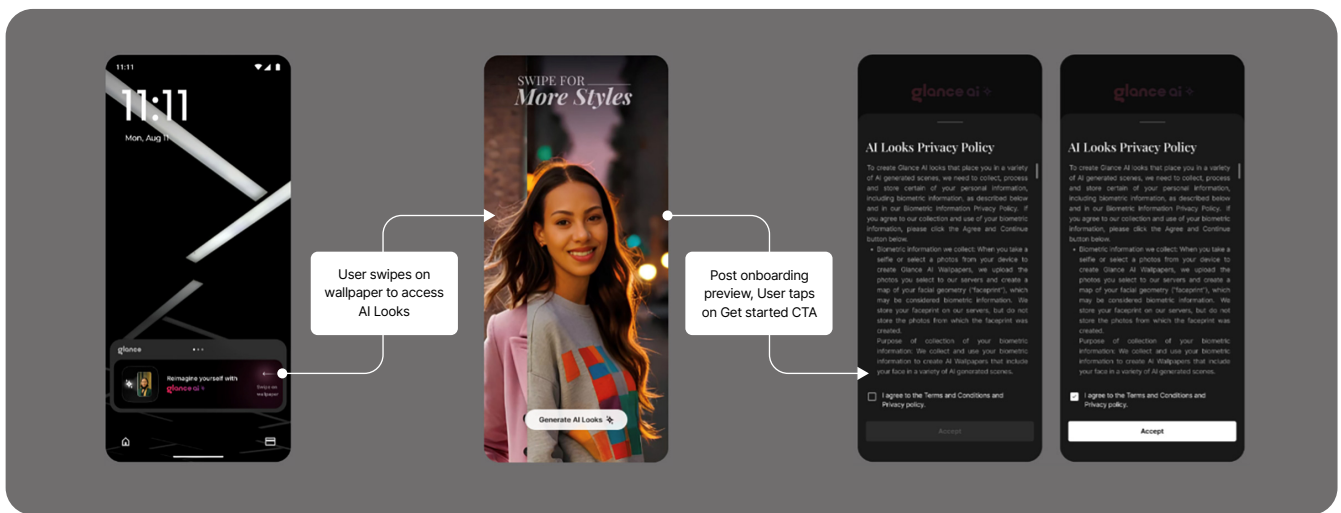
Glance's AI promise

We have already been leveraging AI to enhance content personalization, delivering curated and engaging experiences to users. As we advance, Glance AI unlocks new possibilities with features like personalized AI-generated looks, dynamic brand curation, AI-powered shopping, and personalized fashion trends and much more. Throughout these innovations, we strive to creating ethical and transparent AI offerings founded upon strong privacy and EaiD principles.

Glance's Responsible AI Framework

Security:
Protecting AI systems, data, and infrastructure.

Transparency:
Ensuring openness about AI usage and privacy practices.

Our Fundamental Tenets

Privacy:
Respecting user privacy through consent, data rights, and purposeful use.

Fairness and Inclusiveness:
Mitigating bias to ensure fairness in AI decision-making.

Accountability:
Maintaining ethical AI practices through clear policies, ethical oversight, and regular audits.

We have established a robust governance framework that includes an AI Governance Committee to oversee ethical and responsible use of AI technologies. This committee is supported by a comprehensive guideline and endeavours to ensure that we adhere to the fundamental tenets. We aim to fostering trust, mitigate risks, and deliver valuable AI-driven experiences.

- **Transparency**

This involves openly communicating when AI technologies are involved and how they function, indicating a clear view of AI's capabilities and limitations for an informed choice. We provide users with accessible information and tools to understand and manage their interactions with AI. Our efforts include creating clear documentation, maintaining open channels for feedback, and involving users in discussions about AI's role in their digital experience.

- **Privacy**

At Glance, protecting user privacy is a fundamental principle that guides all our AI initiatives. Our commitment to privacy is woven into every aspect of product development and deployment, where we adhere to a privacy-by-design approach that embeds safeguards from the start. Glance incorporates principles embedded in The California Consumer Privacy Act (CCPA) such as giving consumers opt-out rights with respect to "automated decision-making technology,"

By enabling choice, respecting their rights, minimizing the data we collect and processing only what is necessary, we reduce risks while aligning with global privacy standards. We ensure that users are fully informed and in control of how their data is handled and manage their information in accordance with applicable laws and best industry standards. We also implement rigorous third-party risk assessments to ensure that our partners and service providers adhere to the same high standards of privacy protection. Our data management practices include regular audits, privacy risk assessments, data protection impact assessments, transparent retention policies, and secure deletion processes to prevent unauthorized access and ensure data is not retained longer than necessary.

By continuously evaluating our AI systems and data handling practices, we proactively identify and address potential privacy risks, reinforcing our commitment to maintaining the highest standards of data privacy throughout the entire lifecycle of our products and services.

- **Accountability**

While we believe our use cases pose limited risks to users and their nature is largely to facilitate entertainment/gaming/shopping experiences, we proactively conduct regular evaluations of our AI systems and closely monitor their performance, impact and risk profile. We have developed an AI guideline, training modules, and awareness campaigns and collaborate with reputed partners and external experts to continuously assess and address potential risks, taking proactive steps to keep our AI systems aligned with global ethical standards and user expectations. We endeavour to ensure that the data we use to train our AI models do not include copyrighted works unless licensed or is not a wholesale reproduction of another party's database. Oversight from our AI Governance Committee provides strategic direction for responsible use AI technologies. All AI systems undergo rigorous pre-deployment and ongoing reviews to assess their performance, impact, and adherence to ethical and compliance standards, not only at launch but on an on-going basis.

- **Security**

We are deeply committed to maintaining the trust that users and partners place in us by implementing a dynamic and adaptive security framework. This framework is built on robust, multi-layered defences tailored to the specific sensitivities of the data we handle. We employ a range of techniques to protect data throughout its lifecycle, including strong encryption, hashing, anonymization, and pseudonymization to safeguard both data at rest and in transit. Our security measures are complemented by strict access controls and data segmentation strategies, ensuring that only authorized personnel have access to sensitive information. We also maintain rigorous monitoring and auditing processes to detect and respond to potential threats swiftly.

- **Fairness and Inclusiveness**

Ensuring fairness in AI outcomes is a priority. We take proactive steps to minimize biases and create equitable experiences for all users. Our diverse development team brings varied perspectives to every stage of the AI lifecycle, from design to development. We systematically assess the quality and diversity of our training data, regularly validate model outputs for potential biases, and use advanced tools to ensure fairness. In areas where risk is higher, we employ a 'human-in-the-loop' approach, incorporating human judgement to enhance decision-making.

The Road Ahead
A Commitment to Trust and Integrity

At the heart of any product company is user love, which can be attained only by establishing trust, care and upholding of privacy rights – we understand and are committed towards this. Building trust in AI is not just a policy, but rather a core value that must guide product companies to build their products to arrest and mitigate the foreseeable trust gaps and uncertainties of AI technologies. AI and privacy principles go hand in hand and developers and technology companies have a significant role to play in this arena, prioritizing ethical considerations and integrating industry best practices into their development processes. Our commitment towards overall Trust and Integrity can be discovered further in our Trust Center which showcases our products, their features, privacy practices as validated by external advisors who are celebrated names in the privacy sector: https://glance.com/trust-center