Confidential computing:

A non-technical guide

00

Contents

01

Executive summary

In this digital world, where concerns about privacy and security are paramount, businesses can't afford to make missteps with their data. Maintaining trust online is crucial, particularly as global data regulations continue to evolve to meet people's privacy expectations. The future of digital advertising will use privacy-enhancing technologies to open up powerful opportunities for businesses to use their responsibly-collected customer data with protections built in that weren't previously possible.

Confidential computing is emerging as a pivotal technology for the advertising industry, addressing these concerns head-on and giving regulators a new opportunity to support user privacy and the businesses that rely on digital ads.

Confidential computing is a hardware-based ***privacy-enhancing technology*** (PET) that sets a new standard for how data can be processed securely by providing verifiable assurances of data protection. It provides transparency that can help foster trust between businesses and consumers, and pave the way for a more ethical and sustainable digital ecosystem.

Two key principles underpin this revolutionary technology:
(1) data is isolated in a ***trusted execution environment*** during use to protect against unauthorized access by anyone - including the environment's operator, and
(2) data security and usage is formally certified through an auditable ***attestation*** process via an independent third-party.

Confidential computing offers a transformative solution for digital advertising, by enabling businesses of all sizes to transparently protect their data, building trust with prospective and existing customers, establishing safeguards and enabling a more sustainable advertising ecosystem.

By incentivizing the use of privacy-enhancing technologies (PETs) like confidential computing into new or revised regulatory frameworks, policymakers have a crucial opportunity to accelerate the adoption of confidential computing.

This can help foster a more trustworthy online environment, encourage widespread adoption of privacy-enhancing technologies and ultimately drive data privacy and economic growth.

02

Introduction

Every day, people go online to learn new things and get things done, and to stay connected, entertained and informed — all thanks to a web that is open, easily accessible and home to countless businesses of all sizes. This digital ecosystem creates value for everyone involved: people, businesses, nonprofits, publishers, job seekers, creators, and developers alike.

Data sits at the core of this thriving, vast ecosystem and enables experiences that reflect all of the interactions happening online — from people planning their next vacation, to a business reaching customers interested in its services, to a nonprofit connecting with new donors, or a creator promoting a new fitness class.

The importance of consumer trust

Growing concerns about how data is used and protected are affecting consumer trust online, prompting businesses to rethink how they interact with their customers, each other, and how they collect and activate information that their customers chose to share with them directly.

Businesses today are facing multiplying challenges. Not only are they looking to grow while catering to their customers' needs, they also have a legal and ethical obligation to uphold more stringent data practices.

80%

of people are concerned about the state of their online privacy.

However, people still expect helpful experiences with brands online

74%

of people say they **only** want to see ads that are relevant and useful to them

Source: i.) Google / Storyline Strategies, Ad Controls, US, UK, CA, AU, MX, BR, FR, DE, IN, JP, n=1,000 per market, A18–55 with Internet access, March 2022. ii.) BCG / Google, "Consumers Want Privacy. Marketers Can Deliver." BCG, January 21, 2022.

03

The regulatory landscape

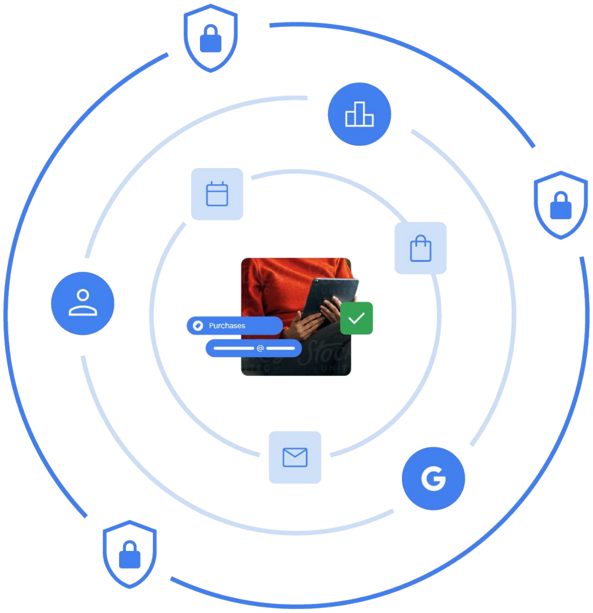
Data practices are increasingly being shaped by regulatory efforts to strengthen individual privacy protections — a reflection of the growing concern among consumers about how their digital information is collected, processed, and shared.

Take the General Data Protection Regulation (GDPR) as an example. The GDPR came into effect for the European Economic Area (EEA) in May of 2018, and set a new standard for data protection, focusing on rules that govern the processing of personal data by data controllers — an approach that was eventually replicated by other countries, such as Brazil and South Africa.

Meanwhile, in the United States, some individual states have pursued different strategies to govern privacy and data protection, sometimes focusing on how information may be shared or sold. In other parts of the world, some countries have taken approaches that are more conservative than the GDPR, such as India's Digital Personal Data Protection Act (DPDP) or South Korea's Personal Information Protection Act (PIPA). These are just a few examples that highlight how global and diverse the privacy regulatory landscape for data privacy has become.

Even though privacy regulations can vary across the globe, the core concerns they aim to address remain consistent - balancing the important role data plays in sustaining competitiveness and economic growth, while delivering on key consumer privacy protections, including but not limited to:

- Giving users transparency and clear, meaningful data controls
- Responsibly restricting how data is shared and used beyond the context in which it was collected
- Limiting how people are tracked across the web and limit the amount of data being collected
- Providing added protections to prevent data misuse for at-risk groups, including minors



These regulations have redefined online experiences and business practices, and specifically called for additional safeguards. PETs secure data through its lifecycle — from collection to processing. There is a tension when it comes to digital advertising. While specific regulation across the globe differs, there are consistent approaches in defining technologies that are private by design.

The National Science and Technology Council in the U.S. has highlighted that the deployment of PETs should be practical and efficient, ensuring their accessibility to smaller players.

The Council describes PETs as ways that let companies gain insights from personal data without exposing or allowing access to people's' sensitive information, such as email addresses or birth dates. This definition of PETs is similar to those of other regulators, including the UK's Information Commissioner's Office (ICO) and data minimization provisions in the EU's General Data Protection Regulation (GDPR). The Federal Trade Commission (FTC) recognizes a variety of PETs, each with unique benefits and use cases, that can be combined within a company's privacy strategy.

The NSTC's definition above is consistent with the approaches put forth by the United Kingdom's Information Commissioner's Office (ICO) and the General Data Protection Regulation (GDPR).

Privacy is of course important to people. Research from BCG and Google indicates that when people are shown ads online, 74% of them still prefer to see ones that are relevant and helpful. And that relevance is delivered with ads personalization, which requires some data to work. So a key challenge emerges: balancing privacy protection with business needs, especially for smaller, local enterprises. It's why more companies everywhere are turning to privacy-enhancing technologies for solutions that can help everyone strike an appropriate balance in their marketing.

Privacy Enhancing Technologies support a safer ads ecosystem

04

Privacy Enhancing Technologies

The role of privacy-enhancing technologies

As more companies collect and share first-party data with each other - for example, for marketing purposes, privacy-enhancing technologies (PETs) offer an opportunity to redefine security, and data protection.

Privacy-enhancing technologies transform privacy promises into real-world, technical solutions that can strike an appropriate balance between addressing people's privacy concerns and enabling businesses to thrive. They allow for data to be stored, collected, analyzed or processed while protecting individuals' privacy. They do this through a technical architecture that is private by design.

Businesses that utilize privacy-enhancing technologies in their marketing practices can responsibly use data to create genuinely positive customer experiences, which in turn helps support regional competitiveness on a global stage, by igniting economic growth and fostering a sustainable, thriving digital ecosystem.

However, the necessary technology for data privacy and personalization must not be limited only to large enterprises with the resources to develop or implement it. It's vital that new tools are accessible for everyone, especially small businesses that rely on digital ads to level the playing field with established competitors when trying to reach customers, and publishers that depend on ad revenue so that they can provide content at little to no cost for their audiences.

Some PETs minimize data exposure during processing:

Differential privacy adds "noise" to datasets, hindering individual identification, but potentially impacting insight accuracy.

Secure multiparty computation (SMPC) enables joint calculations without revealing individual inputs, but is complex to implement and audit.

Other PETs restrict data access:

On-device processing keeps data on the user's device, reducing the need for remote servers, but is limited by device capabilities.

Confidential computing, the focus of this whitepaper, which we'll explore next, isolates data processing in secure environments.

05

Confidential computing

What is confidential computing?

Confidential computing is a ***privacy-enhancing technology*** that safeguards data while it's being actively used or processed, using a secure, isolated space called a ***trusted execution environment*** (TEE) within a computer's hardware.

This technology addresses challenges of privacy, utility, and scalability by ensuring:

Data confidentiality throughout its lifecycle: Sensitive data remains protected even during processing within the trusted execution environment. Even though data is collected individually, it is aggregated in a way that is both useful and doesn't reveal information about any one person.

Verification of trust: Attestation, a feature of confidential computing, allows for auditing and verification of the trusted execution environment's integrity and the software running within it.

This combination of isolation and ***attestation*** ensures that data remains confidential and protected from unauthorized access, including system managers, addressing a crucial vulnerability in traditional data security.

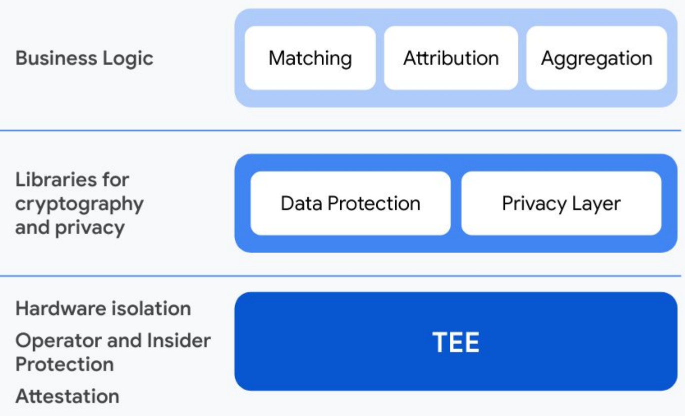
How confidential computing enables privacy

A TEE is part of a broader system, and it needs other components to work. Let's look at the three levels that go into operation of a TEE:

LEVEL 3: What is the application that runs on the TEE? It may match data, have features like data protection, or aggregate data

LEVEL 2: The data is encrypted with a key whose policy permits decryption solely by the TEE

LEVEL 1: A TEE is an environment like a server that runs in the cloud



Business Logic: Matching, Attribution, Aggregation

Libraries for cryptography and privacy: Data Protection, Privacy Layer

Hardware isolation, Operator and Insider Protection, Attestation: TEE

What are the benefits of confidential computing?

Enhanced privacy: isolation from the rest of the system
Confidential computing uses Trusted Execution Environments (TEEs) that are physically and logically separated from the rest of the server or other device. Only the people who collected the information directly, and with permission, know who they are — no one else.

Verifiable security: attestation
Confidential computing includes a feature called attestation, which allows anyone — whether an advertiser, a publisher, a regulator, or an independent third party — to audit and verify that the data within the TEE has not been tampered with, and that the software running in the TEE remains uncorrupted. This ability to prove the integrity of the environment ensures that privacy isn't just a claim but a verified fact.

How does confidential computing work?

Step 1: Secure hardware and rules of operation
Confidential computing uses a trusted execution environment which can't be accessed by anyone - including the system operator. The operations that can be performed within the trusted execution environment are governed by a set of predefined rules.

Step 2: Data encryption
When data needs to be processed, participants encrypt that data with a cryptographic key, configured to assure only a trusted execution environment running approved software can decrypt the data. The encrypted data is loaded into the trusted execution environment. The encryption configuration helps ensure that only authorized code within the environment itself can decrypt and access the data.

Step 3: Secure processing
The trusted execution environment executes the code that processes the data. This code operates within the secure boundaries of the enclave, preventing any external interference or tampering. Even if the operating system or other software is compromised, the data within the trusted execution environment remains protected.

Step 4: Attestation
To ensure trust, trusted execution environments use a mechanism called attestation. This process cryptographically verifies the trusted execution environment's identity and integrity, confirming that it's running the expected software. This provides assurance to participants that their data is being processed in a genuine and secure environment.

Example of confidential computing in financial services:

Imagine a mobile payment app using confidential computing. When you make a payment, your credit card information is encrypted and processed within a trusted execution environment. The TEE uses its cryptographic keys to decrypt the data, perform the transaction, and then re-encrypt the result before sending it back to the app. This ensures that your information is never exposed to the operating system or other apps on your phone. And companies like MonetaGo are leveraging confidential computing to enable financial fraud detection.

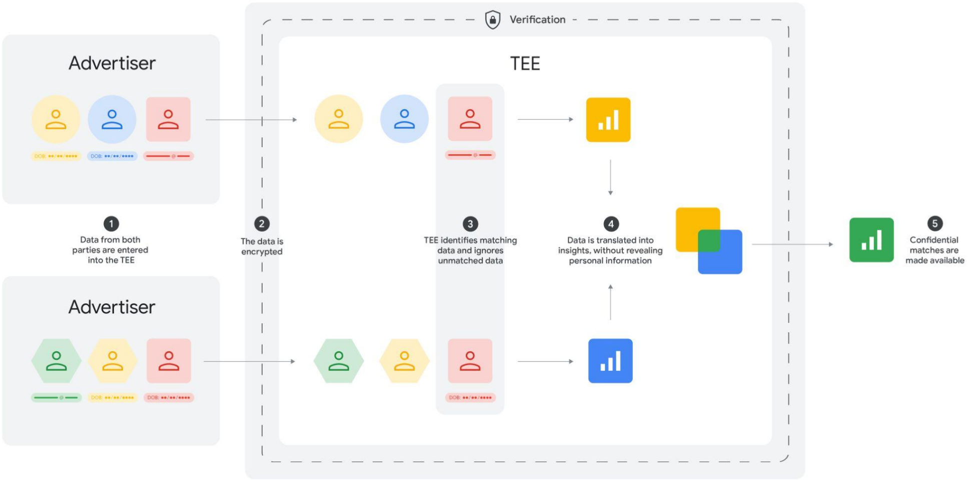
Example of confidential computing for digital advertising

Say that an advertiser, such as a retailer, wants to assess how many sales their digital marketing campaign with a certain publisher is driving for their stores. That's because many people often see online ads but then decide to go into a store to inspect the product before they buy it.

So, to bridge the gap between these online and offline activities, businesses have to match individual records about who interacted with a digital ad with who ended up buying something in-store. Confidential computing can make this process possible without revealing any additional data between the parties involved. Here's how it works:

1. The advertiser encrypts their store sales data and uploads the encrypted data to the trusted execution environment.

2. Similarly, the other party (for example, a publisher) encrypts data on how its audience has interacted with the ads displayed on its platform and uploads it to the trusted execution environment.


Verification
Advertiser
TEE
DOB: ••/••/••••
DOB: ••/••/••••
1
Data from both parties are entered into the TEE
2
The data is encrypted
3
TEE identifies matching data and ignores unmatched data
4
Data is translated into insights, without revealing personal information
5
Confidential matches are made available
Advertiser
DOB: ••/••/••••
DOB: ••/••/••••
DOB: ••/••/••••

3. Within the secure environment, confidential computing decrypts both data sets.

4. The software in the trusted execution environment then identifies the overlap of the data sets, matching users who interacted with an ad to those who made a purchase in-store.

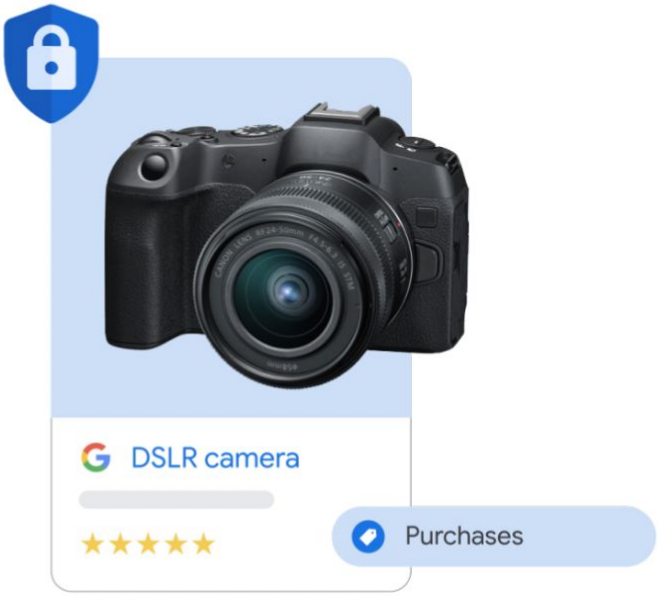
5. Finally, confidential computing generates an aggregated summary report that shows how many of the purchases happened after the purchaser viewed an ad.

Throughout this process, neither the advertiser, the publisher, nor the administrator of the confidential computing system can access the raw data, or learn new information. These privacy protections can work for any business, advertiser or publisher, big or small. Advertisers can leverage the technology to improve ad measurement without compromising user privacy. This technology can reassure everyone — advertisers and their customers, as well as publishers and their audiences — that their data is being kept private.

06

Conclusion

Privacy-enhancing technologies like confidential computing transform privacy promises into real-world, technical solutions. They give our industry the best chance to stop reacting to regulatory and platform changes and instead, drive towards a sustainable future that is good for people, advertisers and publishers.



In a digital landscape facing increasingly sophisticated cyber threats, confidential computing offers a powerful tool for policymakers to champion individual privacy while fostering a thriving digital economy. By incentivizing the use of these technologies in privacy regulations, policymakers can set a clear standard for data protection, encouraging widespread adoption and unlocking new opportunities for innovation and data sharing. This proactive approach not only safeguards sensitive information but also promotes trust among individuals and businesses, ultimately benefiting all stakeholders in the digital ecosystem. Policymakers can promote the development and adoption of confidential computing technologies by providing incentives, establishing clear standards, and fostering collaboration between industry stakeholders.

07

Glossary

Attestation

Attestation is a process used in confidential computing to provide cryptographic verification that the Trusted Execution Environment (TEE) is configured in a specific way. It confirms that the confidential computing software matches predefined standards. This provides auditable assurances for the integrity of confidential computing.

Confidential computing

Confidential computing is a privacy-enhancing technology that uses a combination of hardware and software to isolate data processing from the rest of a system or device, preventing unauthorized access.

Cryptographic key

A cryptographic key is a string of characters or numbers that can be used to encode or decode data through a cryptographic algorithm.

Differential privacy

Differential privacy is a statistical technique that introduces "noise" into datasets to protect any individual identities in the data. By adding randomness to the data, it becomes more difficult to trace specific data points back to individuals.

On-device processing

On-device processing is the execution of data analysis directly on a user's device, rather than sending the data to an external server or cloud.

Secure multiparty computation

Secure multiparty computation is a protocol that allows multiple parties to jointly compute a function without revealing their individual inputs to one another.

Trusted execution environment

A Trusted Execution Environment (TEE) is a secure area within a computer or device that isolates data processing from the rest of the system, preventing unauthorized access even from privileged users or administrators. TEEs are a key principle to the architecture of confidential computing.