CONFIDENTIAL COMPUTING CONSORTIUM

USE CASE:

Confidential AI for Digital Marketing & Data Collaboration

Executive Summary

Digital advertising has become one of the world's largest and most competitive industries, with global advertising spend projected to exceed $600 billion annually. Brands face constant pressure to improve campaign performance, reduce wasted spend, and identify winning creative before investing heavily in media distribution.

AI-driven emotion and attention measurement has emerged as a scalable alternative to traditional consumer testing, enabling marketers to evaluate advertising effectiveness faster and at lower cost. However, the effectiveness of these models depends on access to large, diverse datasets. In practice, many of the most valuable datasets remain inaccessible because of privacy regulations, biometric data protections, and commercial concerns surrounding proprietary information.

Confidential Computing addresses this challenge by enabling organizations to collaborate on AI training and analytics while maintaining control over sensitive data. By protecting data during active computation and providing verifiable assurances about how data is processed, Confidential Computing allows organizations to participate in data-driven innovation without exposing underlying datasets.[1, 2]

Business Challenge

An AI measurement company specializing in facial coding and consumer attention analytics had developed a model capable of predicting advertising effectiveness by analyzing emotional and attention responses at scale. The technology offered an alternative to traditional in-lab advertising research, which can be both time-consuming and expensive. Initial deployments with a large consumer goods company demonstrated strong results, but further improvements depended on expanding the model's training data with additional biometric and behavioral datasets from third-party providers.

Those datasets existed but remained largely unavailable.

Data owners lacked sufficient technical guarantees that their proprietary datasets would remain protected throughout the processing lifecycle. Traditional cloud security approaches could safeguard data at rest and in transit, but data was still exposed while being processed. At the same time, regulations such as GDPR and CCPA increased scrutiny around the handling of sensitive consumer information and cross-border data use.

As a result, access to the data needed to improve model accuracy became the primary constraint on further AI development.[1,3]

How Confidential Computing Addressed the Need

The solution was deployed on Confidential Computing-enabled GPU infrastructure, creating hardware-protected Trusted Execution Environments (TEEs) for AI training and analytics workloads.

Within these environments, sensitive biometric and behavioral datasets remained protected throughout computation. Data owners could verify the integrity of the execution environment through hardware-based attestation before authorizing access to their data. This ensured that only approved code could process information and that data remained inaccessible to cloud providers, infrastructure administrators, and other unauthorized parties.[1,2]

By shifting trust from contractual agreements to cryptographic verification, Confidential Computing fundamentally changed the data-sharing model. Organizations that had previously been unwilling to contribute sensitive datasets gained the technical assurances necessary to participate in collaborative AI initiatives.

This approach enabled privacy-preserving access to larger training datasets while maintaining regulatory, commercial, and security requirements.[2,3]

Results & Business Value

With Confidential Computing in place, the available training dataset expanded by 319%, providing a significantly broader foundation for model development and validation.[4]

The enriched training data improved the model's ability to predict advertising effectiveness across audiences, channels, and geographies. According to a published case study, a consumer packaged goods company leveraging AI-driven attention and emotion analytics achieved approximately 5% sales growth by identifying higher-performing advertising creatives earlier in the campaign development process.[4]

The increased scale and diversity of the training data also reduced dependence on expensive real-world testing and accelerated the generation of actionable insights across multiple advertising formats.
Beyond marketing applications, the same Confidential AI architecture provides a foundation for data collaboration in other highly regulated sectors where sensitive data access remains a barrier to innovation, including financial services, healthcare, and biometric analytics.[1,3]

Key Takeaway

For many AI initiatives, the limiting factor is no longer model architecture or compute capacity—it is access to high-quality data.

Confidential Computing addresses this challenge by protecting data not only at rest and in transit, but also during active processing. Combined with hardware-based attestation, it provides a verifiable foundation for trust that enables organizations to collaborate on AI and analytics without relinquishing control of sensitive information.

As organizations seek to unlock greater value from distributed and proprietary datasets, Confidential Computing offers a practical path to scaling AI innovation while maintaining privacy, security, and regulatory compliance.

References

1. Confidential Computing Consortium. Confidential Computing Definition and Overview.
https://confidentialcomputing.io
2. Google Cloud. How Confidential Computing Lays the Foundation for Trusted AI.
https://cloud.google.com/blog/products/identity-security/how-confidential-computing-lays-the-foundation-for-trusted-ai
3. Opaque Systems. AI and Confidential Computing: A Virtuous Cycle of Value and Innovation.
https://www.opaque.co/resources/articles/ai-and-confidential-computing-a-virtuous-cycle-of-value-and-innovation
4. Canonical & Super Protocol. Case Study: Confidential AI for Digital Marketing & Data Collaboration.
https://assets.ubuntu.com/v1/65e4a630-Super%20Protocol%20x%20Canonical%20Case%20Study.pdf