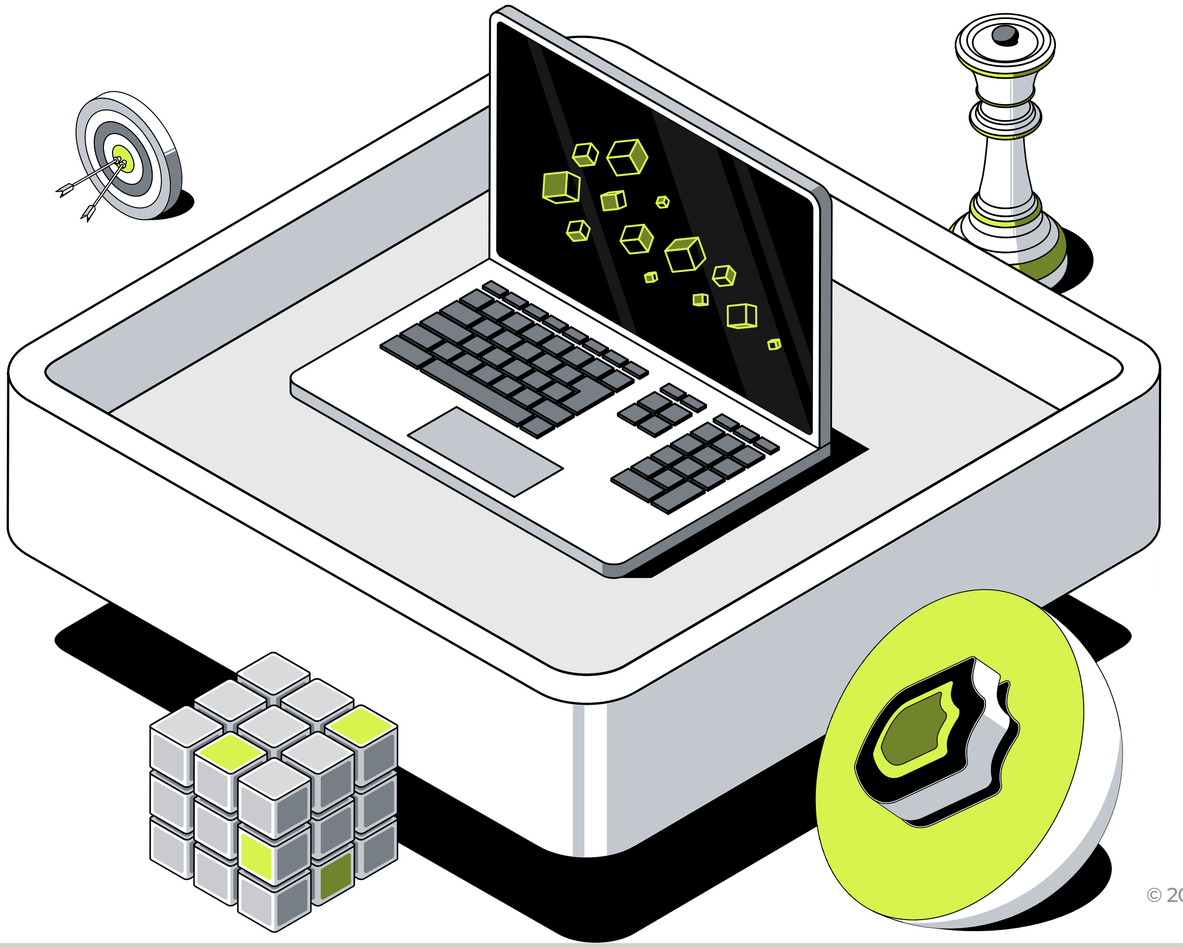
Privacy Game Changers

Understanding Privacy-Enhancing Technologies

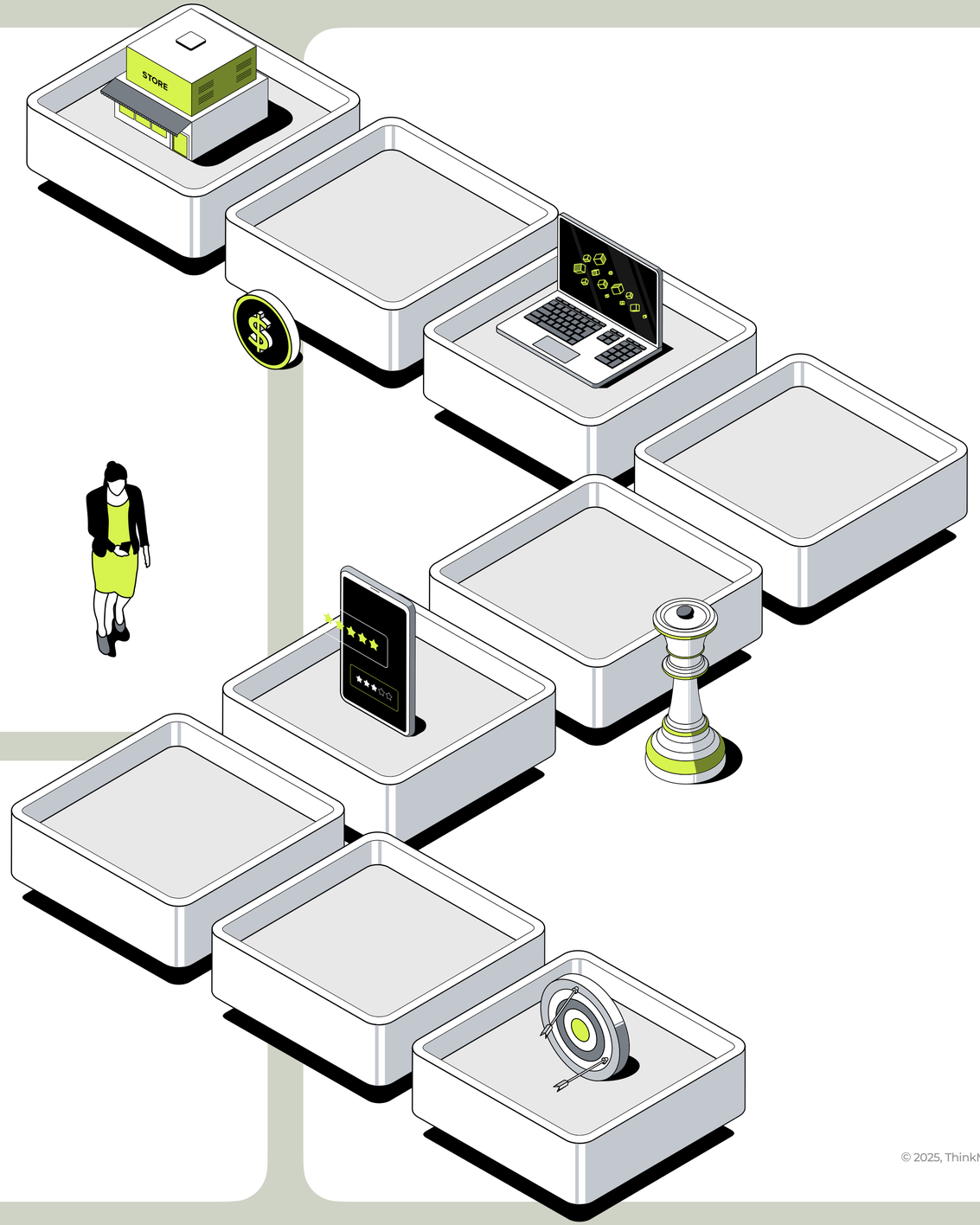


with support from

Privacy Sandbox

Views expressed by ThinkMedium are their own.

Content and services on the Internet have been supported by advertising for decades.



Online advertising has enabled personalized experiences for consumers and increased effectiveness for businesses, but **opaque practices and over-reliance on individual user data have led to growing concerns.**

Eroded consumer trust is now having real consequences for businesses.

The rise of privacy regulations and platform policies are attempts to **reflect consumer preferences and achieve a sustainable balance** for advertising use cases.

These changes have an immediate impact for businesses around the world.

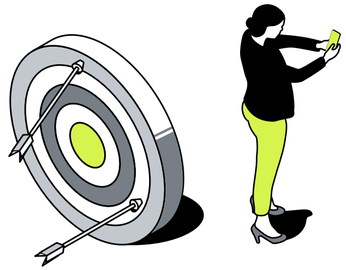
Business leaders now need to consider...

Signal Loss and Data Restrictions

Less Data and Reduced Ability to Match Consumer Data

▼

Less Personalized and Effective Advertising

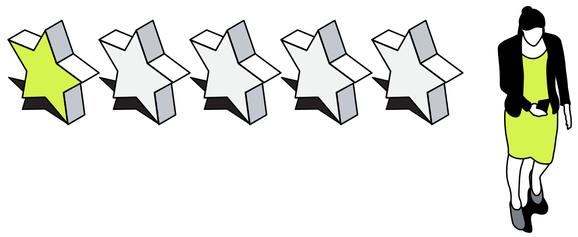


Privacy Reputation Risks

Data Breach from Poor Privacy Practices

▼

Major Financial, Branding, and Legal Consequences

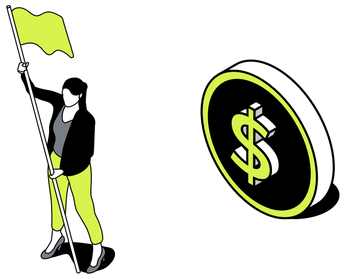


Intellectual Property (IP) Leaks

Risk of IP Leakage when Sharing Data with Partners

▼

Failure to Uphold Fiduciary Responsibilities

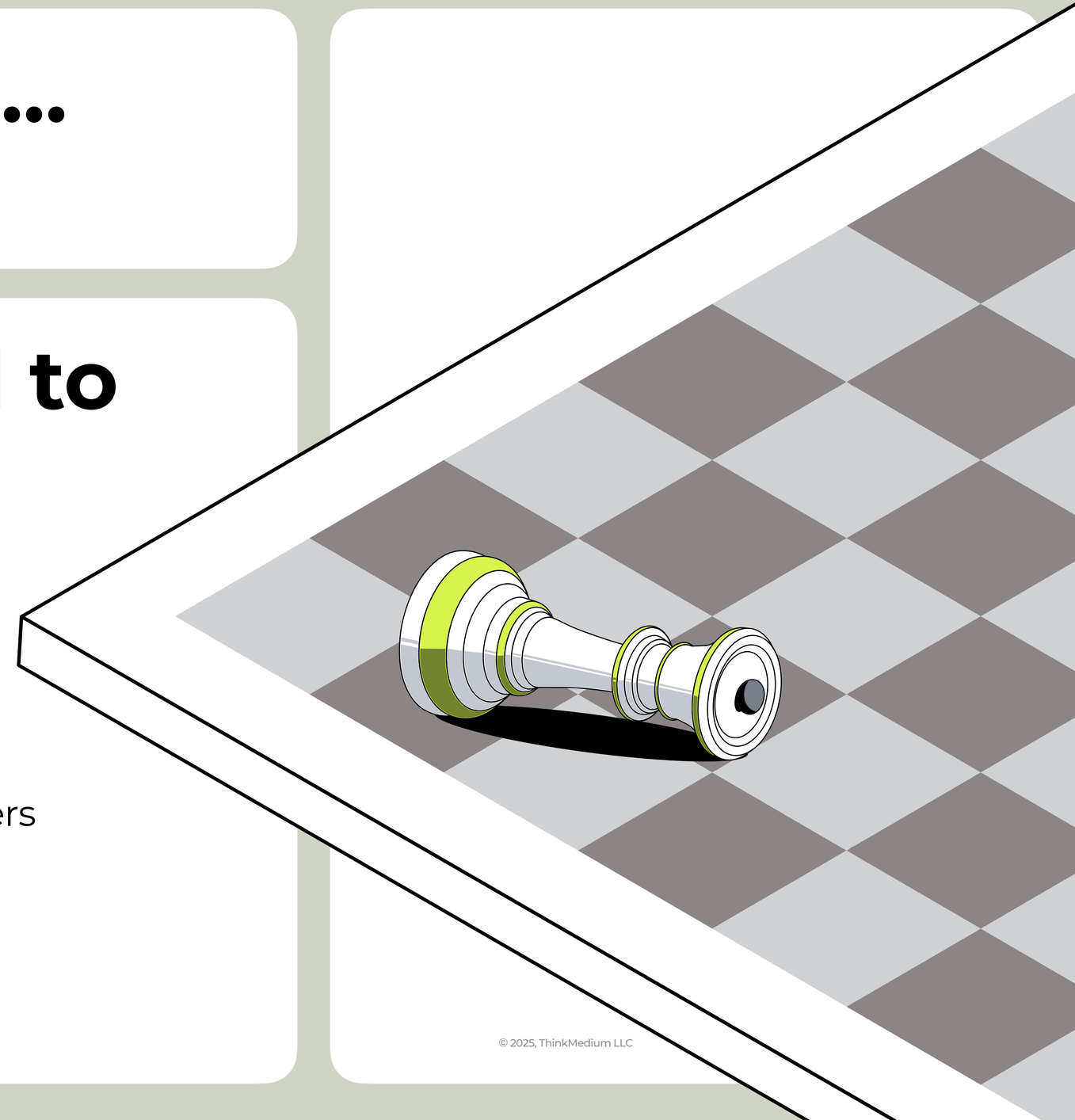


The model is broken...

...but it doesn't need to stay that way.

Privacy-Enhancing Technologies (aka PETs) offer solutions.

PETs can support a new balance where consumers maintain privacy and advertising can continue to support quality content and services.



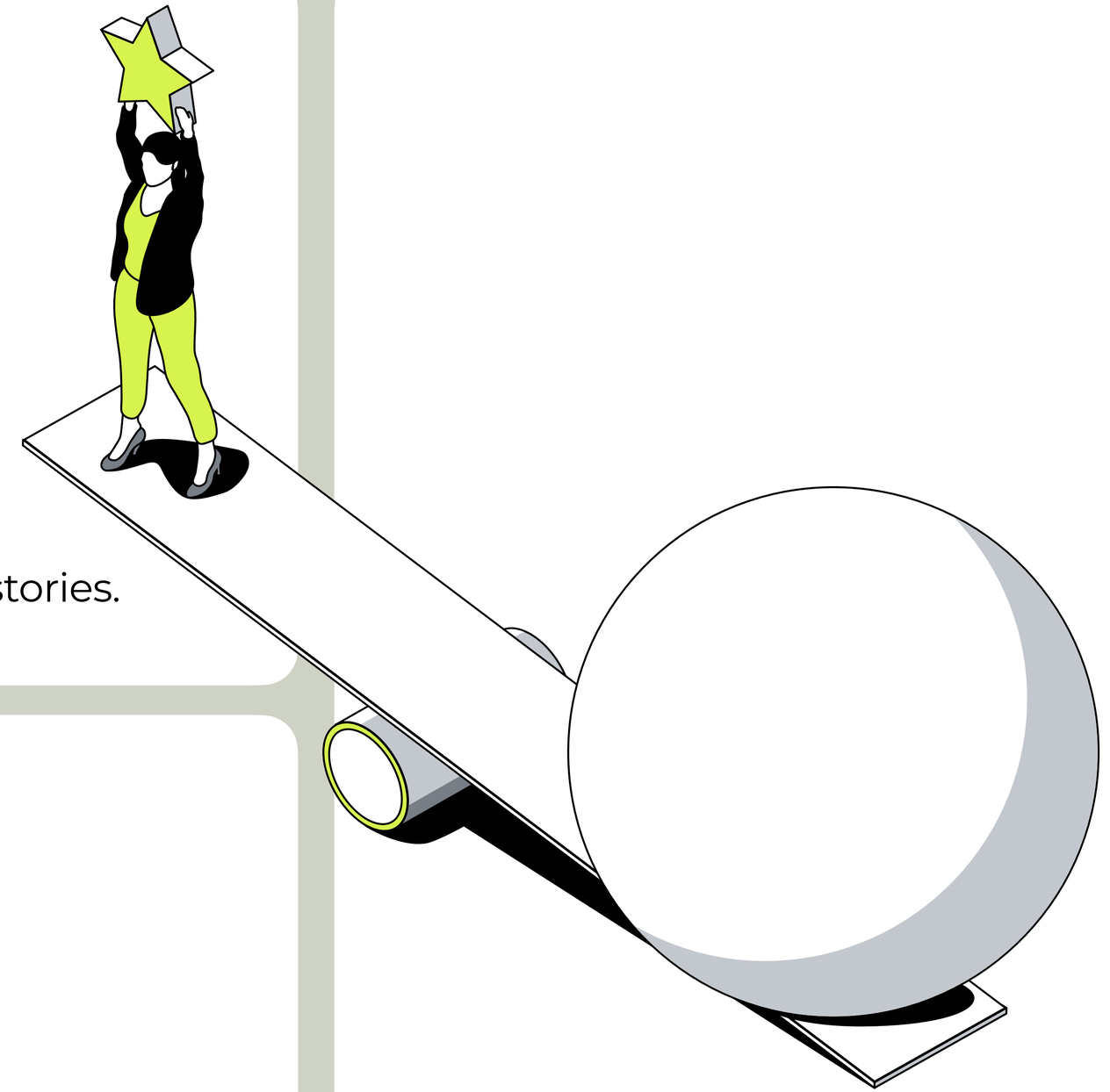
PETs have seen increasing adoption recently.

They are a collection of technologies and techniques that can “change the game” by enabling key business use cases with greater privacy and security – and reduced risk. Some PETs are methods for anonymization, while others support collaborative analysis on datasets without sharing underlying data.

When used effectively, PETs allow unique benefits of online advertising to shine, while increasing individual privacy.

PETs can support a healthy balance of privacy and ad performance.

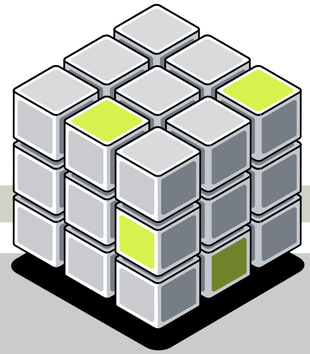
Today, advertising use cases often involve publishers, marketers, and other parties having access to person-level information and browsing histories. This level of data exposure isn't always necessary.



PETs can enable “collaborating without sharing”, preserving useful insights while exposing less data.

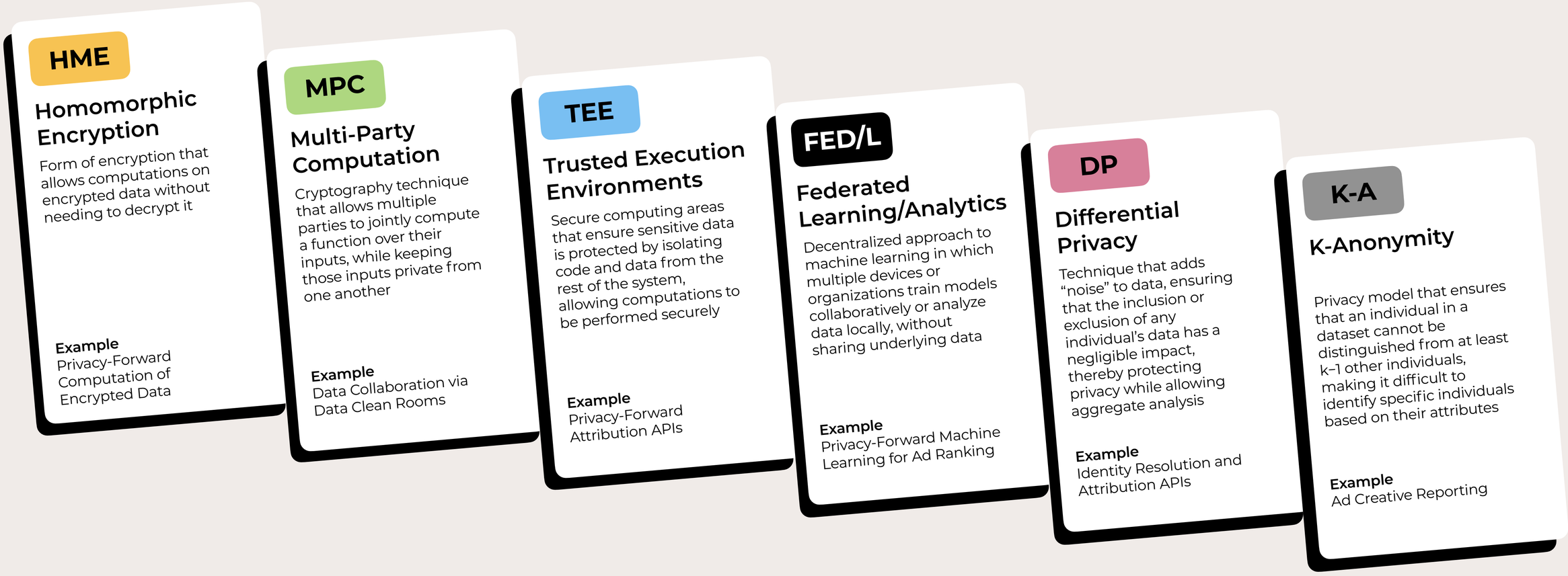
Many advertising use cases have depended upon consumer-level data.

But in most cases, addressing advertising business needs doesn't require consumer-level data resolution. **Consider these examples:**



Advertising Use Case	Business Needs
Reach & Frequency	Ensure an audience sees an ad one or more times, but not too many times
Fraud Detection	Avoid paying for ads no one sees and investing in invalid traffic
Audience Activation	Ensure ads reach their intended target personas
Remarketing	Re-engage known customers/prospects through ads
Lookalike Modeling	Prospect for new customers with attributes similar to known customers
Brand Lift	Ensure people seeing an ad knew what it was for and remembered it
Attribution & Incrementality	Assign credit for outcomes to the correct source and gauge incremental value

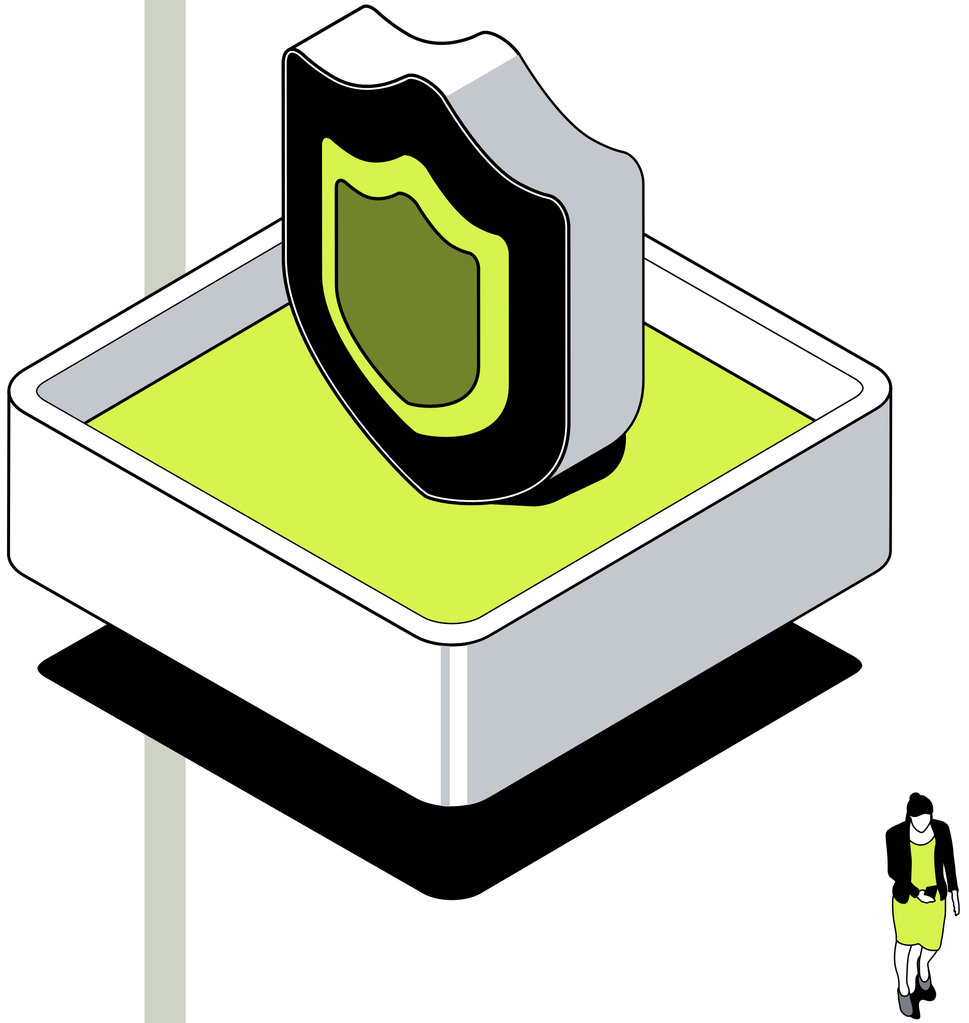
Solutions built on PETs can address the same business needs with greater privacy.



Here’s an example of how Trusted Execution Environments (TEEs) can attribute an ad-driven purchase to an ad network.

TEEs are computer hardware environments in which computation can happen in a controlled manner, with stringent control on any data going in or going out.

Software running inside the TEE can be attested, meaning that all parties can know how the TEE is processing data, and, if programmed not to, that it cannot log out user level data.
This shows how TEEs enable advanced analytics while protecting consumer data.



How does it work?

When a consumer makes a purchase, each party records data about the transaction.

Before: User Level Attribution

CONSUMERS

Clicks ad from Network A.
Browses Brand B site.
Buys pair of jeans.

AD NETWORK A

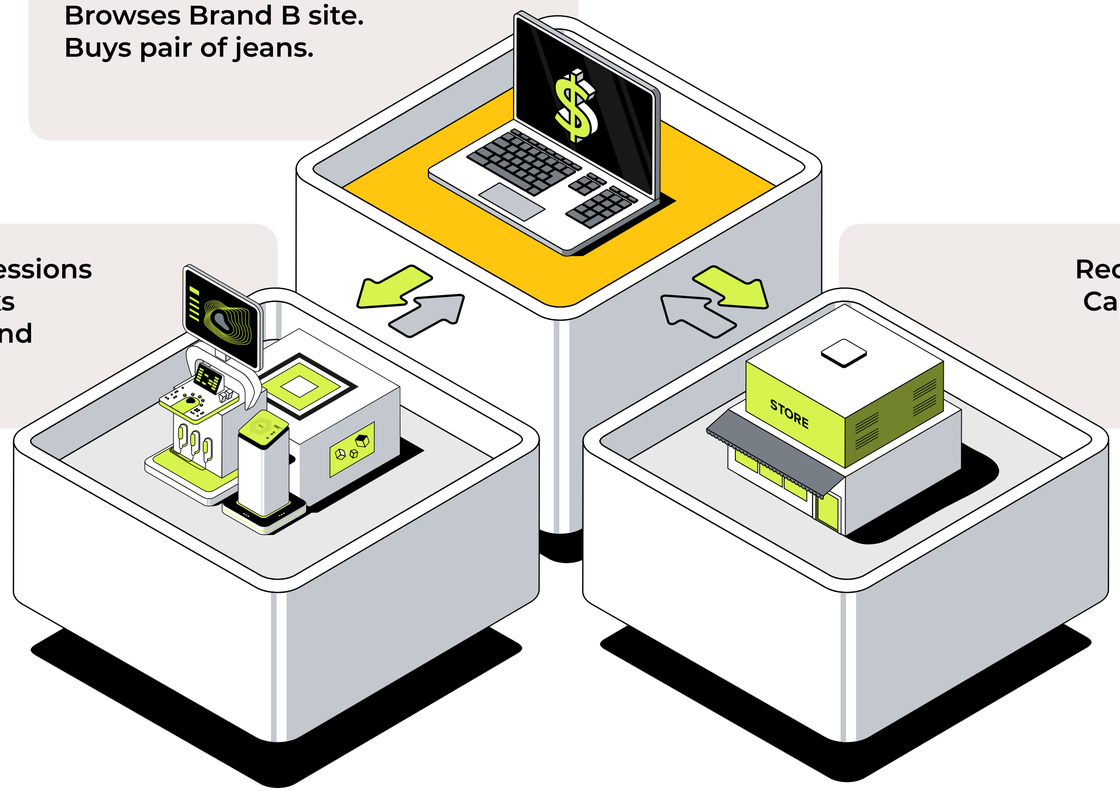
Records ad impressions
Captures ad clicks
Captures email and identity signals

Impression data
Email
Campaign

BRAND B

Records a purchase.
Captures email and identity signals.

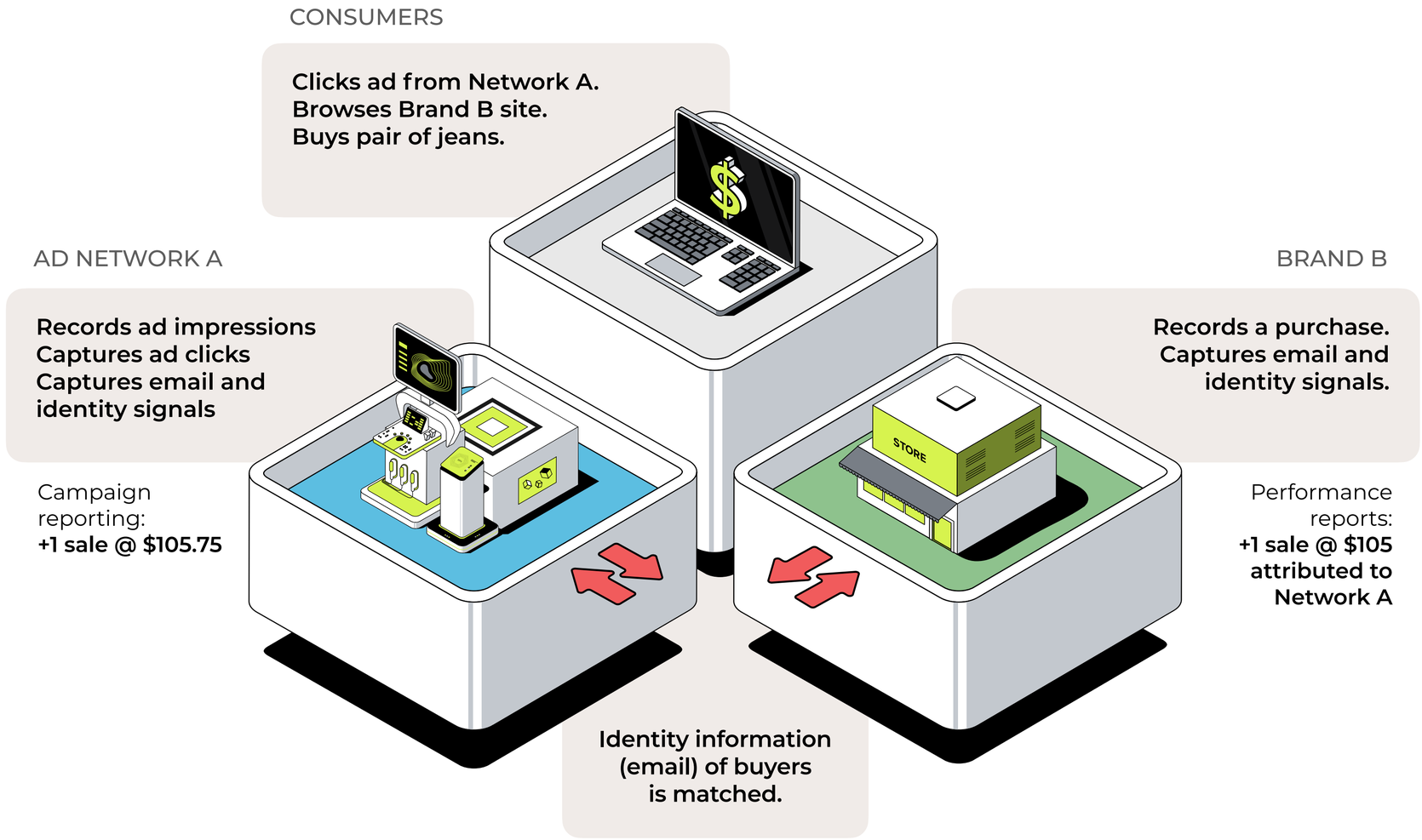
Sales data
Email
Revenue



How does it work?

To reconcile data and validate the attribution of the purchase to ads operated by Ad Network A, both parties need to exchange potentially sensitive information about the consumer.

Before: User Level Attribution



Great! But...

Processing such sensitive information without protections creates risk if data is leaked in the process of being shared with the another party.

Before: User Level Attribution

CONSUMERS

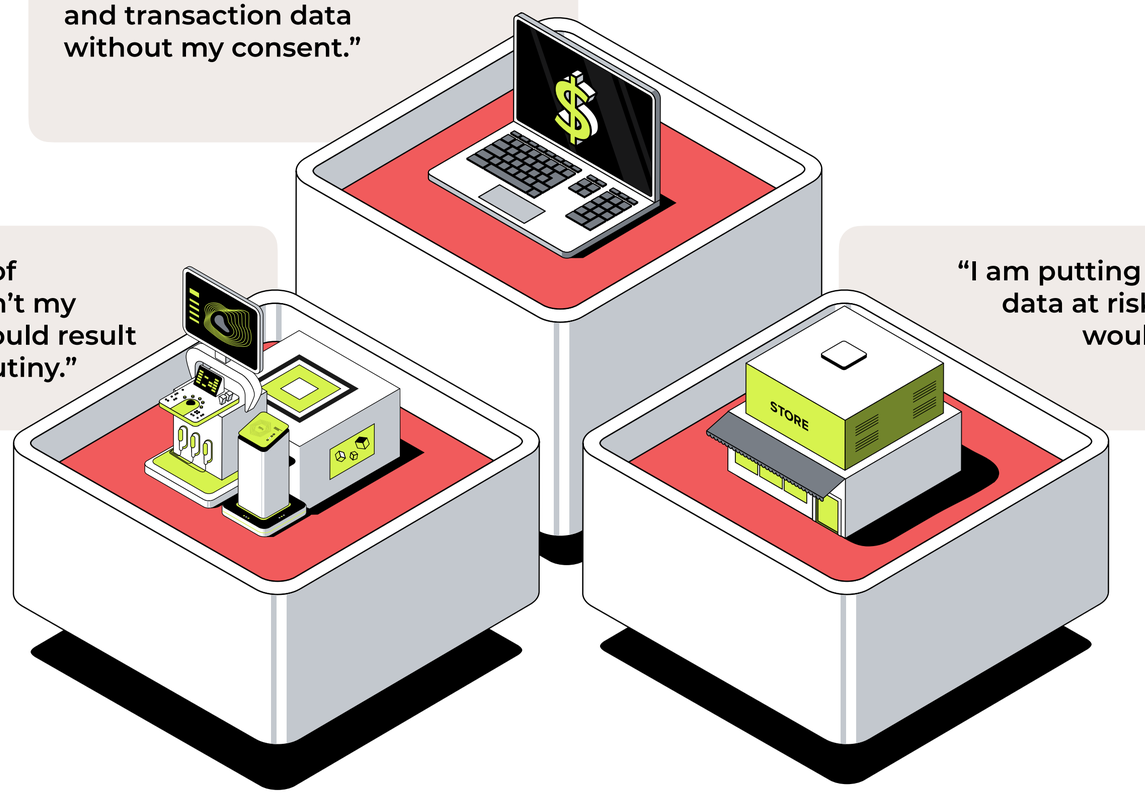
"A 3rd-party has my email and transaction data without my consent."

AD NETWORK A

"I have the data of someone who isn't my customer. This could result in regulatory scrutiny."

BRAND B

"I am putting my customer's data at risk. Data leakage would also damage my brand."



How does it work?

Trusted-Execution Environment (TEE)

Now consider the same example using Trusted Execution Environments (TEEs) to perform the attribution, with computation occurring in a controlled manner.

After: Attribution with TEE

CONSUMERS

Clicks ad from Network A.
Browses Brand B site.
Buys pair of jeans.

AD NETWORK A

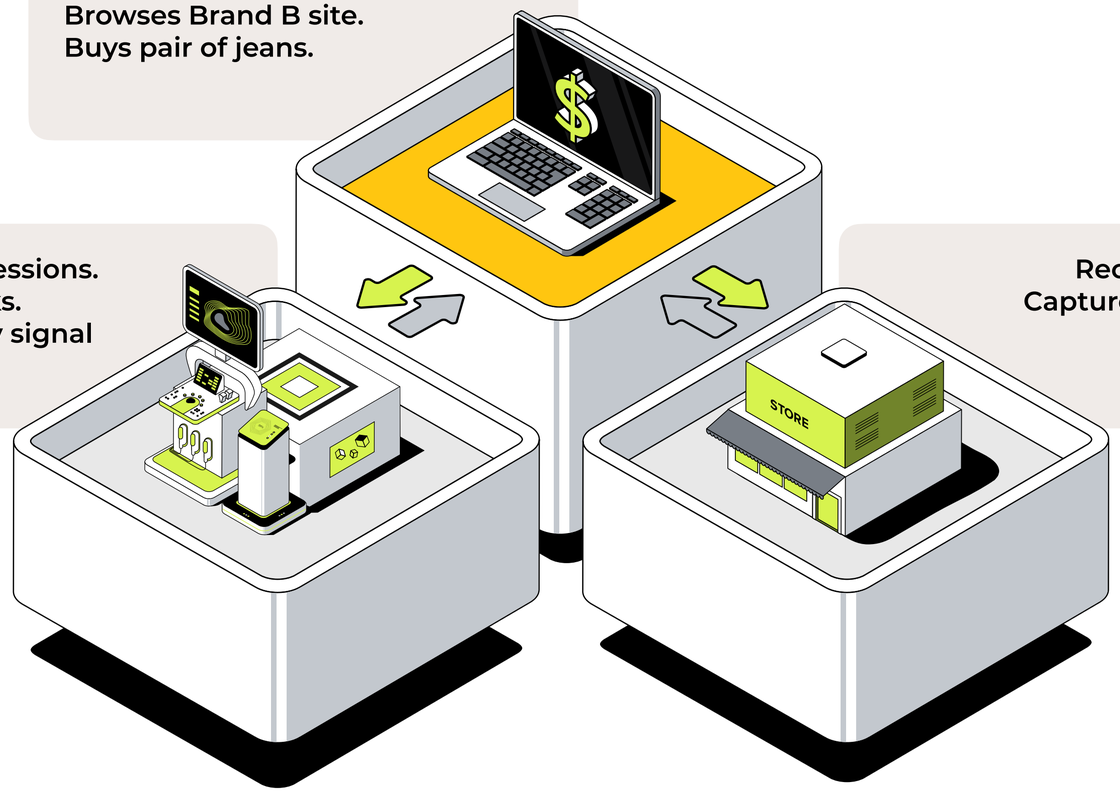
Records ad impressions.
Captures ad clicks.
Captures identity signal if needed.

Impression data
Email
Campaign

BRAND B

Records a purchase.
Captures identity signal if needed.

Sales data
Email
Revenue



How does it work?

Trusted-Execution Environment (TEE)

As in a controlled laboratory, experiments can't be observed or contaminated by other people. In our case, both sides send their data into the TEE with the intent to attribute the purchase.

After: Attribution with TEE

CONSUMERS

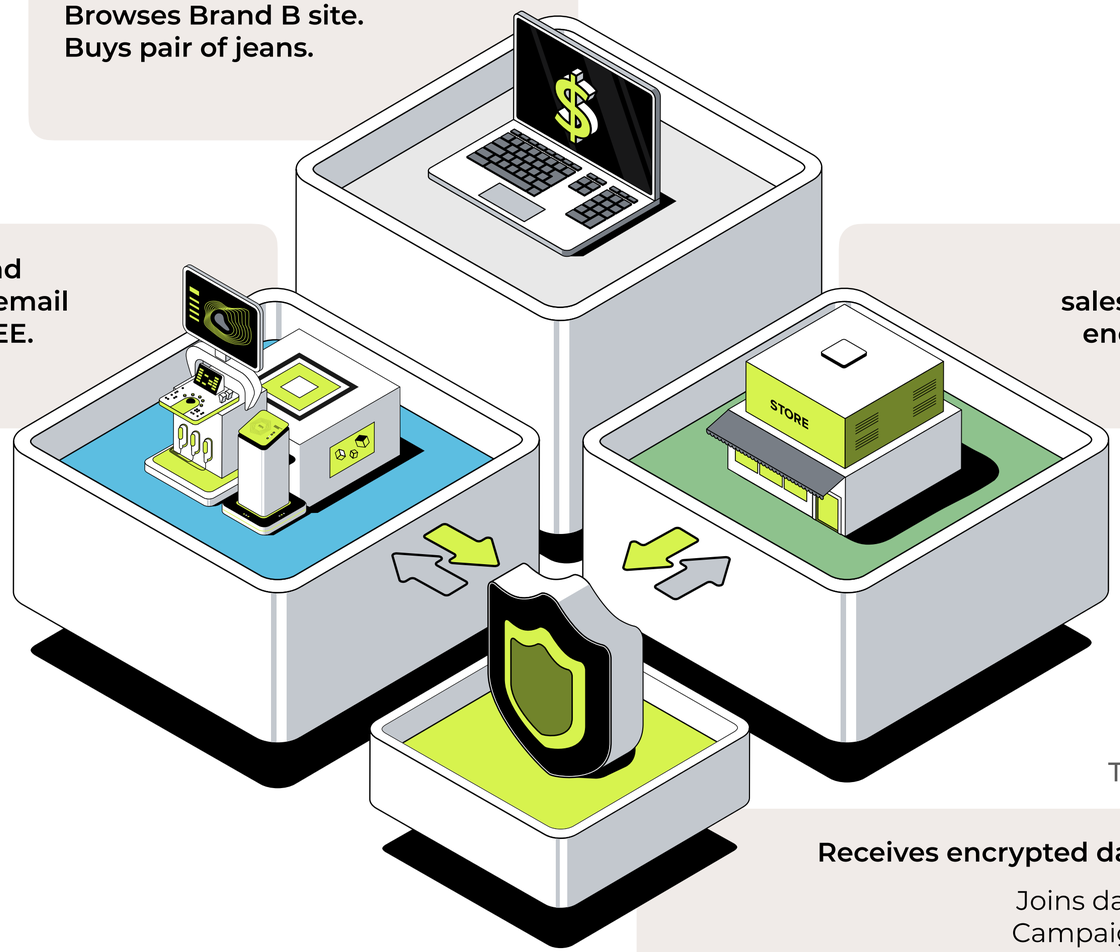
Clicks ad from Network A.
Browses Brand B site.
Buys pair of jeans.

AD NETWORK A

Sends recorded ad interaction with email encrypted into TEE.

BRAND B

Sends recorded sales data with email encrypted into TEE.



TEE

Receives encrypted data

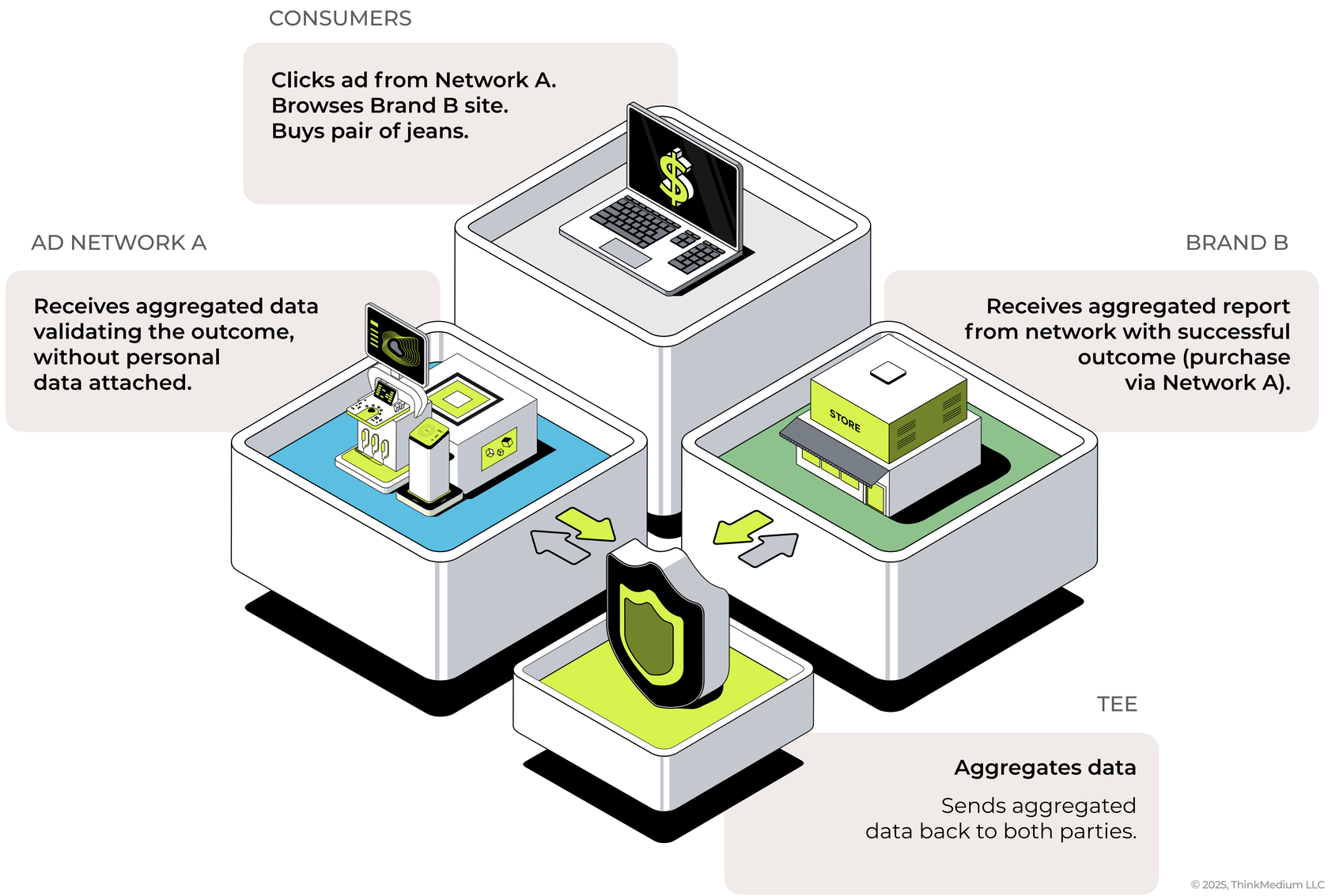
Joins data:
Campaign,
Encrypted Email, Revenue

How does it work?

Trusted-Execution Environment (TEE)

Once processed, insights are sent back securely, so that the Brand can validate that revenue was generated and the Network can receive credit for it – without needing to exchange underlying consumer data.

After: Attribution with TEE

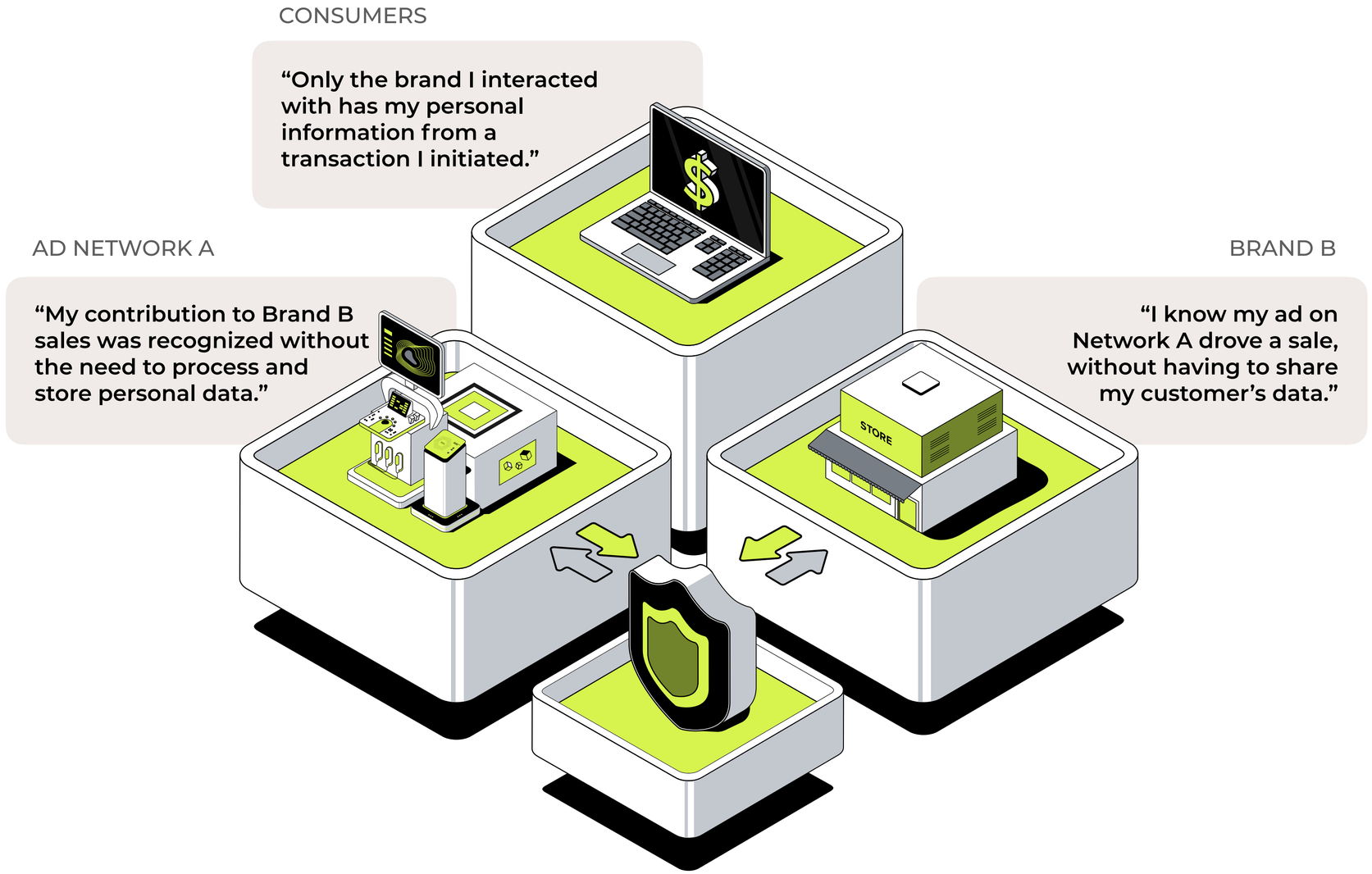


How does it work?

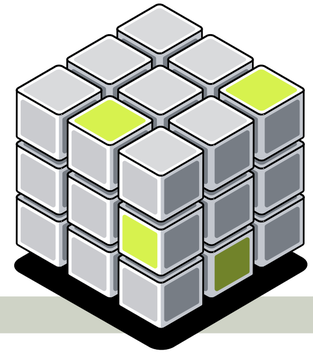
Trusted-Execution Environment (TEE)

TEEs are not foolproof as enablers of complete and secure solutions. But when executed properly, they support privacy-forward solutions to advertising use cases.

After: Attribution with TEE



These PETs are actively being used across all of our examples, today:



Advertising Use Case	DP *Differential Privacy*	FED/L *Federated Learning*	K-A *K-Anonymity*	HME *Homomorphic Encryption*	TEE *Trusted Execution Environments*	MPC *Multi-Party Computation*
Reach & Frequency	X	O	O	X	O	O
Fraud Detection	O	X	O	O	O	X
Audience Activation	X	O	X	X	X	O
Remarketing	O	X	O	O	X	X
Lookalike Modeling	X	X	O	X	X	O
Brand Lift	X	O	O	X	O	O
Attribution & Incrementality	X	O	O	X	X	X

What’s the Next Move?

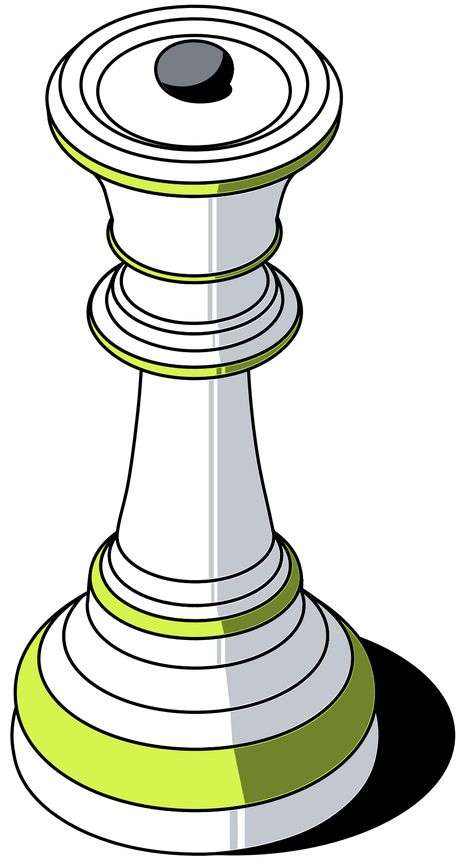
Everyone in the advertising ecosystem has a role to play in achieving privacy and security that meets the demands of consumers, regulators, and businesses.

Marketers and publishers need to understand PETs and advocate for their partners to adopt them.

Technology platforms (e.g., browsers, operating systems, ad tech providers) should continue offering developers PETs-based advertising APIs.

Trade organizations should develop standards to facilitate adoption and interoperability.

As the ecosystem and consumers become increasingly privacy-aware, companies embracing PETs will benefit.



Taking Action Now

- [ ] Think about your advertising use cases that benefit from PETs
- [ ] Engage subject matter experts at your organization
- [ ] Research and browse available industry resources
- [ ] Dive into in-market solutions utilizing PETs, such as the Privacy Sandbox
- [ ] Reach out to your platform teams and technology vendors – and our team!