

Bespoke Threat Models: Achieving Realistic Privacy Guarantees for Deployed Protocols

Kyle Hogan

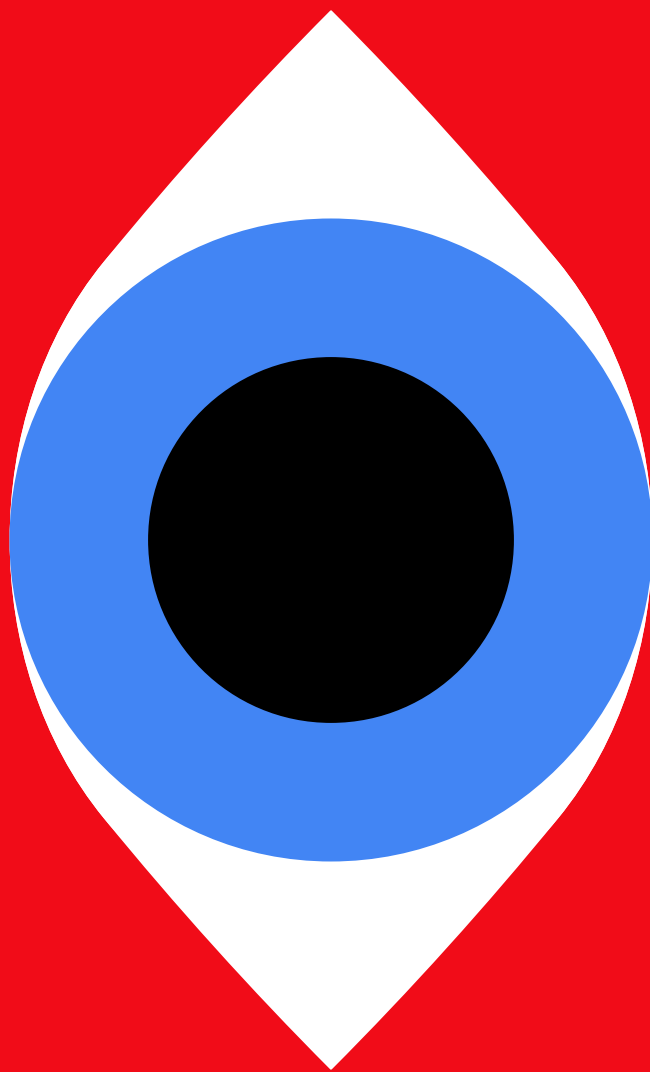
TV
PG
LV



This film has been modified
as follows from its original
version: it has been formatted
to fit your screen, to run
in the time allotted, and
edited for content.

Let's talk about ads.

***Privacy
Preserving***



***Surveillance
Capitalism***



AdBlock

Here's The Thing With Ad Blockers

We get it: Ads aren't what you're here for. But ads help us keep the lights on. So, add us to your ad blocker's [whitelist](#) or pay \$1 per week for an ad-free version of WIRED. Either way, you are supporting our journalism. We'd really appreciate it.

Sign Up

Already a member? [Log in](#)



**We have noticed
you are using an ad blocker**

We rely on advertising to fund our award-winning journalism.

Please whitelist our website or [subscribe](#) to Independent Premium our new membership service which includes an advertising-free experience, exclusive content, events and more - for as little as 30p a day.

For help accessing our website, visit our [ad blocking](#) page.

Subscribe

Log in

**It looks like you're
using an ad-blocker!**

Business Insider is an advertising supported site and we noticed you have ad-blocking enabled.

HERE ARE 2 WAYS YOU CAN KEEP READING

Turn off your ad-blocker.

DO IT NOW

Continue with BI PRIME for just \$1.

GET ACCESS NOW

TO READ THE FULL STORY, PLEASE [LOG IN](#), [SUBSCRIBE](#) OR WHITELIST.

LOOKS LIKE YOU'RE RUNNING AN AD BLOCKER

SUPPORT JOURNALISM IN COLORADO

To continue reading The Denver Post:

- [Log in to your print account](#) to get access.
- [Subscribe starting at 99¢](#) for the first month.
- Whitelist [denverpost.com](#) in your ad blocker.

99¢

FOR THE FIRST MONTH

SUBSCRIBE NOW

Already a print or replica subscriber? [Get access.](#)

Here's The Thing With Ad Blockers

We get it: Ads aren't what you're here for. **But ads help us keep the lights on.** So, add us to your ad blocker's whitelist or pay \$1 per week for an ad-free version of WIRED. Either way, you are supporting our journalism. We'd really appreciate it.

Sign Up

Already a member? [Log in](#)



We have noticed
you are using an ad blocker

We rely on advertising to fund our award-winning journalism.

Please whitelist our website or subscribe to Independent Premium our new membership service which includes an advertising-free experience, exclusive content, events and more - for as little as 30p a day.

For help accessing our website, visit our [ad blocking](#) page.

Subscribe

Log in

It looks like you're
using an ad-blocker!

Business Insider is an **advertising supported site** and we noticed you have ad-blocking enabled.

HERE ARE 2 WAYS YOU CAN KEEP READING

Turn off your ad-blocker.

Continue with BI PRIME for just \$1.

DO IT NOW

GET ACCESS NOW

TO READ THE FULL STORY, PLEASE [LOG IN](#), [SUBSCRIBE](#) OR WHITELIST.

LOOKS LIKE YOU'RE RUNNING AN AD BLOCKER

SUPPORT JOURNALISM IN COLORADO

To continue reading The Denver Post:

- [Log in](#) to your print account to get access.
- [Subscribe starting at 99¢](#) for the first month.
- [Whitelist denverpost.com](#) in your ad blocker.

99¢

FOR THE FIRST MONTH

SUBSCRIBE NOW

Already a print or replica subscriber? [Get access.](#)

Here's The Thing With Ad Blockers

We get it: Ads aren't what you're here for. But ads help us keep the lights on. So, add us to your ad blocker's whitelist or pay \$1 per week for an ad-free version of WIRED. Either way, you are supporting our journalism. We'd really appreciate it.

Sign Up

Already a member? [Log in](#)



We have noticed you are using an ad blocker

We rely on advertising to fund our award-winning journalism.

Please whitelist our website or subscribe to Independent Premium our new membership service which includes an advertising-free experience, exclusive content, events and more - for as little as 30p a day.

For help accessing our website, visit our [ad blocking](#) page.

Subscribe

Log in

It looks like you're using an ad-blocker!

Business Insider is an advertising supported site and we noticed you have ad-blocking enabled.

HERE ARE 2 WAYS YOU CAN KEEP READING

Turn off your ad-blocker.

DO IT NOW

Continue with BI PRIME for just \$1.

GET ACCESS NOW

TO READ THE FULL STORY, PLEASE [LOG IN](#), [SUBSCRIBE](#) OR WHITELIST.

LOOKS LIKE YOU'RE RUNNING AN AD BLOCKER

SUPPORT JOURNALISM IN COLORADO

To continue reading The Denver Post:

- [Log in to your print account](#) to get access.
- [Subscribe starting at 99¢](#) for the first month.
- [Whitelist denverpost.com](#) in your ad blocker.

99¢

FOR THE FIRST MONTH

SUBSCRIBE NOW

Already a print or replica subscriber? [Get access.](#)

Subscriptions

Pay a periodic fee in order to
access content without
advertisements



The New York Times

Gain unlimited access
to all of The Times.

WELCOME OFFER

~~\$6.25~~ \$1/week



Watch and listen ad-free, offline, and in
the background all year long

Subscriptions

Pay a periodic fee in order to access content without advertisements

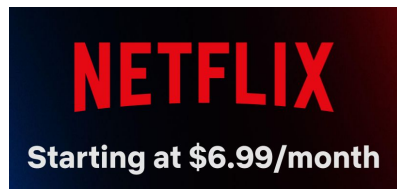


The New York Times

Gain unlimited access to all of The Times.

WELCOME OFFER

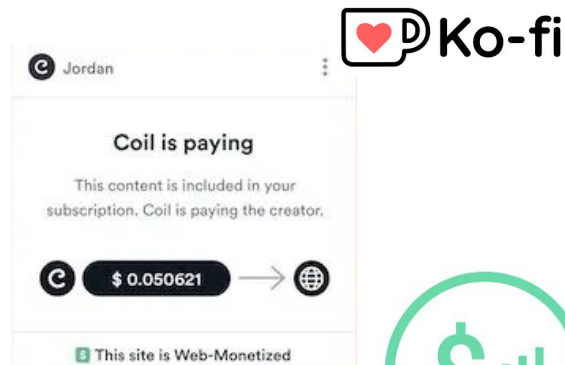
~~\$6.25~~ \$1/week



Watch and listen ad-free, offline, and in the background all year long

Web Monetization

Micropayments for on-demand content access



Subscriptions

Web Monetization



Pay money OR see ads

Meta

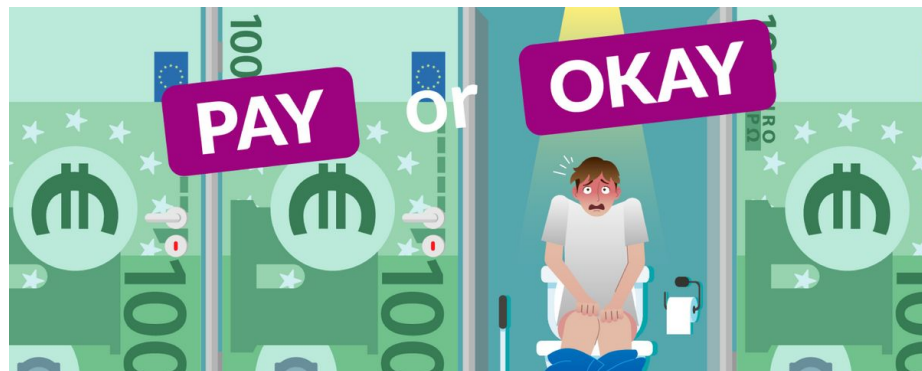
Facebook and Instagram to Offer Subscription for No Ads in Europe

November 12, 2024

[Home](#) > [News](#) >

"Pay or Okay": 1,500 € a year for your online privacy?

[Forced Consent & Consent Bypass](#) / 19 March 2024



Pay money or “consent” to use of personal data

Meta

Facebook and Instagram to Offer Subscription for ~~No Ads~~ in Europe

Privacy

November 12, 2024

Yes: Pay for ad-free experience

No: Pay for privacy

People have a right to privacy on the internet,
whether or not they can pay.

Advertising must be private.

Spoilers:

- 1) Advertising is inherently leaky. There is no 'perfect' solution for private advertising.

Spoilers:

- 1) Advertising is inherently leaky. There is no 'perfect' solution for private advertising.
- 2) Normative privacy $\neq$ information leakage. Whether leakage is 'acceptable' depends on context.

Spoilers:

- 1) Advertising is inherently leaky. There is no 'perfect' solution for private advertising.
- 2) Normative privacy $\neq$ information leakage. Whether leakage is 'acceptable' depends on context.
- 3) Privacy in advertising is about groups as much as individuals.



This talk is about the fundamental leakage inherent to advertising.

Not about the (way more than necessary) leakage in the current advertising ecosystem.

It's intended to guide future work and help avoid pitfalls.

Privacy for Advertising

Privacy as leakage:

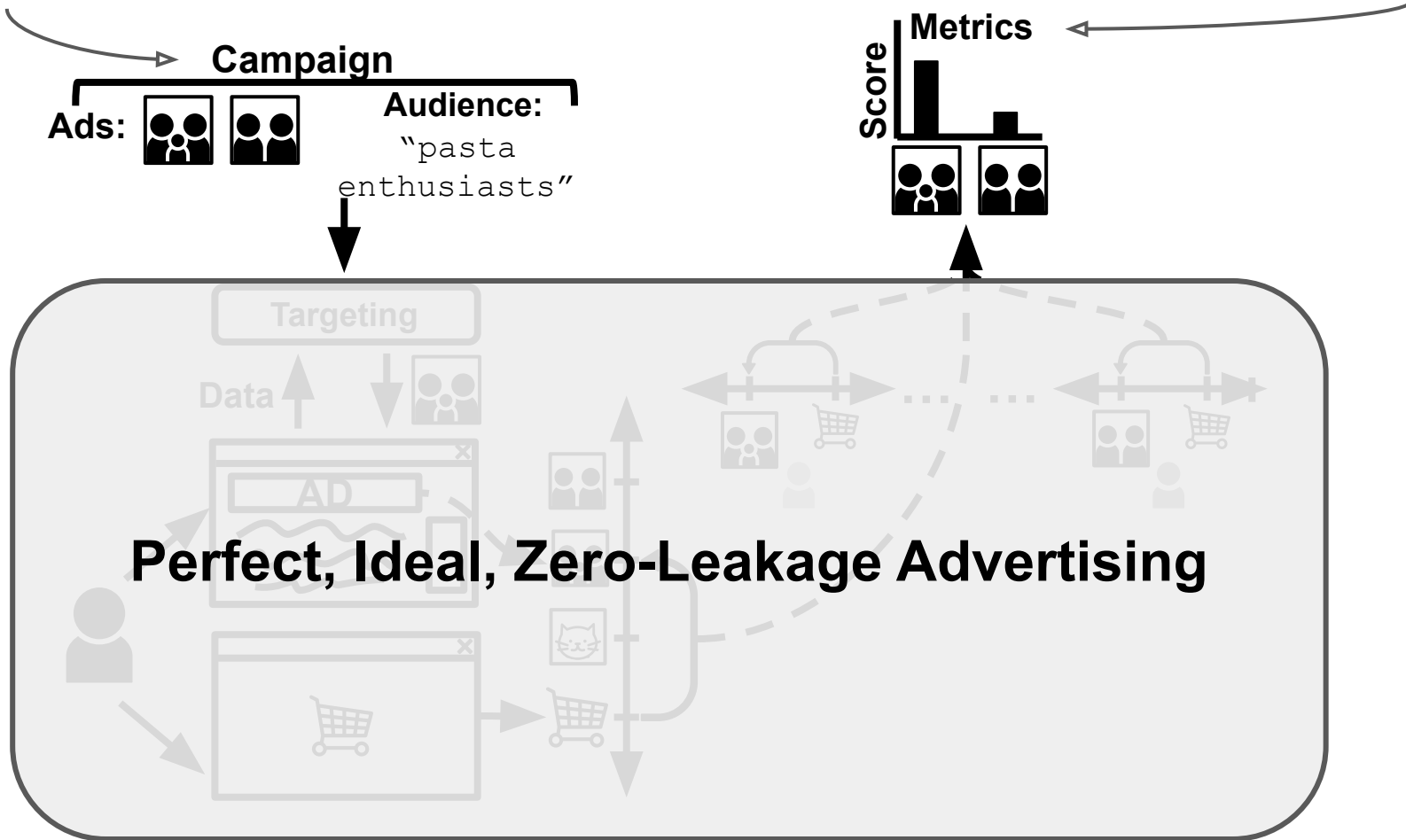
Some party learns **new information** about another party
as a result of their participation in the protocol.

Privacy as leakage:

Advertisers learn **new information** about **users** as a **result of their participation** in the protocol.

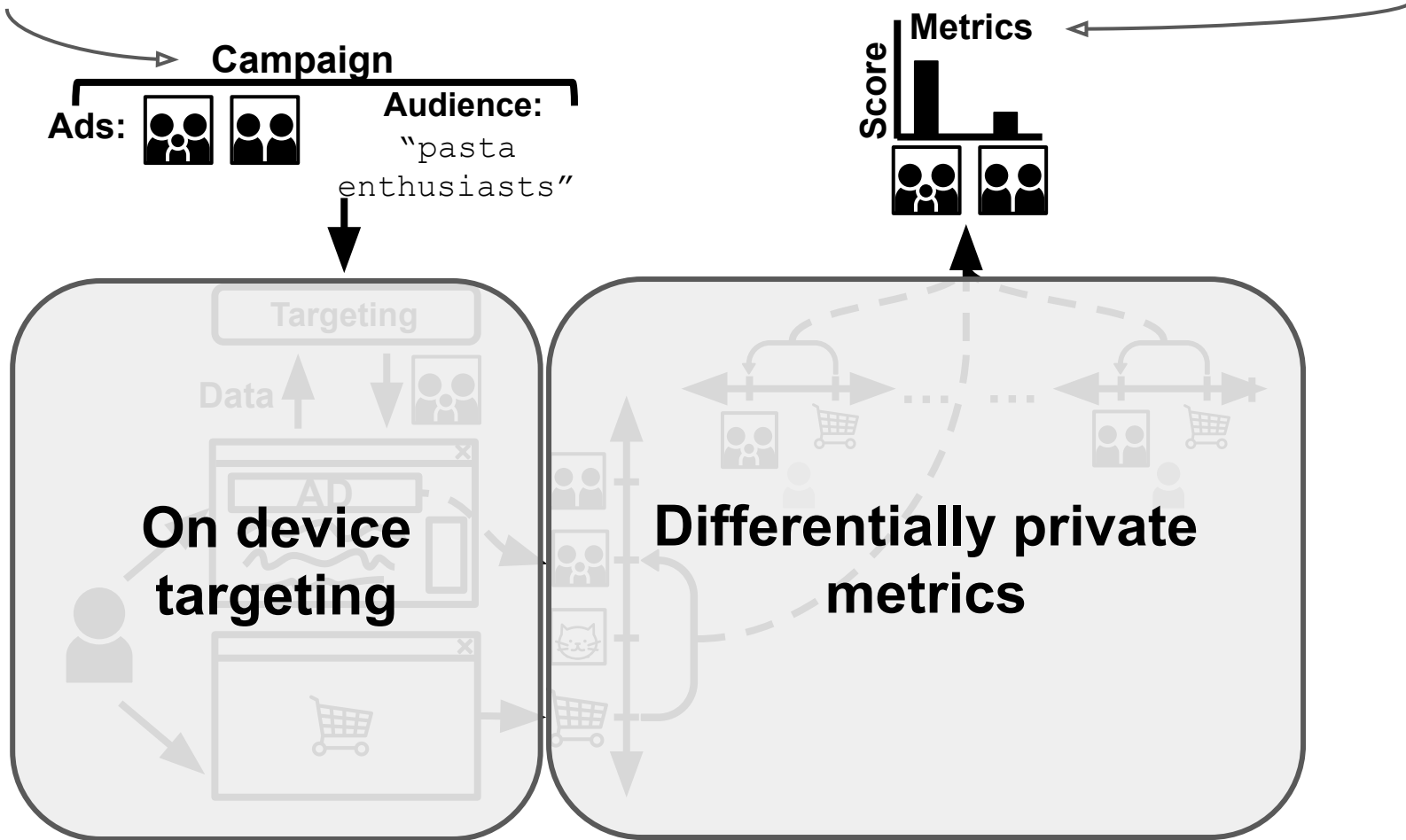
input

output



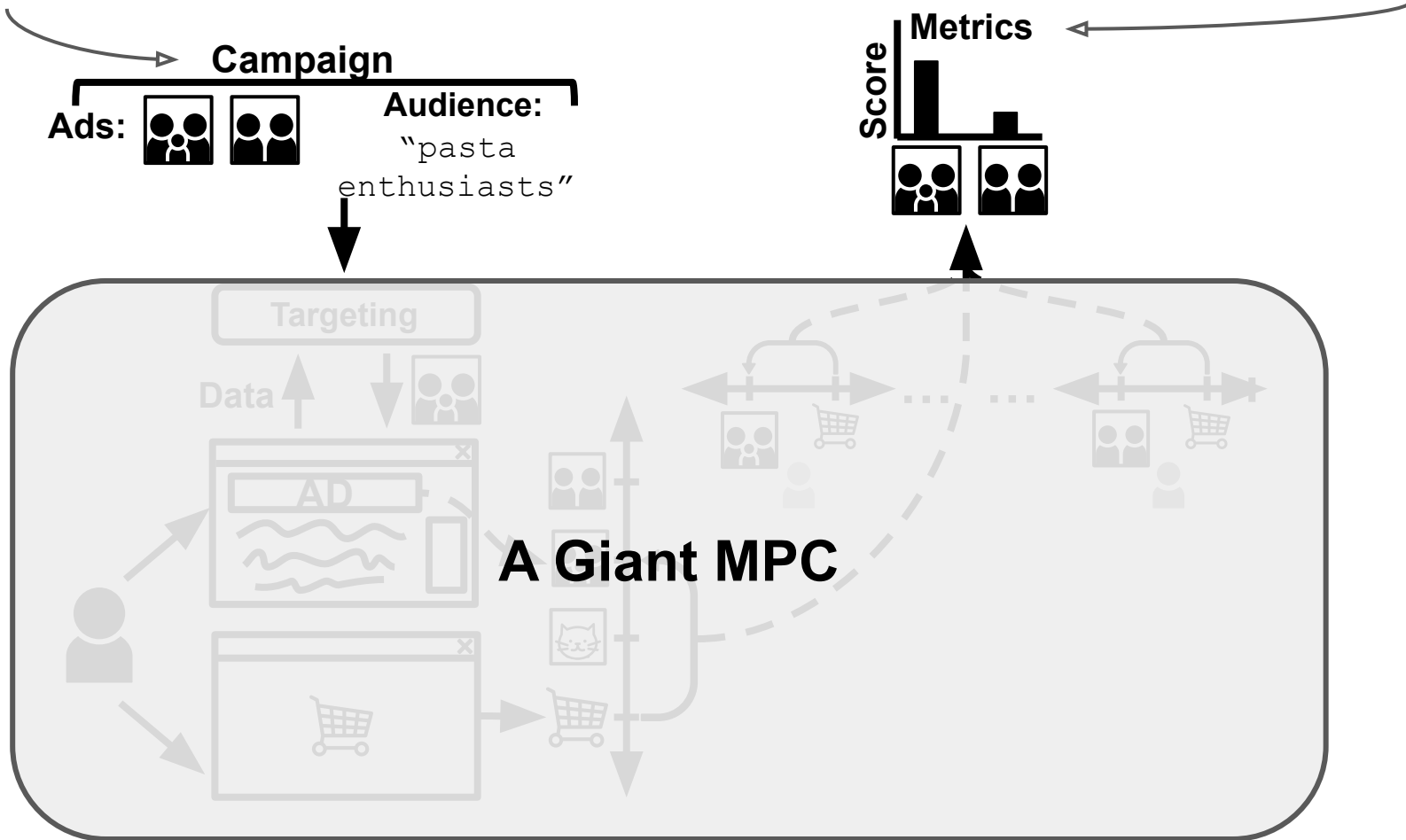
input

output

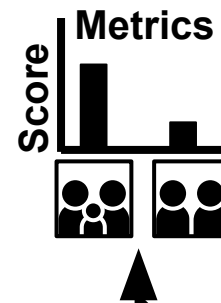
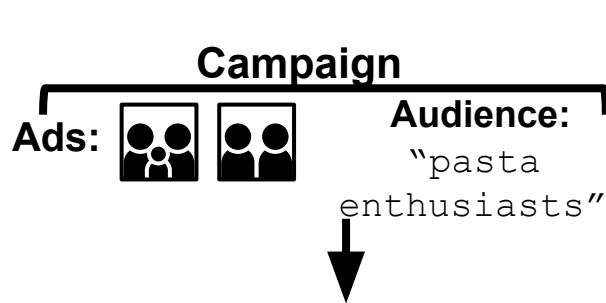


input

output



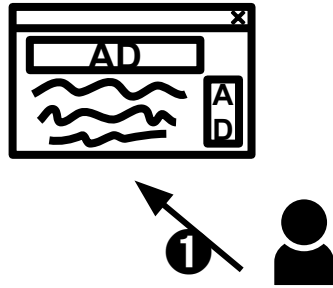
Advertiser

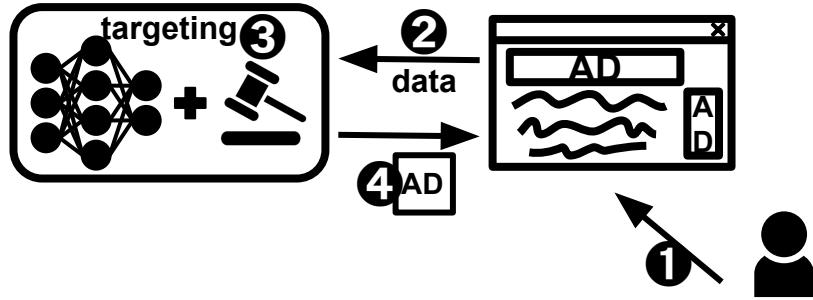


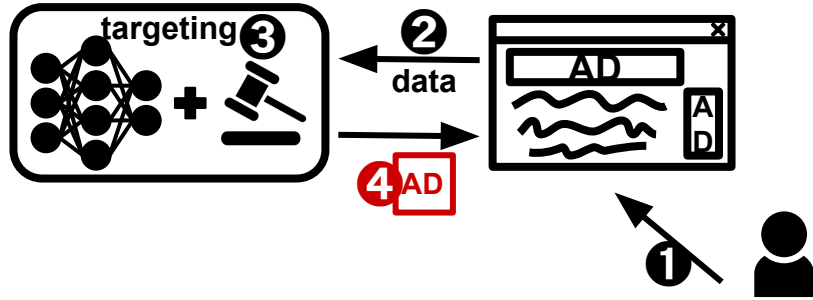
Ad
Network



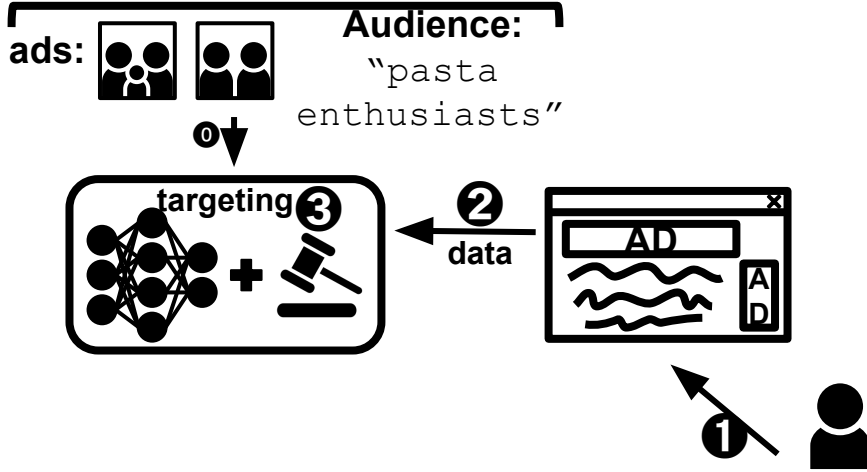
What *new information* can advertisers learn about users from metrics data on the advertiser's own campaigns?



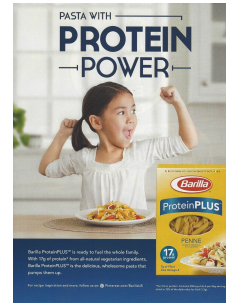


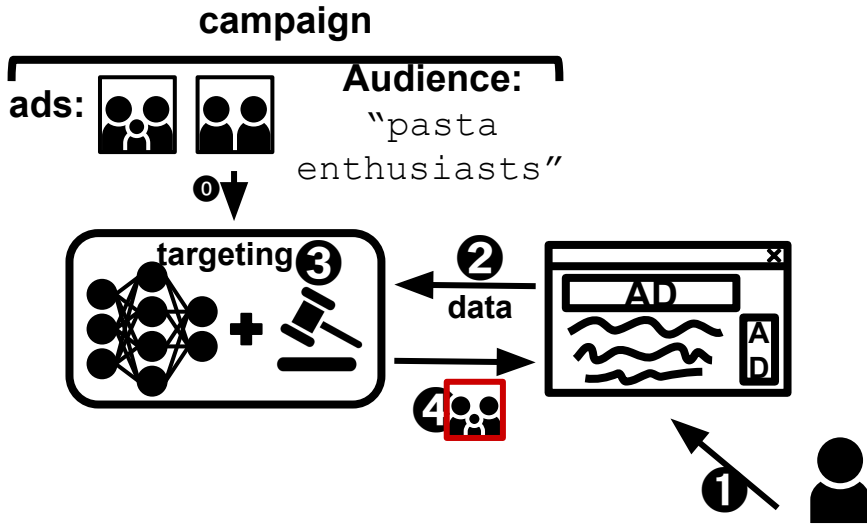


campaign



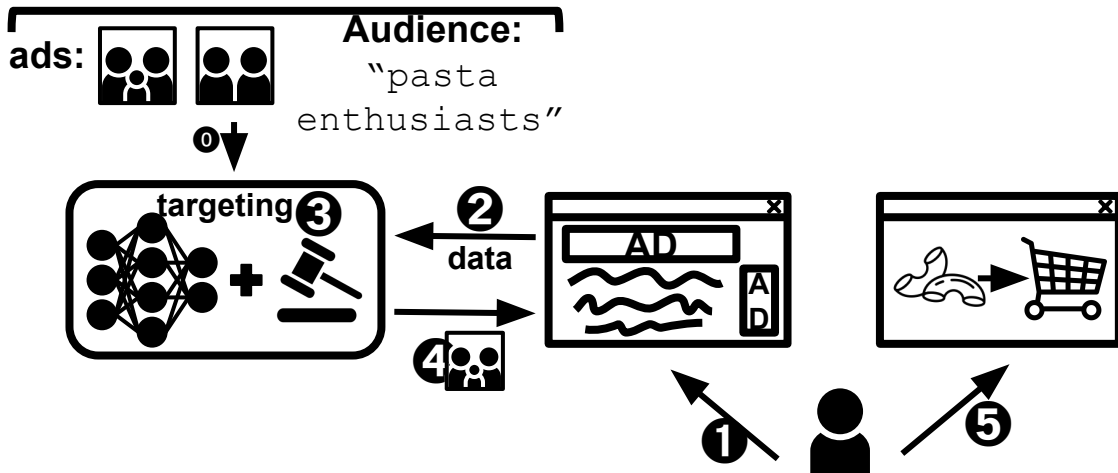
- ① The advertiser registers a campaign with the ad network. The campaign has both creatives (ads) and the audience (what kind of user to show them to)





③ Advertisers participate in a real-time auction and bid for the user and ad slot. ④ The winning ad is delivered to the user.

campaign



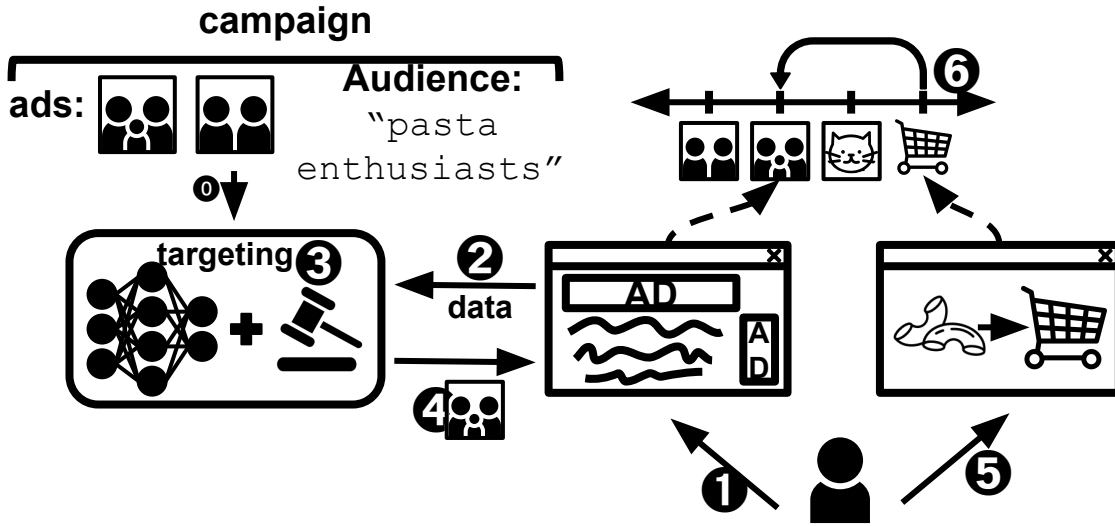
⑤ “conversions” aren’t just clicks.
 Maybe this pasta ad was so good that
 the user later goes and buys macaroni
 on a grocery delivery site.

instacart

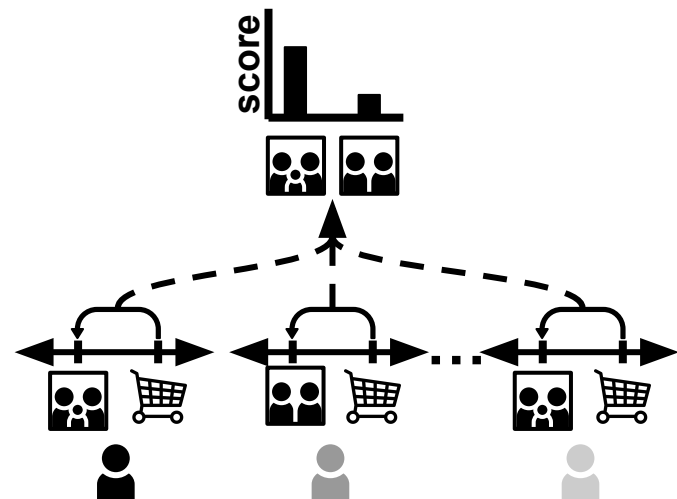
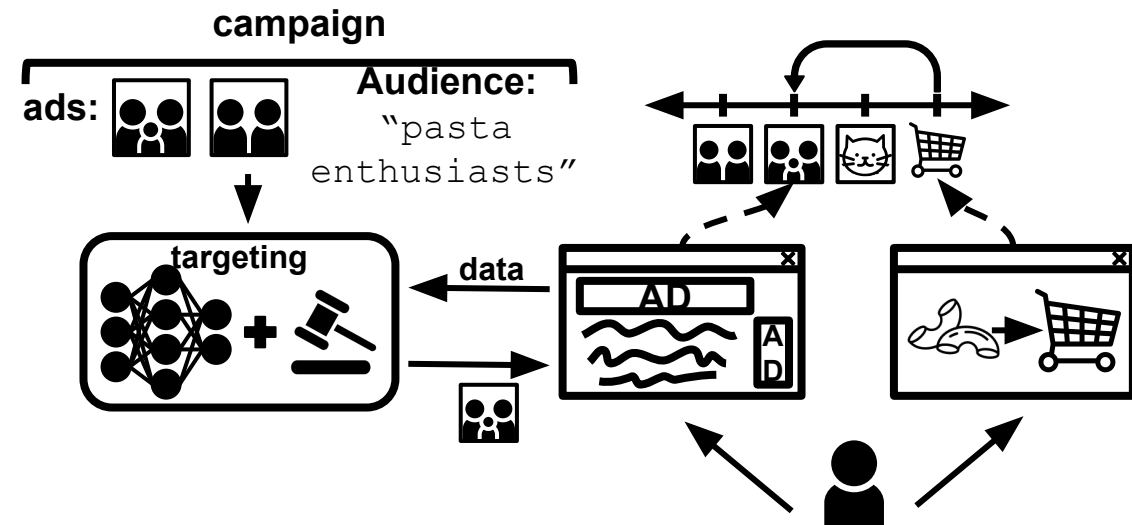
Q pasta

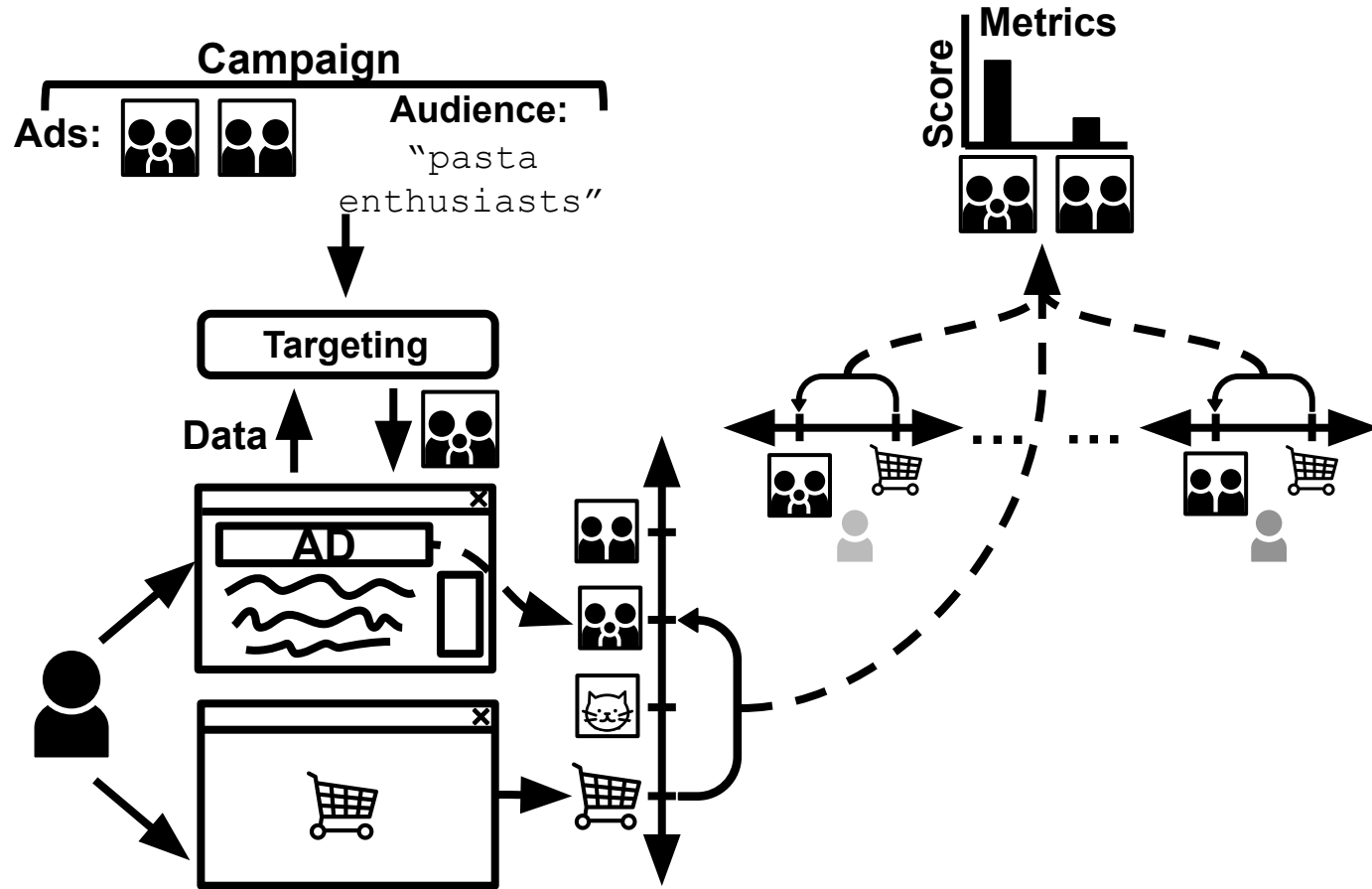
Shop Pasta for delivery or pickup





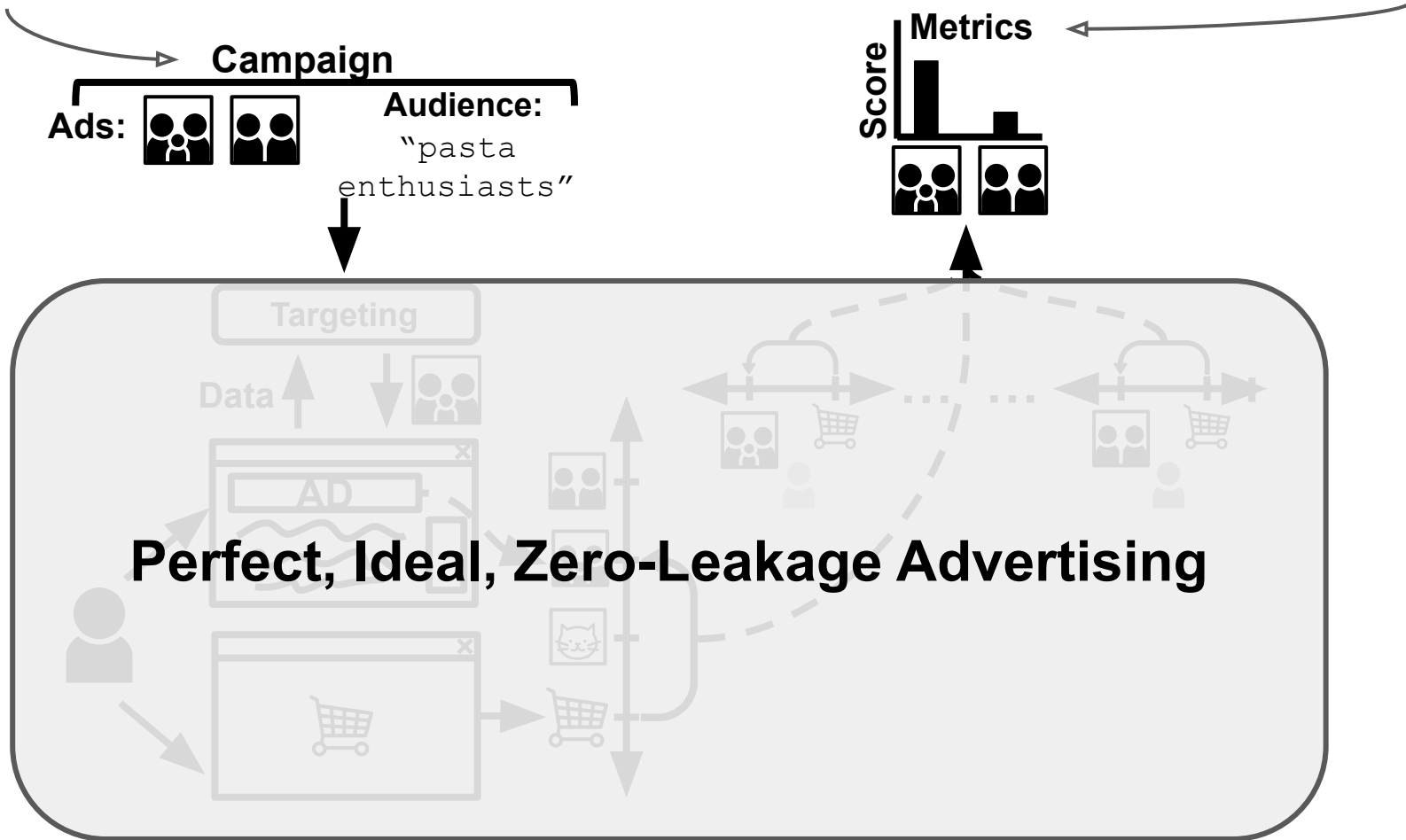
⑥ this purchase is “attributed” to the ad that was responsible. This can be “last touch” or the most recent (relevant) ad seen prior to the purchase

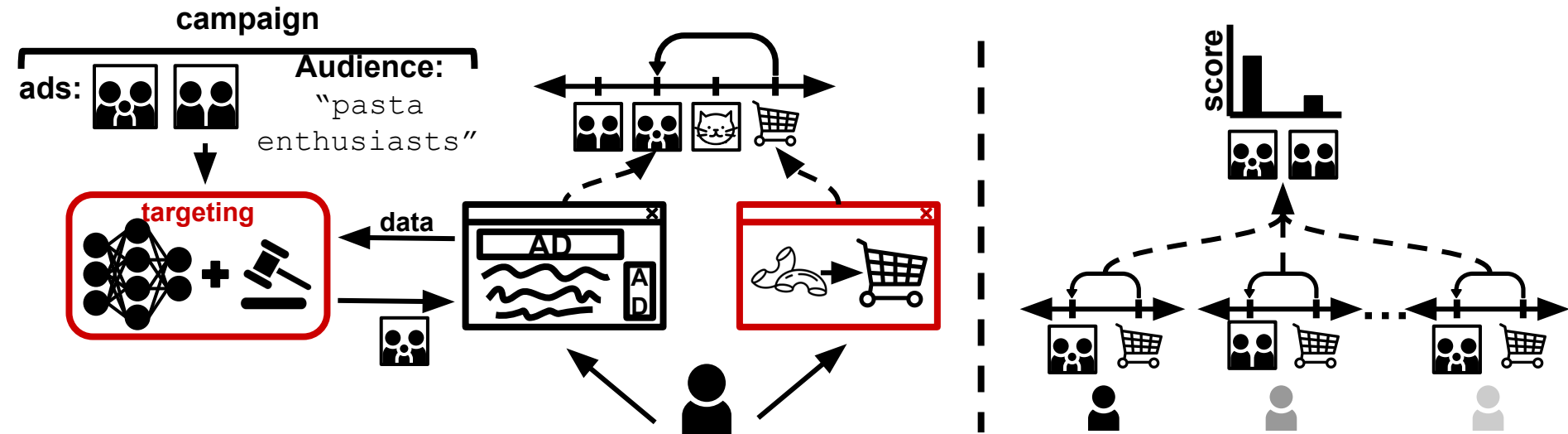




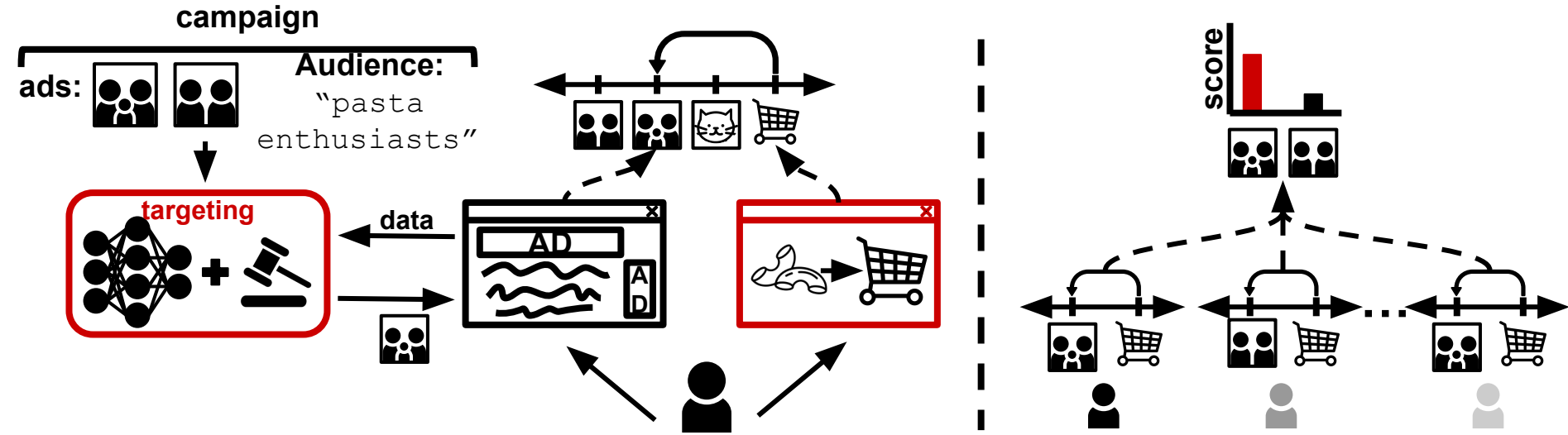
input

output





Information about users is embedded into metrics via **targeting** and **engagement**.



More conversions on the **kid-focused ad** implies that pasta enthusiasts are **typically parents**.

This is not “*no information*”

The advertiser was able to learn something new about their audience – their parental status.

Can we address this leakage?

Not perfectly.

Utility for Advertising Functionalities

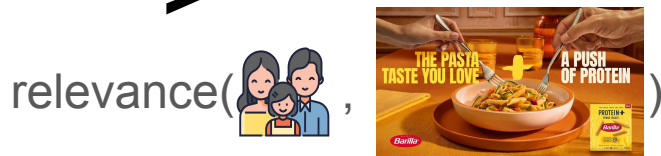
(for *any* ad ecosystem – private or otherwise)

Targeting Utility: Relevance

Targeting is useful if, for some internally consistent definition of “relevant”, it has a higher probability of outputting the ad that is more relevant to the user

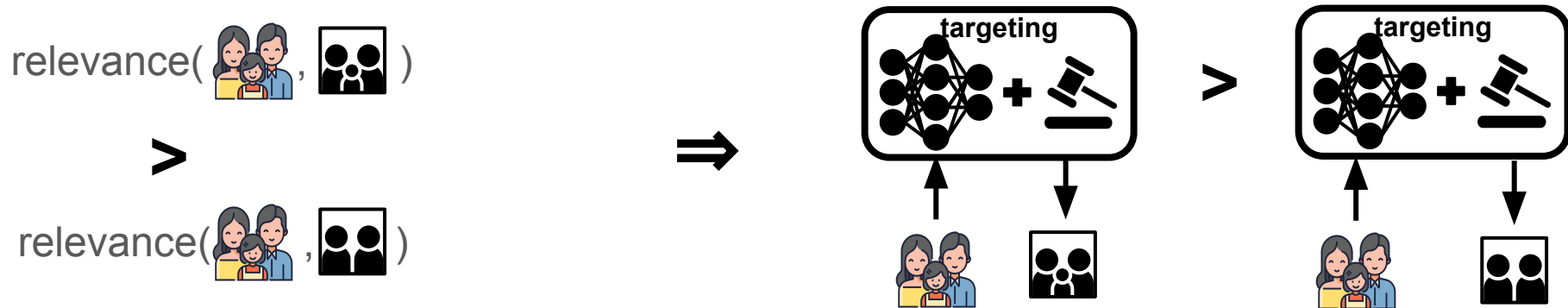


>

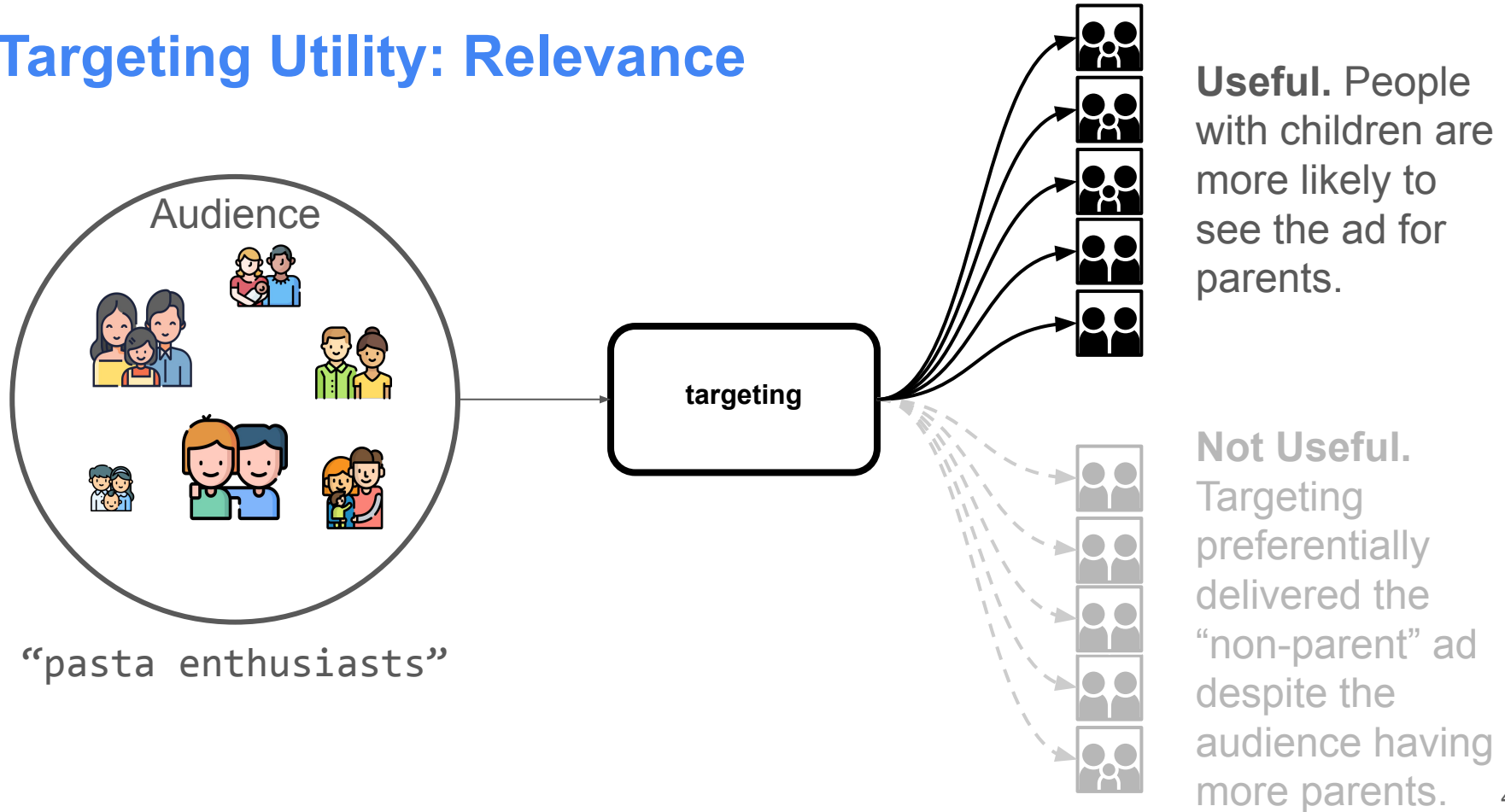


Targeting Utility: Relevance

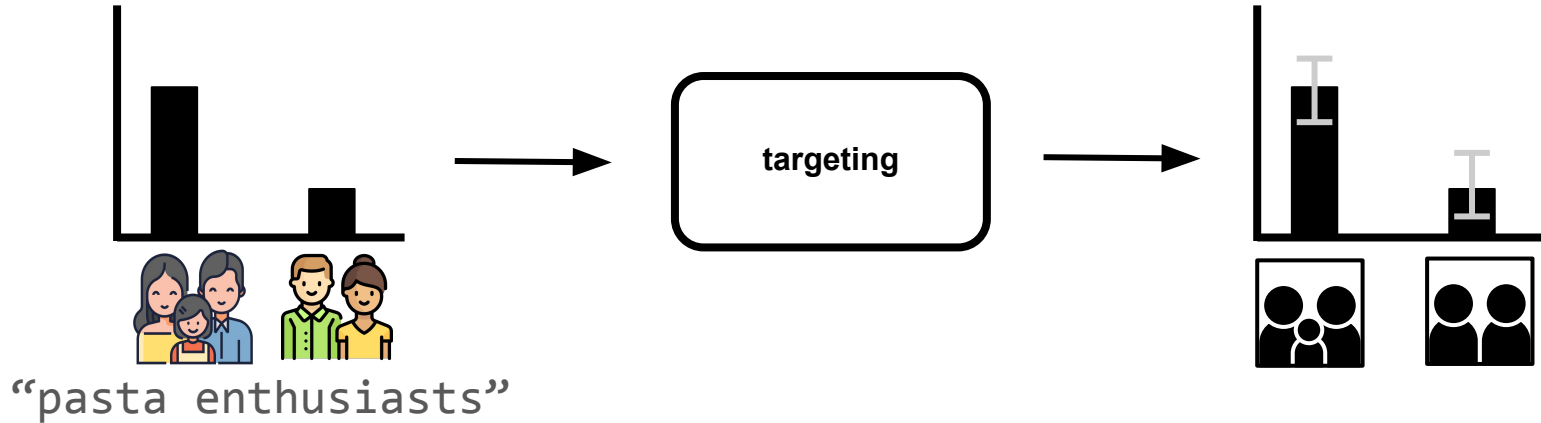
Targeting is useful if, for some internally consistent definition of “relevant”, it has a higher probability of outputting the ad that is more relevant to the user



Targeting Utility: Relevance

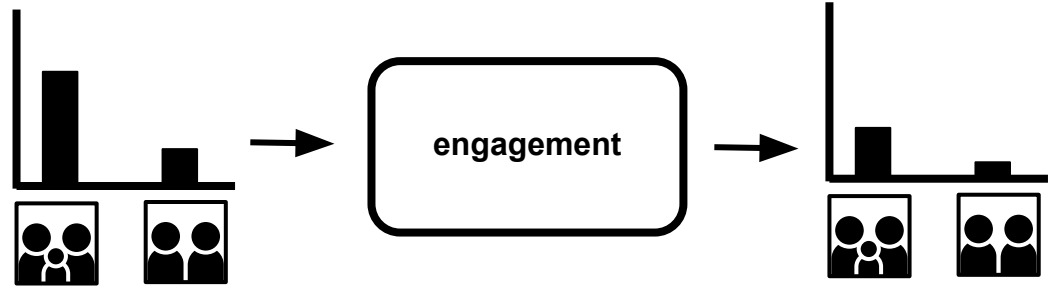


Targeting Utility Preserves Audience Distribution



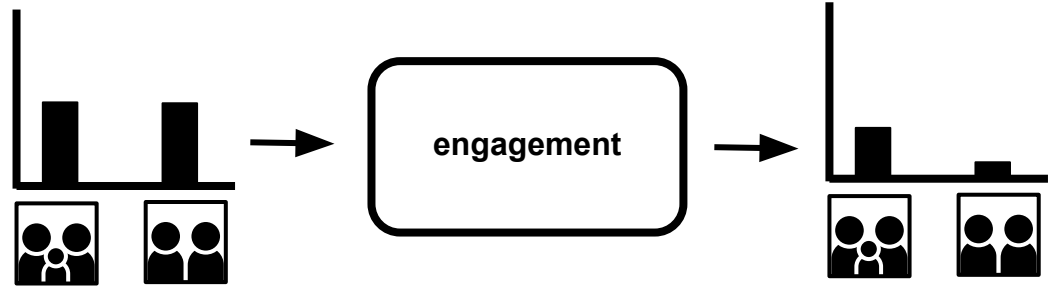
Engagement Boosts Targeting Utility

People are more likely to engage with ads that are relevant to them



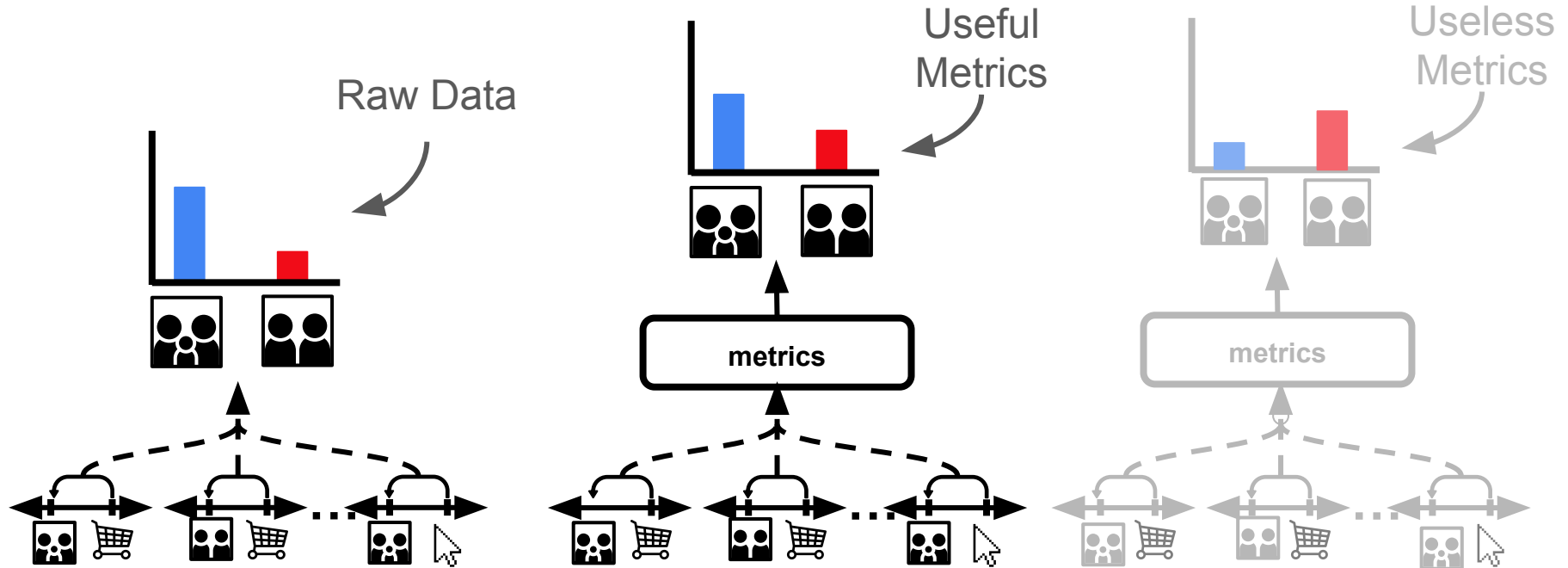
Engagement Boosts Targeting Utility

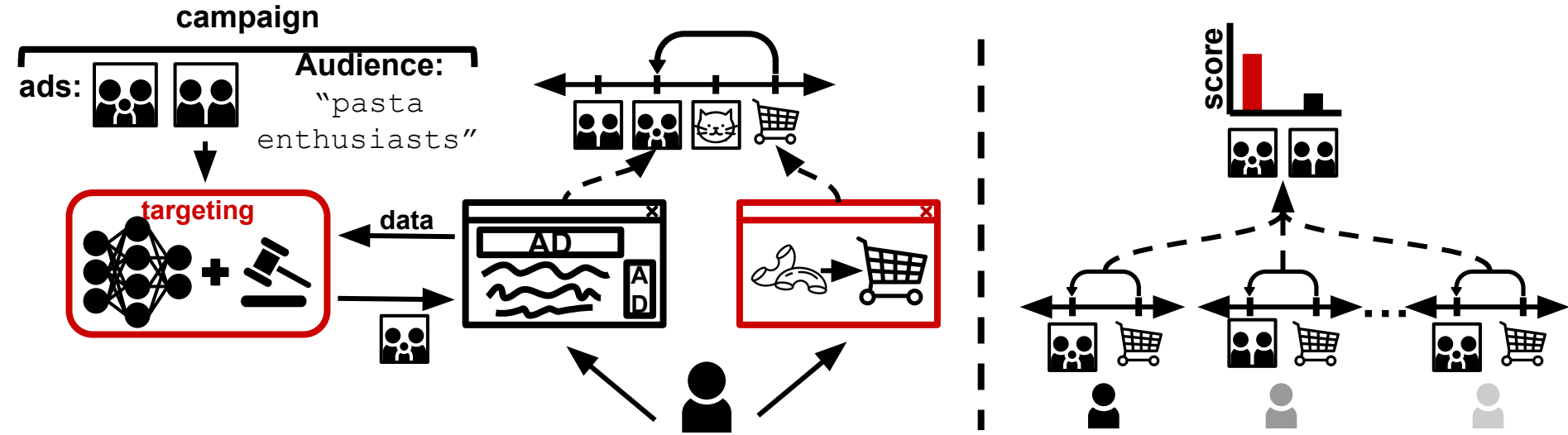
People are more likely to engage with ads that are relevant to them



Metrics Utility: Accuracy

The advertiser draws the same conclusion from some statistical test – like an A/B test – on the metrics output as on the raw data





Information about users is embedded into metrics via **targeting** and **engagement**.

While this information can be removed for **individual users***, removing it for the **audience** renders the metrics data useless.

Any *useful* ad ecosystem will have this kind of leakage.

Or, conversely, if you successfully privatize an ad ecosystem and eliminate this leakage... it also *doesn't function.*

Detour: Differentially Private Ad Metrics

Differential Privacy Intuition [Dwork 06]

Permits learning information about **populations**, but **not individuals**.

→ The output should be the same whether or not your data was included

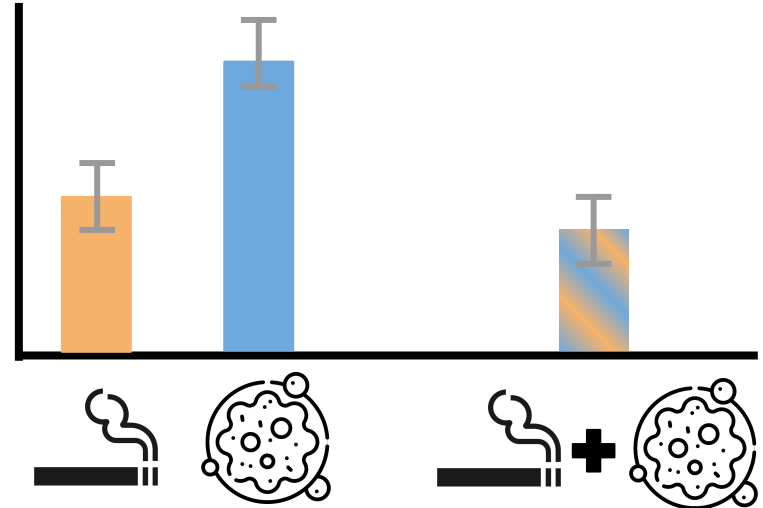
Differential Privacy Intuition

Permits learning information about **populations**, but not **individuals**.

→ The output should be the same whether or not your data was included

Standard example: Doctors conduct a study that reveals a correlation between smoking and cancer.

⌈ Noise: how much can **Alice's** data impact the result?



Differential Privacy Intuition

Holds when you have a **representative sample** whose **membership is unknown**.

Consider instead a non-representative sample with known membership: workplace satisfaction surveys!

Differential Privacy Intuition

Consider instead a non-representative sample with known membership: workplace satisfaction surveys!

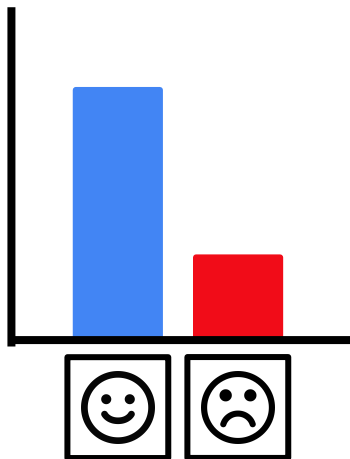
Please respond honestly. We value your feedback and all responses will be anonymous and differentially private. :)

Differential Privacy Intuition

Consider instead a non-representative sample with known membership: workplace satisfaction surveys!

Please respond honestly. We value your feedback and all responses will be anonymous and differentially private. :)

Company results:

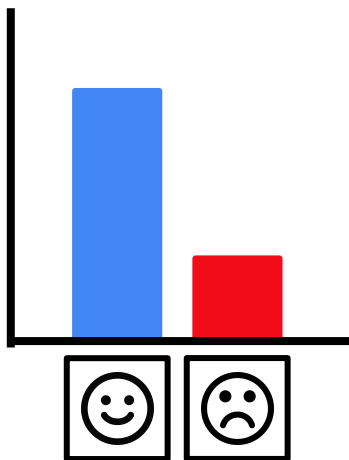


Differential Privacy Intuition

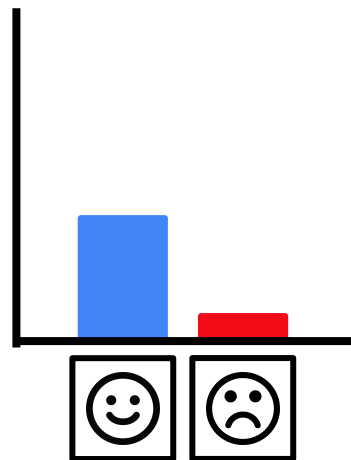
Consider instead a non-representative sample with known membership: workplace satisfaction surveys!

Please respond honestly. We value your feedback and all responses will be anonymous and differentially private. :)

Company results:



Your team:

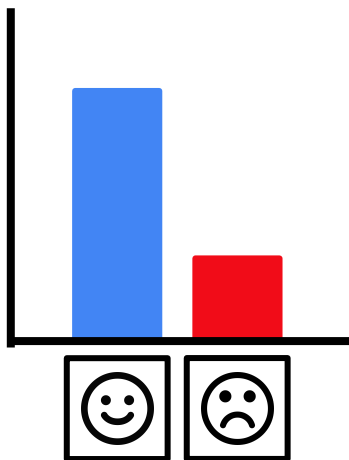


Differential Privacy Intuition

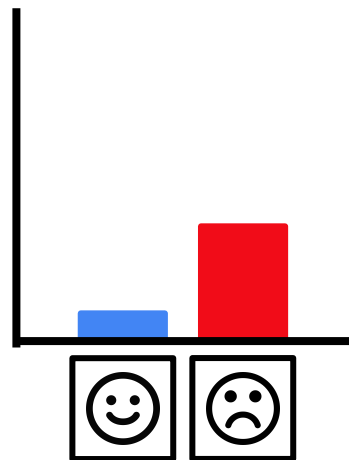
Consider instead a non-representative sample with known membership: workplace satisfaction surveys!

Please respond honestly. We value your feedback and all responses will be anonymous and differentially private. :)

Company results:



Your team:

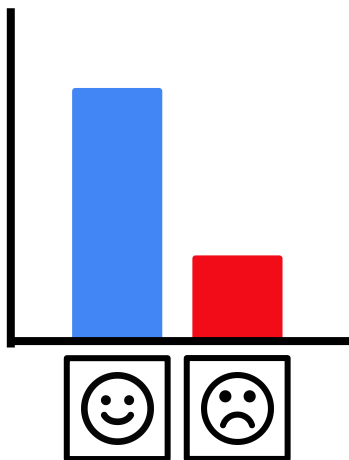


Differential Privacy Intuition

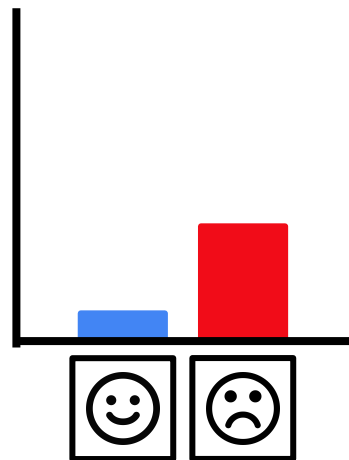
Your team was non-representative. While *your individual* participation did not impact the results, the participation of your team *as a group* allowed collective statistics:

The company's expectation about *your individual* happiness has changed as a result of this survey.

Company results:



Your team:



Advertising audiences are ***not representative*** of the general population and can be composed of people whose identity is ***known to the advertiser***.

Differential privacy is ***agnostic to the audience composition***.

It's a, likely necessary, component of privatizing advertising,
but is insufficient on its own.

There is interplay between privacy for ad targeting and privacy
for ad metrics that has been addressed in ad network policies,
but ***not with any technical enforcement*** or
auditability/accountability.

The Case for Normative Privacy

or, some leakage is fine actually.

Contextual Integrity [Nissenbaum 04]

Contextual integrity is a framework for reasoning about whether learning is *appropriate for the context*

For example, conducting a study on the relationship between smoking and cancer is perfectly appropriate in a medical setting, but not in advertising.

How people feel about ad targeting hinges on *what kind* of information is revealed about them.

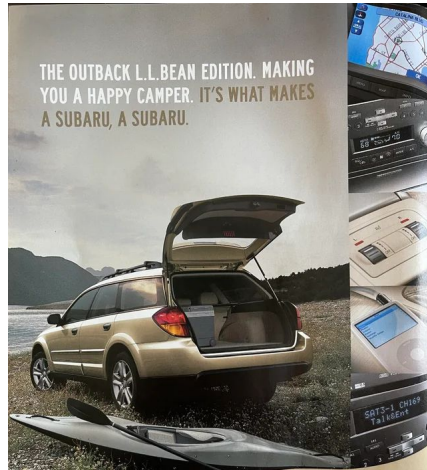
Case 1: 90's Subaru

Subaru is struggling to sell cars in the US. They already know that their cars are a favorite of outdoorsy types and decide to do some market research to focus in on people most likely to buy.

Audience: outdoorsy types

Content: cars & nature

Focus feature:



Different Drivers. Different Roads.
One Car.

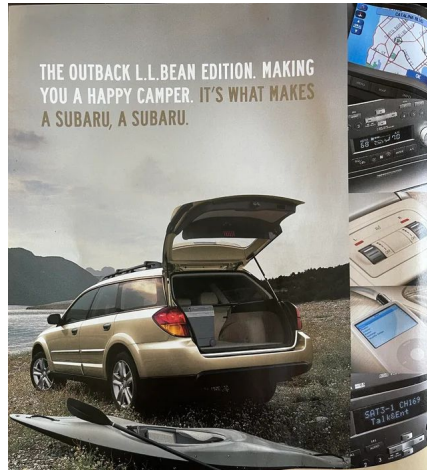
Case 1: 90's Subaru

Subaru is struggling to sell cars in the US. They already know that their cars are a favorite of outdoorsy types and decide to do some market research to focus in on people most likely to buy.

Audience: outdoorsy types

Content: cars & nature

Focus feature: **sexuality**



Different Drivers. Different Roads.
One Car.

Case 2: Post-workout Snacking

A smoothie shop wants to focus their ad spend. They show a variety of ads for different gym activities and learn via metrics that most of their customers are coming from gymnastics.

Audience: gym-going smoothie lovers

Content: smoothies & exercise

Focus feature: gym class



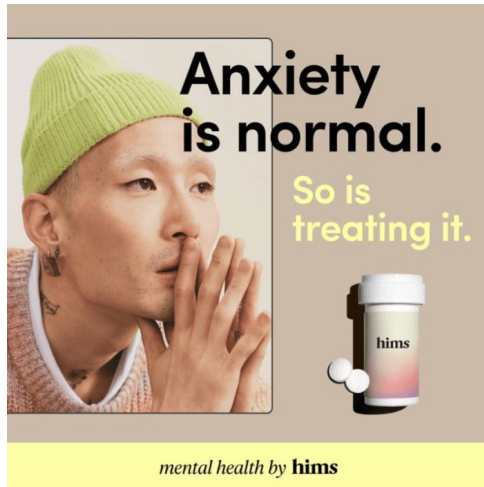
Case 3: Hims

Hims is an online retailer for prescription medication focusing on... personal hardship. They're known for their effective marketing strategies and hire people with expertise in A/B testing.

Audience: people with stigmatized medical issues

Content: health & self image

Focus feature: mental state



Case 3: Hims

Hims is an online retailer for prescription medication focusing on... personal hardship. They're known for their effective marketing strategies and hire people with expertise in A/B testing.

Audience: people with stigmatized medical issues

Content: health & self image

Focus feature: aesthetic

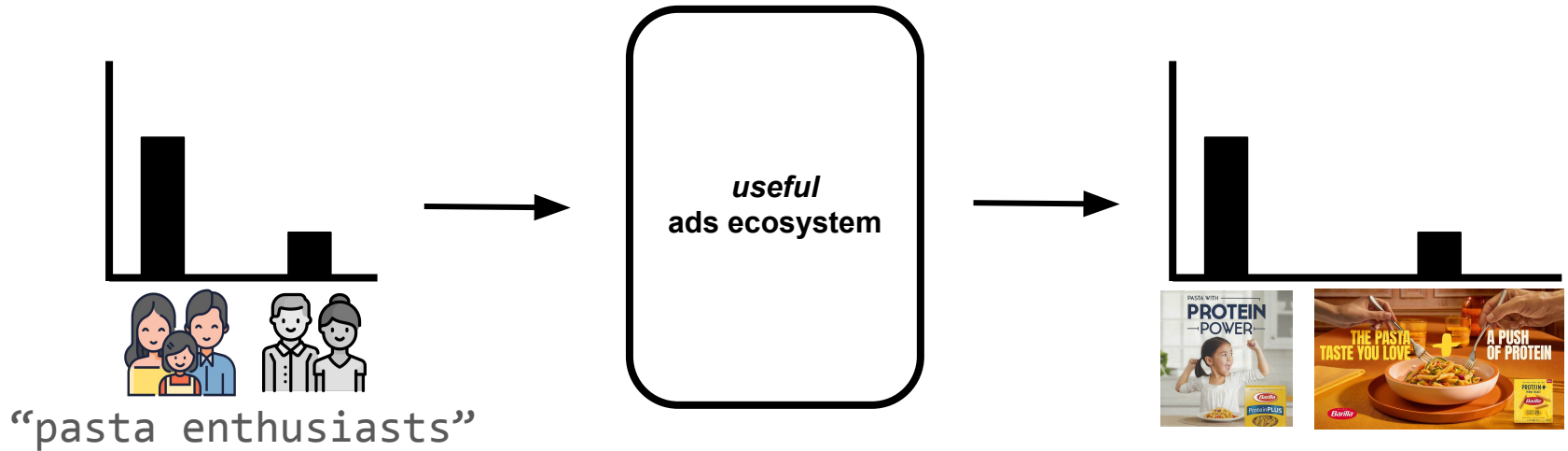


Information leakage from market research is problematic when that information is *sensitive*.

This can be the case when the ads feature sensitive *content* or are targeted to a sensitive *audience*.

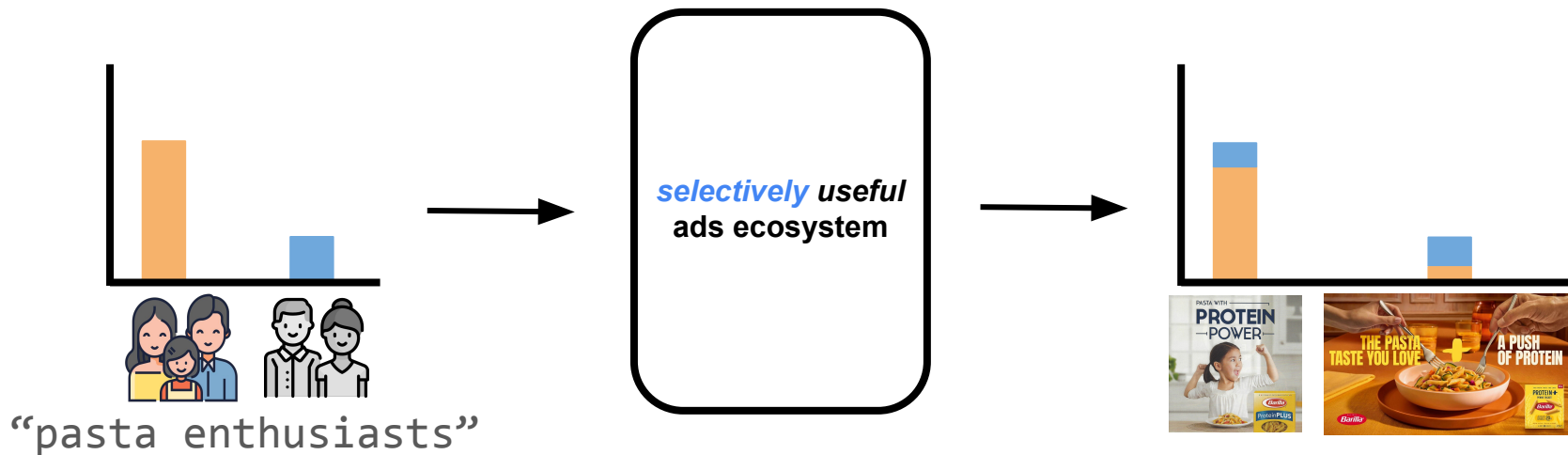
Future Directions: Enforcing Normative Privacy

Alternative Privacy Definitions: Attribute Privacy [ZOC21]



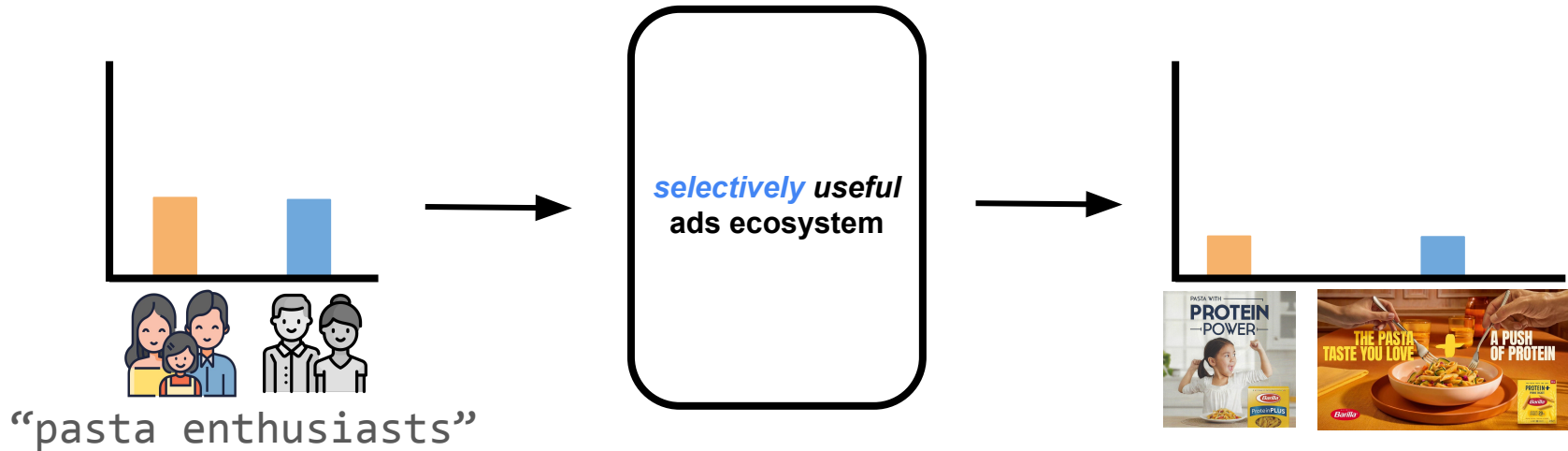
Is learning parental status *appropriate* in the context of *this specific* ad campaign?

Alternative Privacy Definitions: Attribute Privacy



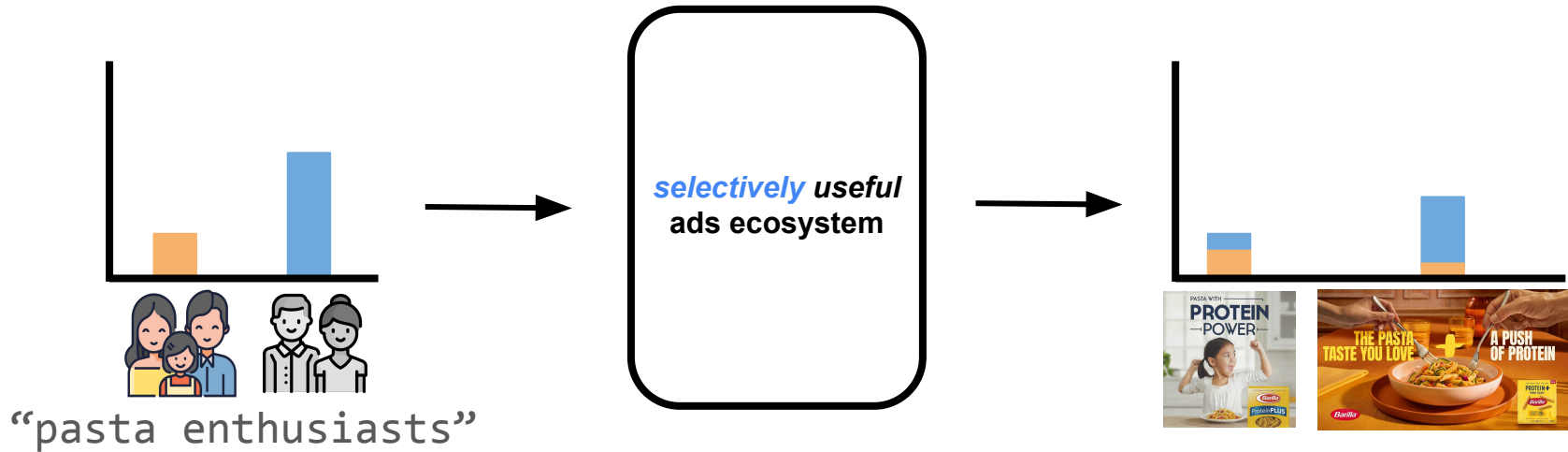
Noise in attribute privacy is relative to how much the *distribution* of the sensitive attribute impacts the output.

Alternative Privacy Definitions: Attribute Privacy



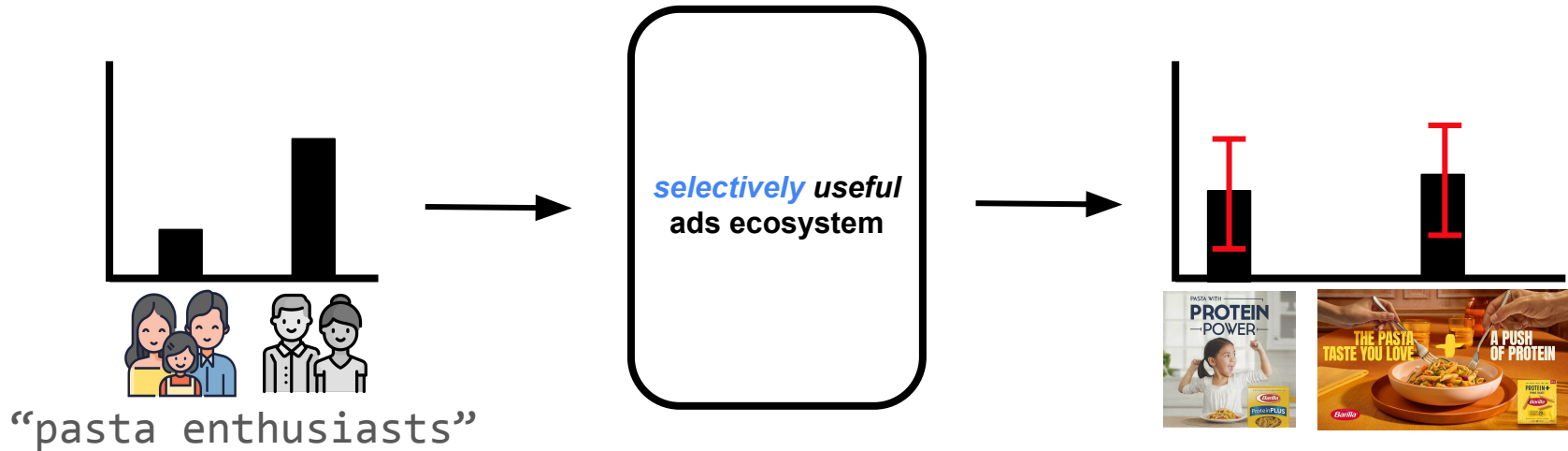
Noise in attribute privacy is relative to how much the *distribution* of the sensitive attribute impacts the output.

Alternative Privacy Definitions: Attribute Privacy



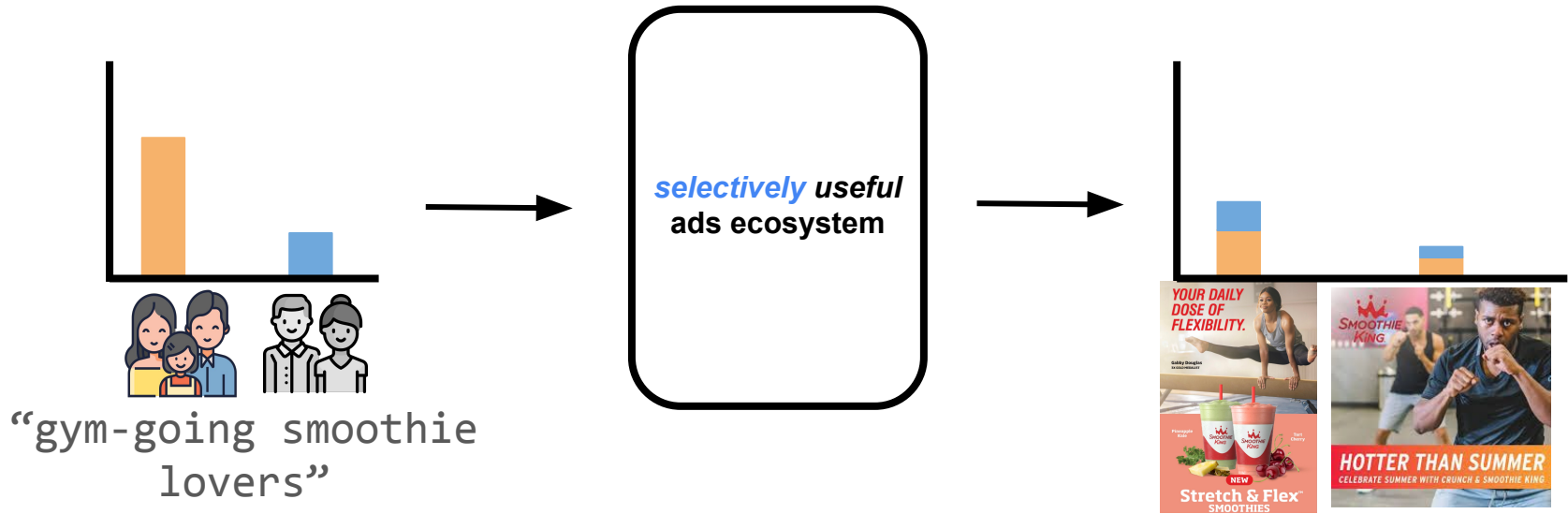
Noise in attribute privacy is relative to how much the *distribution* of the sensitive attribute impacts the output.

Alternative Privacy Definitions: Attribute Privacy



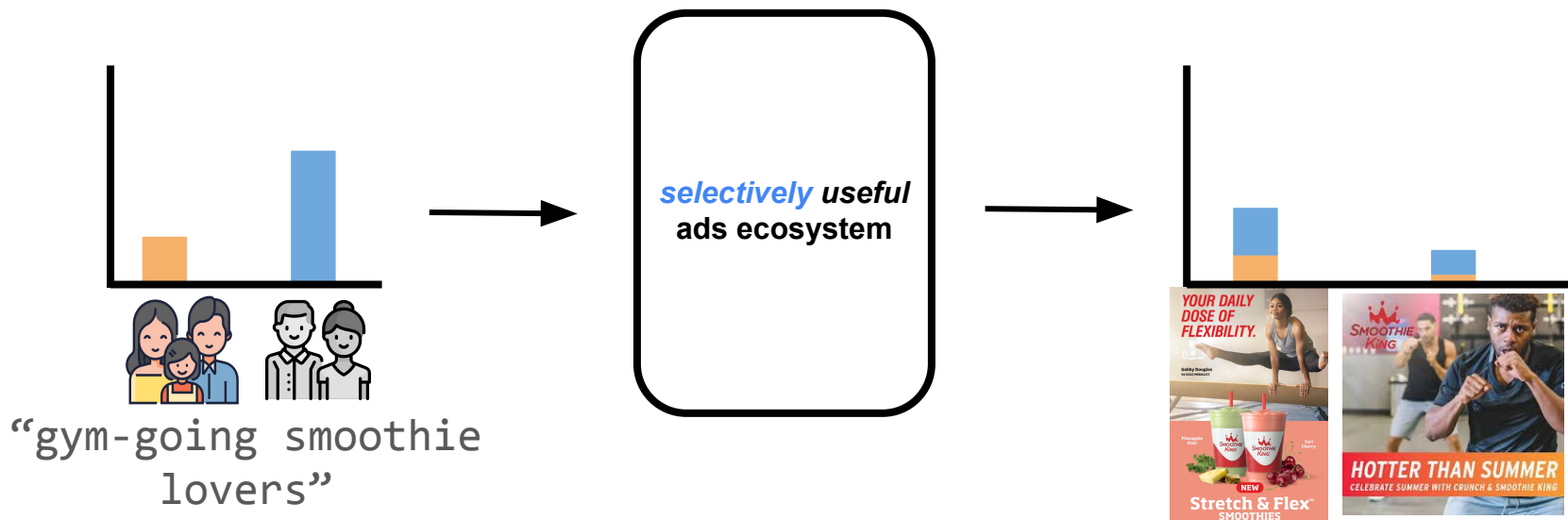
Noise is added to make the output independent of the distribution of the sensitive attribute. If there is a dependence, this is *a lot* and the output will no longer be useful.

Alternative Privacy Definitions: Attribute Privacy



However, if the output does **not** depend on a sensitive attribute, **no noise** is required.

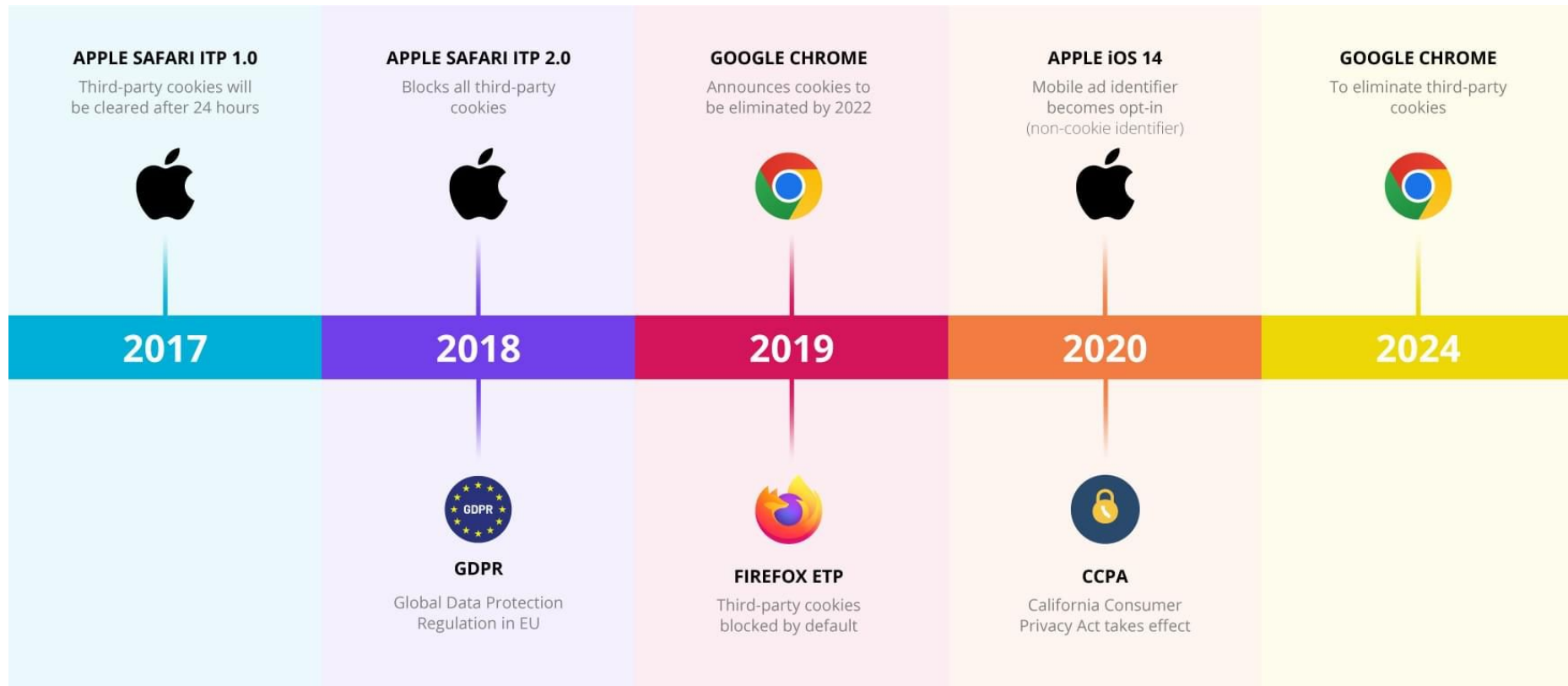
Alternative Privacy Definitions: Attribute Privacy



However, if the output does **not** depend on a sensitive attribute, **no noise** is required.

Future work in private advertising should emphasize
transparently enforcing normative privacy

Where are we now?





**Hating
Privacy Sandbox**

**Privacy
Advocates**

Advertisers

Privacy Advocates



[News](#) [Our work](#) [Exercise your rights!](#) [Support us!](#)



[LATEST](#) [TECH](#) [FOOD](#) [ENTERTAINMENT](#) [HEALTH](#) [HOME & GARDEN](#) [DEALS](#)

[Home](#) → [Tech](#) → [Privacy](#)

How to Disable Google Chrome's New 'Privacy Sandbox' Tracking (and Why You Want To)

Despite the name, "Privacy Sandbox" lets Google and other companies track and sell user data.

[Brendan Hesse](#) [July 13, 2021](#) [11 Comments](#)



Don't Play in Google's Privacy Sandbox

BY [BENNETT CYPHERS](#) | [AUGUST 30, 2019](#)

[Home](#) > [News](#) >

Google Chrome: Agree to 'privacy feature', but get tracking!

[Forced Consent & Consent Bypass](#) / [13 June 2024](#)



[SECURITY](#) [POLITICS](#) [THE BIG STORY](#) [BUSINESS](#) [SCIENCE](#) [CULTURE](#)

[GILAD EDELMAN](#)

[BUSINESS](#) [MAR 18, 2021 1:17 PM](#)

Google and the Age of Privacy Theater

The demise of surveillance capitalism has been greatly exaggerated.

Advertisers

 Reuters

World ▾ Business ▾ Markets ▾ Sustainability ▾ Legal ▾ Commentary ▾ Technology ▾ Investigations ▾ More ▾

Google's Privacy Sandbox adoption costs burden small ad-tech firms, industry says

By Akash Sriram and Harshita Mary Varghese

September 18, 2024 12:19 PM EDT · Updated September 18, 2024



LIFE BEYOND THE COOKIE

After months of testing, Google faces growing pressure to revamp the Privacy Sandbox

Six months after Google began phasing out third-party cookies in Chrome, the verdict on its alternatives is unchanged: they're a financial wrecking ball for publishers and another lever for Google's advertising dominance. The difference? There's now even more proof to back it up.

Digital Marketing Firms Hate Google's Anti-Cookie Initiative

Digital marketers have banded together to oppose Google's new Privacy Sandbox initiative. Which group's right? Tough call.



Written by
Adam Rowe

Published on
 **November 23, 2020**

CHROME PRIVACY SANDBOX

IAB Tech Lab Says The Chrome Privacy Sandbox Is A Time Bomb That Will Break Real-Time Bidding

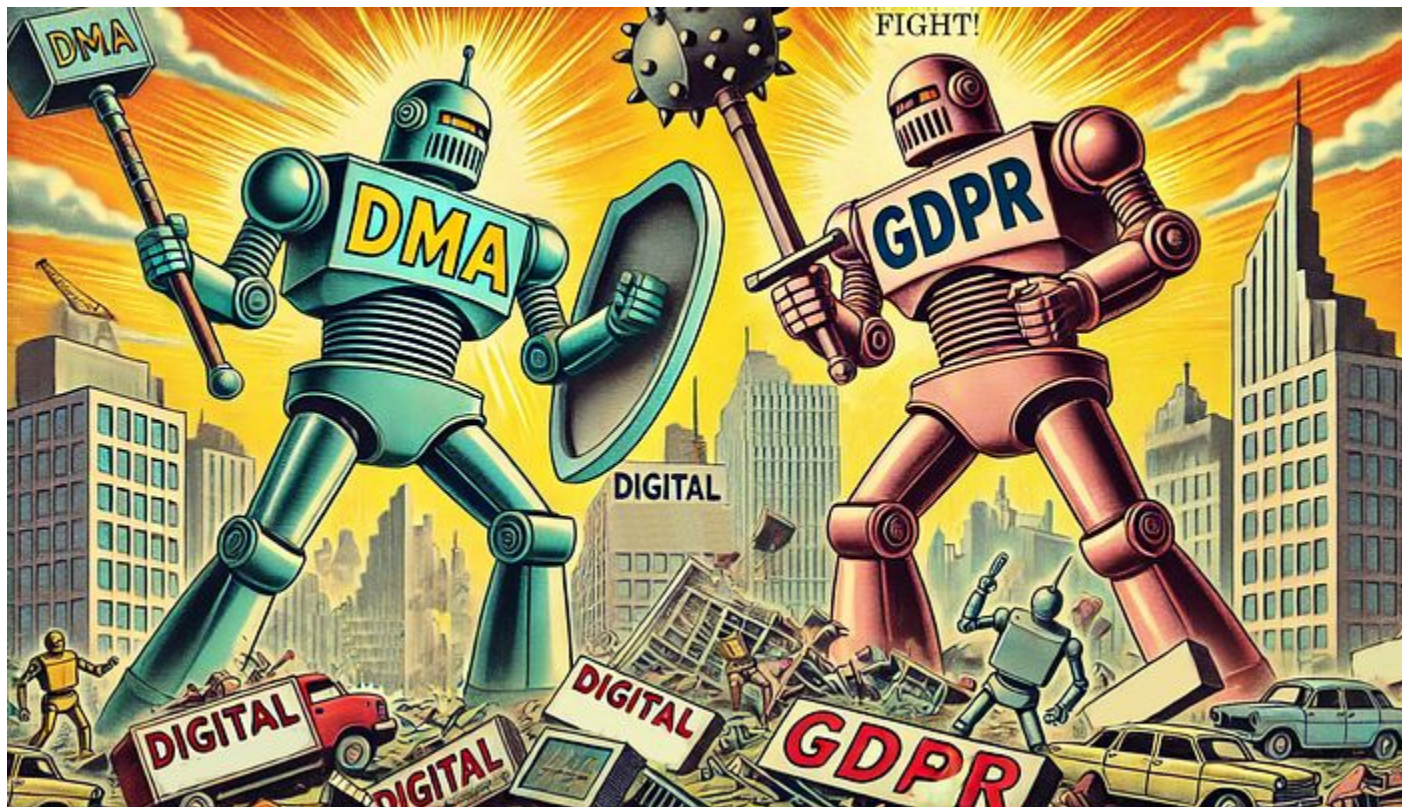


Harrison Schiff

RY 6TH, 2024 - 9:00 AM

SHARE:     

RIBE |

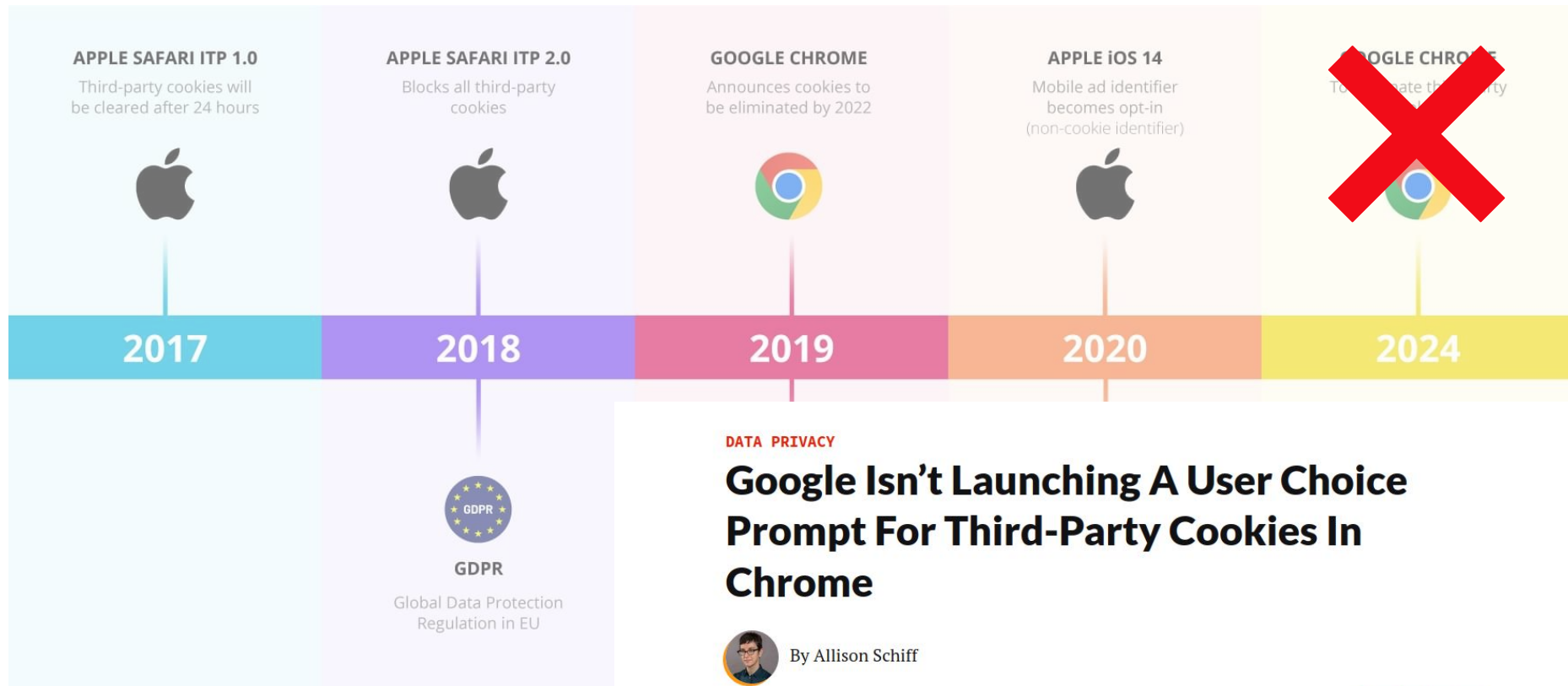


Source: ChatGPT / Kay Jebelli



Ad Tech Briefing: Has Google sacrificed Privacy Sandbox on the altar of antitrust concerns?

By [Digiday Editors](#) • April 25, 2025 •    



DATA PRIVACY

Google Isn't Launching A User Choice Prompt For Third-Party Cookies In Chrome



By Allison Schiff

TUESDAY, APRIL 22ND, 2025 - 12:15 PM

SHARE: [in](#) [en](#) [x](#) [g](#) [+](#)

ADWEEK

AD TECH INDUSTRY NEWS

The Winners and Losers of Google's Big Cookie Reversal

ID providers and open web publishers rejoice—while Privacy Sandbox investors and **privacy advocates nurse their wounds**

APRIL 24, 2025

**Was privacy sandbox our perfect, ideal,
zero-leakage advertising protocol? No.**

Was it better than third-party cookies? Yes.

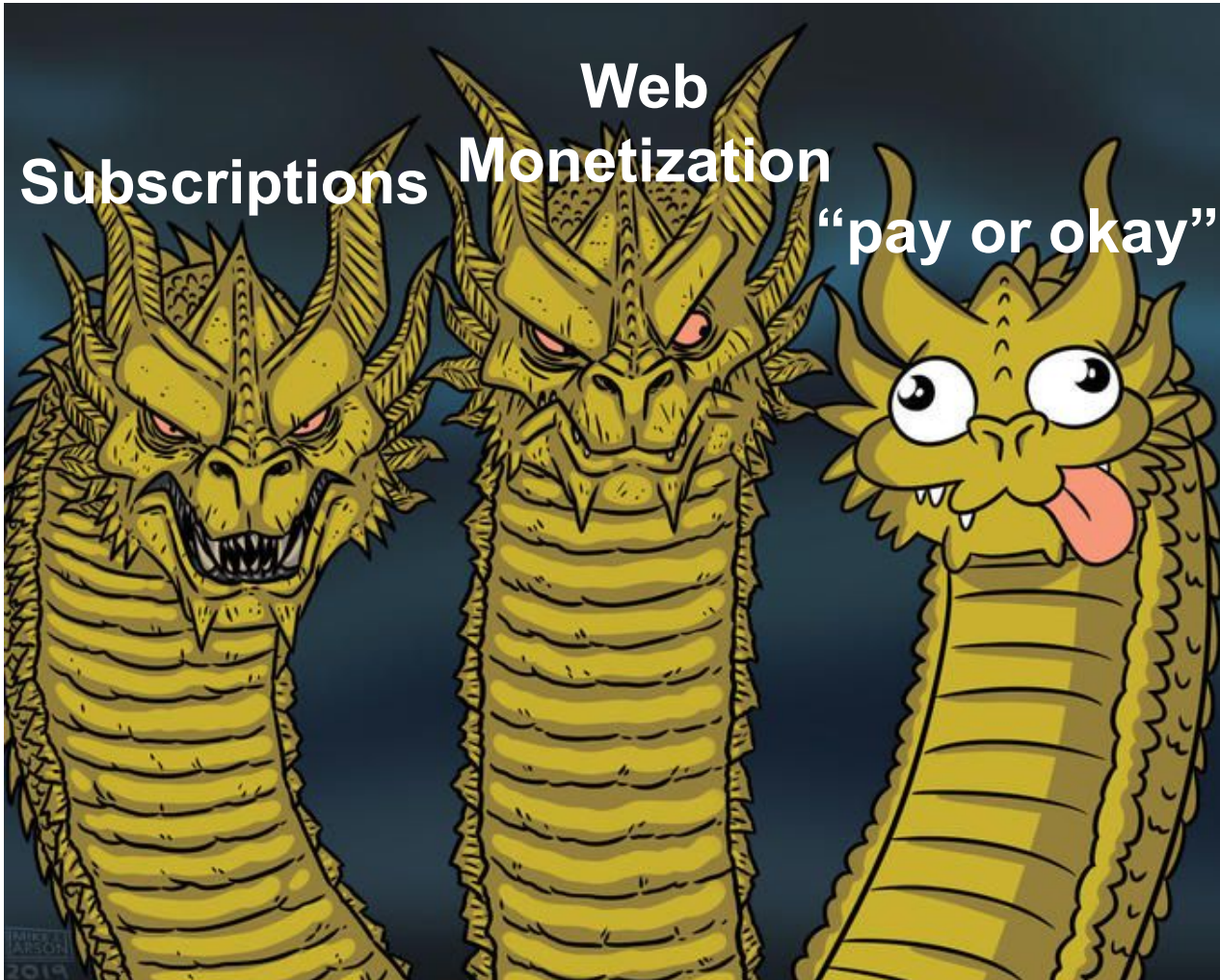
In the long term we want **privacy regulations**
restricting the use of personal data in advertising,
but in the short term we have **competition law** putting
third-party tracking cookies back in Chrome.

Nuanced takes on privacy are required in this space
and we need more people working on it.

- 1) Consider the impact audience targeting has on metrics.
- 2) Refocus on normative privacy. DP is a tool, not a panacea.
- 3) The alternative to private advertising isn't no advertising, it's no privacy.

Appendix

Web
Subscriptions Monetization
“pay or okay”





Google Chrome: Agree to 'privacy feature', but get tracking!

[Forced Consent & Consent Bypass](#) / 13 June 2024

Privacy Advocates:

“Privacy sandbox is collecting too much data!”
(and we hate it)

Advertisers:

“Privacy sandbox isn’t collecting enough data!”
(and we hate it)



CHROME PRIVACY SANDBOX

IAB Tech Lab Says The Chrome Privacy Sandbox Is A Time Bomb That Will Break Real-Time Bidding



By Allison Schiff

TUESDAY, FEBRUARY 6TH, 2024 - 9:00 AM

SHARE: [in](#) [e](#) [x](#) [f](#) [+](#)

Bonus: research studies conducted using ad metrics

Leveraging Digital Advertising Platforms for Consumer Research

MICHAEL BRAUN 
BART DE LANGHE
STEFANO PUNTONI
ERIC M. SCHWARTZ

Banker, Sachin and Joowon Park (2020), “Evaluating Prosocial COVID-19 Messaging Frames: Evidence from a Field Study on Facebook,” *Judgment and Decision Making*, 15 (6), 1037–43.

Testing Work–Life Theory in Marketing: Evidence from Field Experiments on Social Media

[Nita Umashankar](#)  , [Dhruv Grewal](#) , [...], and [Timothy R. Bohling](#)   [View all authors and affiliations](#)

[Volume 61, Issue 2](#) | <https://doi.org/10.1177/00222437231152894>

JOURNAL ARTICLE

Safe Together, Vulnerable Apart: How Interstitial Space in Text Logos Impacts Brand Attitudes in Tight versus Loose Cultures

[Tanvi Gupta](#) , [Henrik Hagtvedt](#) [Author Notes](#)

Journal of Consumer Research, Volume 48, Issue 3, October 2021, Pages 474–491, <https://doi.org/10.1093/jcr/ucab006>

Published: 18 February 2021