Privacy in Internet Advertising: Not all adware is badware

Paul Francis (MPI-SWS)
Bin Cheng (MPI-SWS)
Alexey Reznichenko (MPI-SWS)
Saikat Guha (MSR India)

The Internet is (increasingly) not private

Companies like Google see what you search for, see which websites you visit

Social networks know your personal information

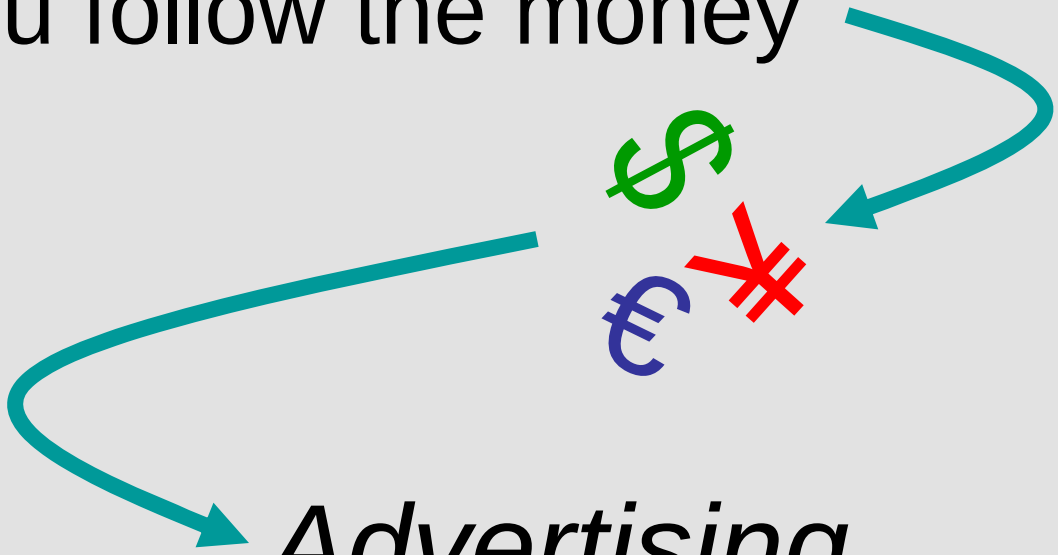
Why do they do this?

Lot’s of reasons, but ……

Why do they do this?

Lot’s of reasons, but ……

If you follow the money



Advertising

Can we replace current advertising systems with one that is private enough, and targets at least as well?

Can we replace current advertising systems with one that is pri enough , and tar

- Follows today's business model
  - Advertisers bid for ad space, pay for clicks
  - Publishers provide ad space, get paid for clicks
- Deal with click fraud
- Scales adequately

Can we replace current advertising systems with one that is private enough, and targets at least as well?

- Most users don't care about privacy
- But privacy advocates do, and so do governments
- Privacy advocates need to be convinced

Can we replace current advertising systems with one that is private enough, and targets at least as well?

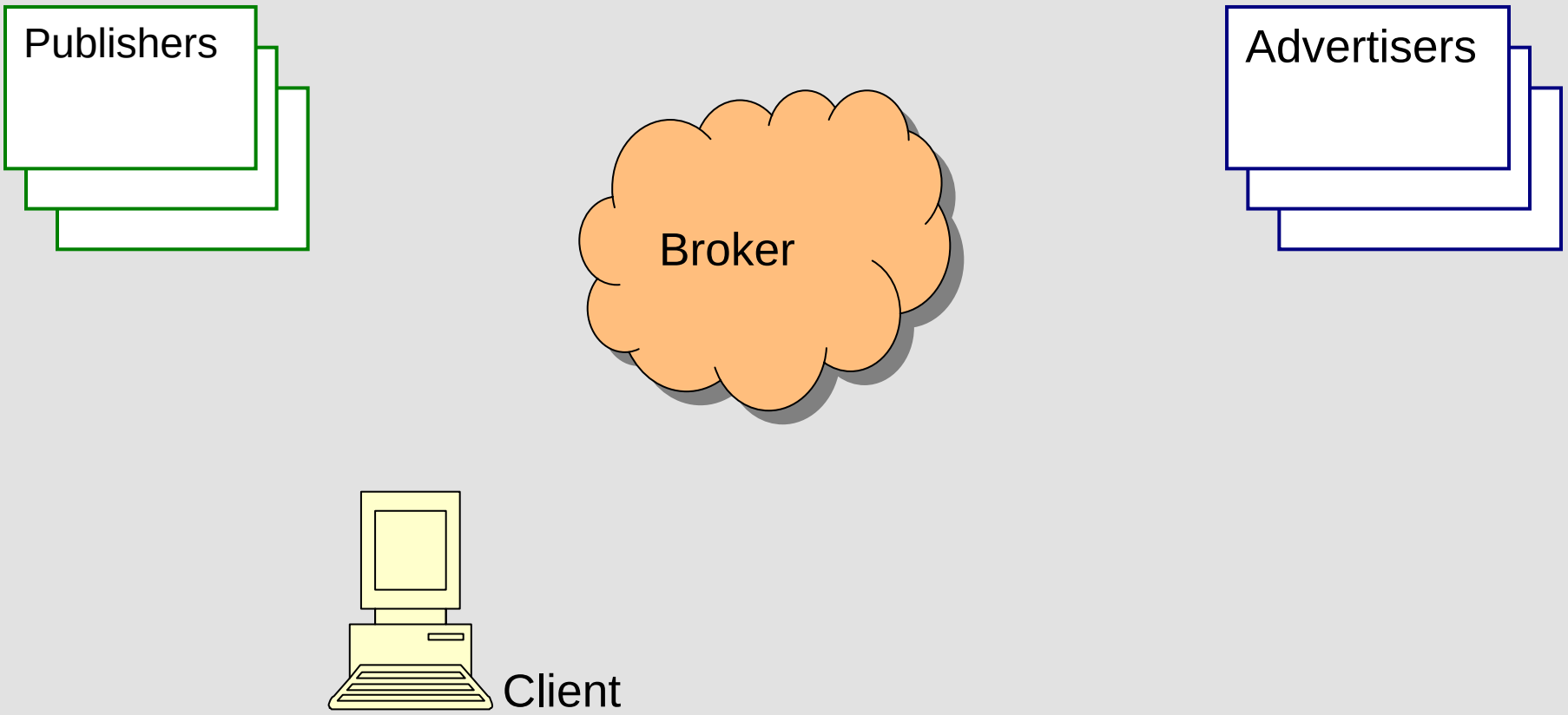
Our approach:

- "As private as possible"
- While still satisfying other goals
- Hope that this is good enough

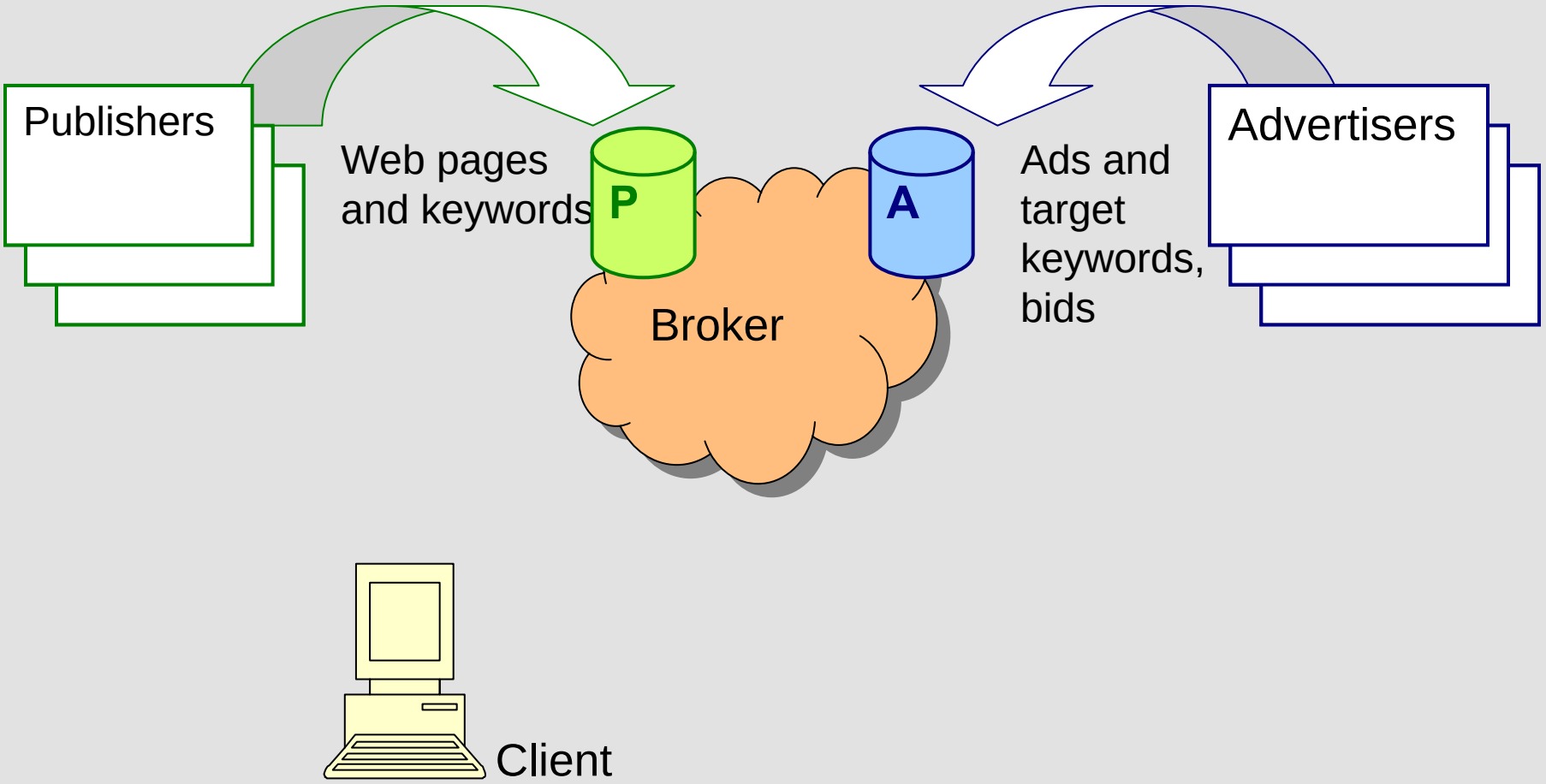
Can we replace current advertising systems with one that is private enough , and targets at least as well?

A principle: Increased privacy begets better personalization

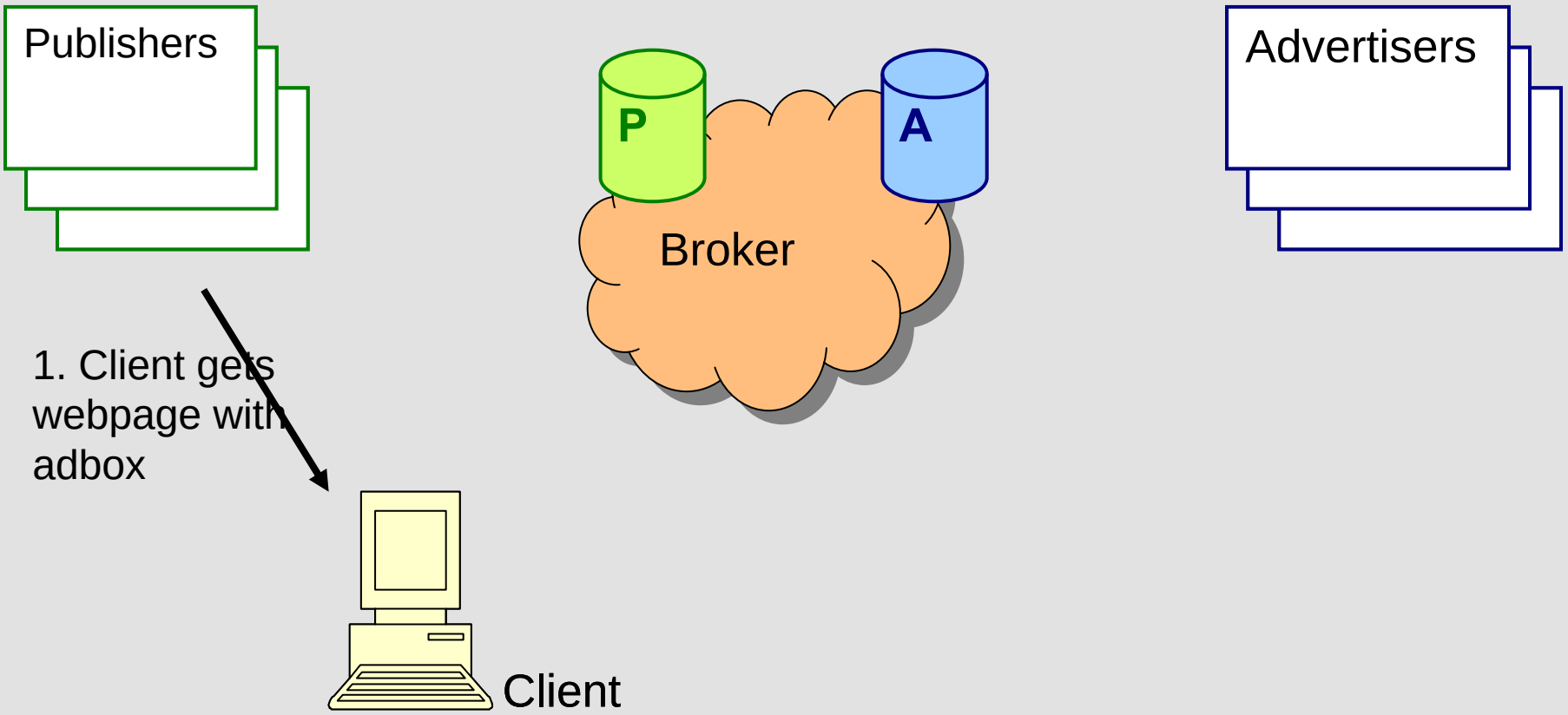
Today’s advertising model



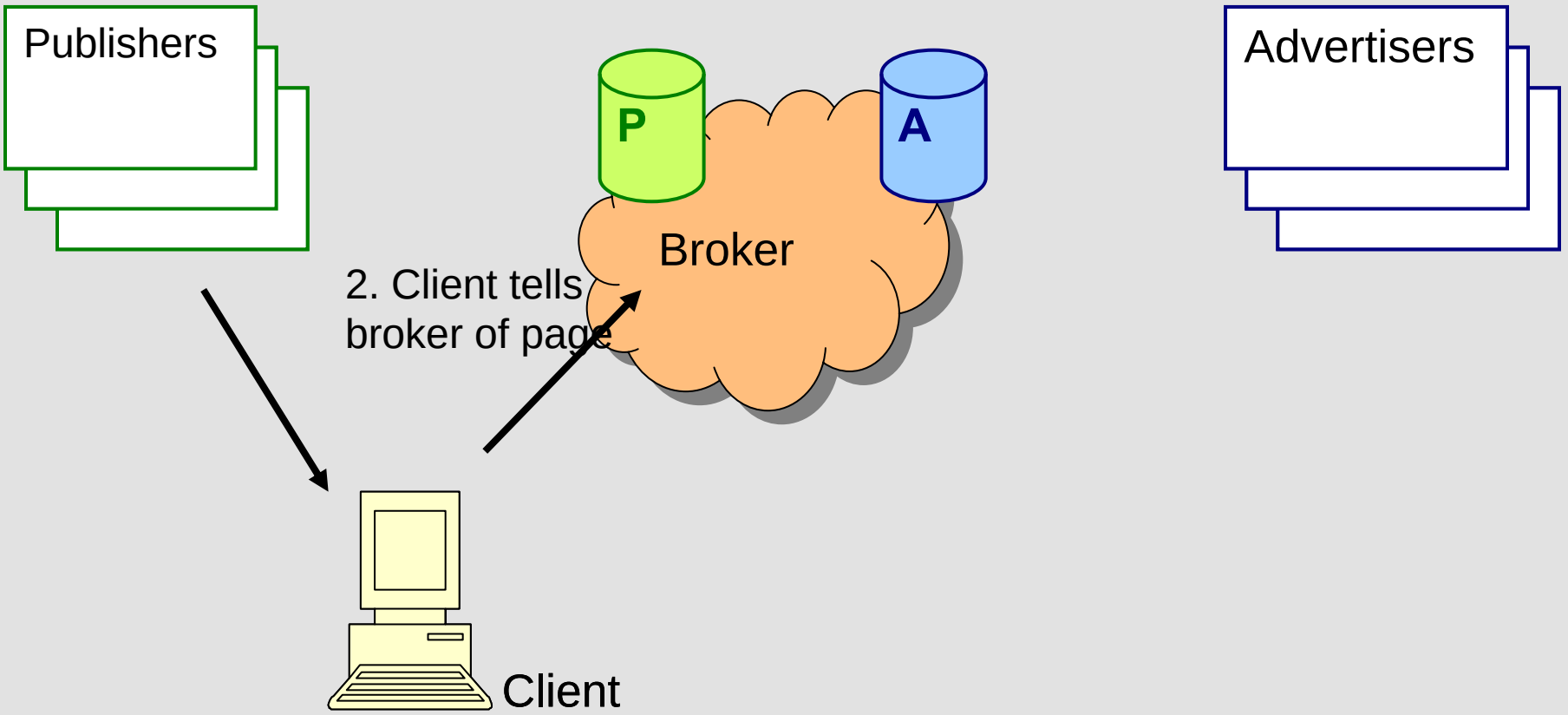
Today's advertising model



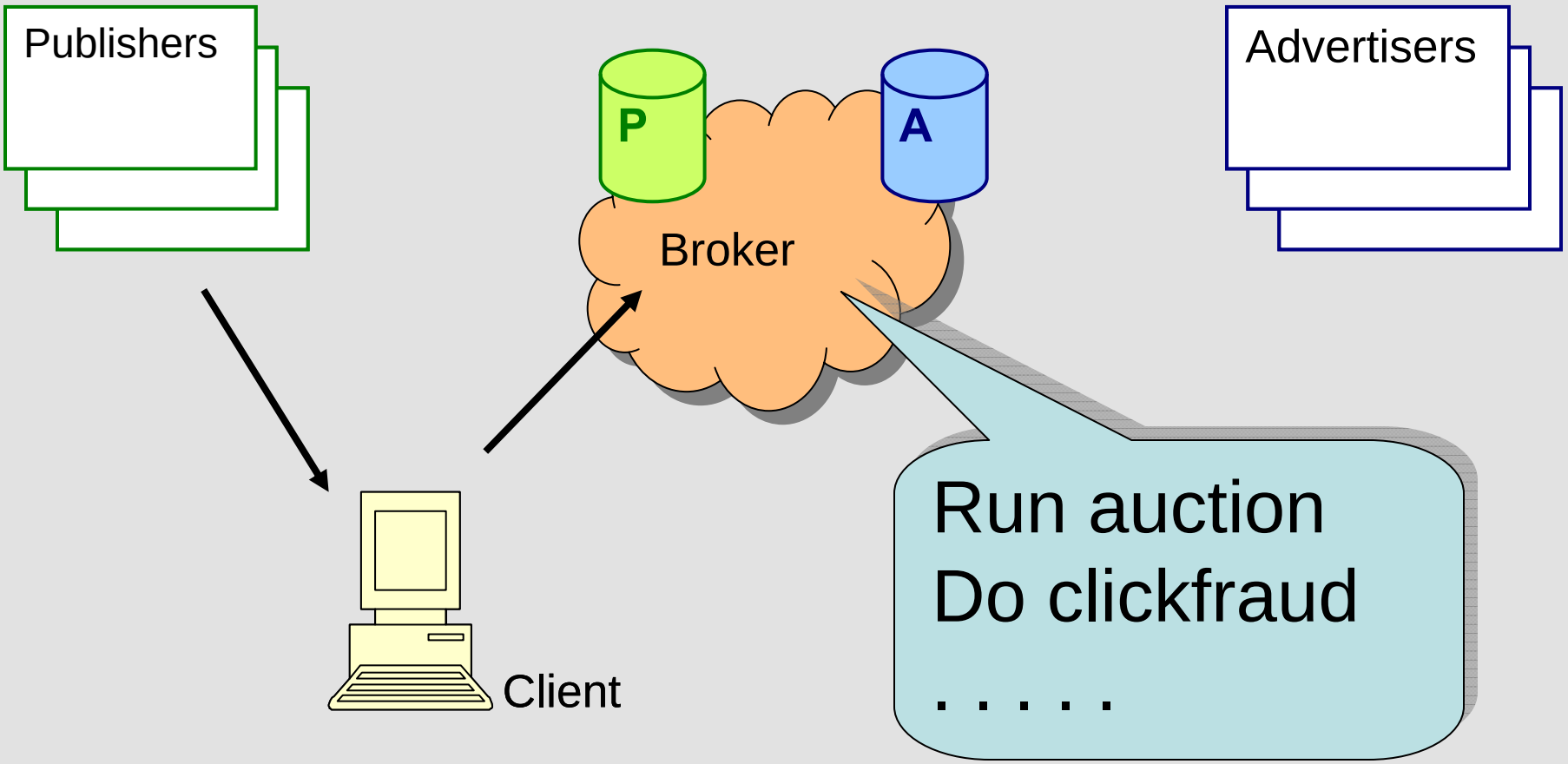
Today's advertising model



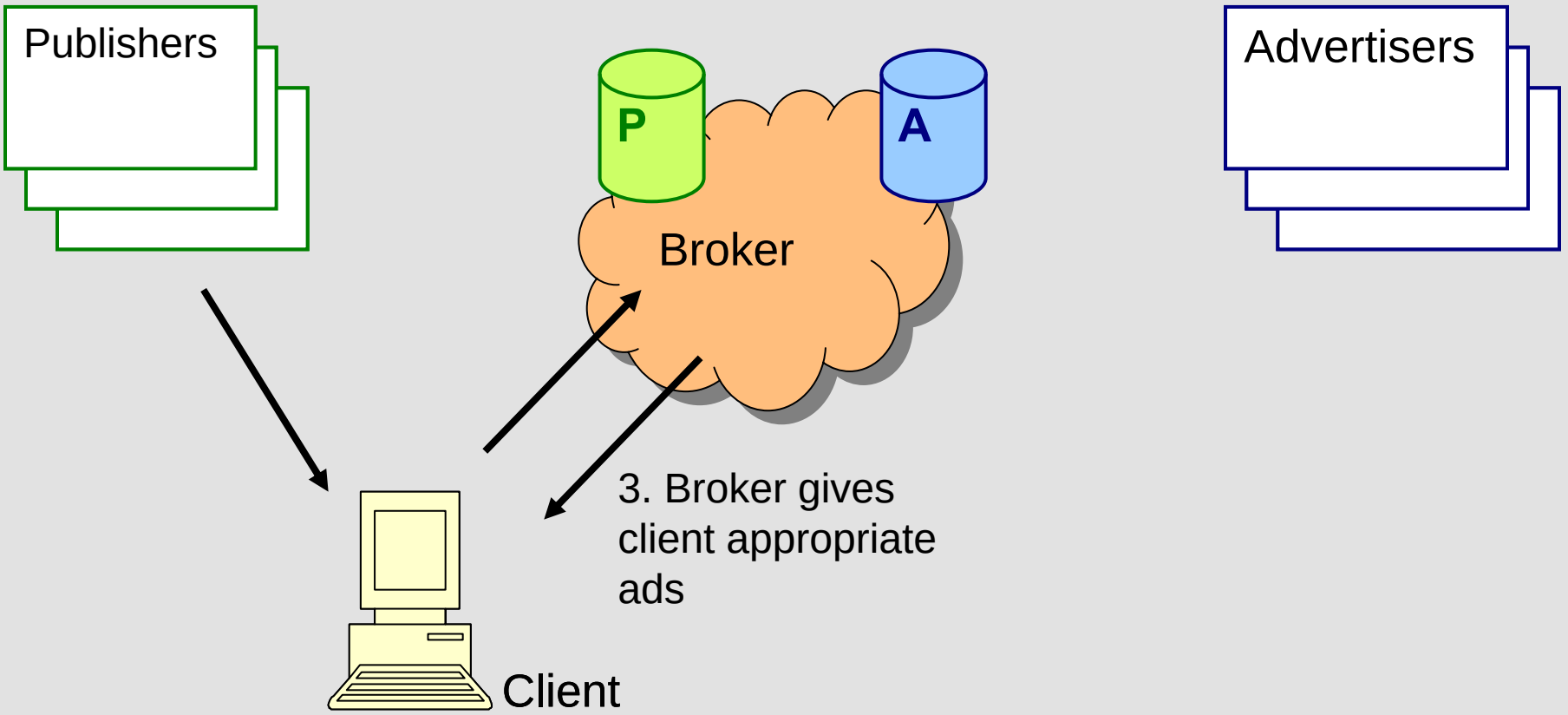
Today's advertising model



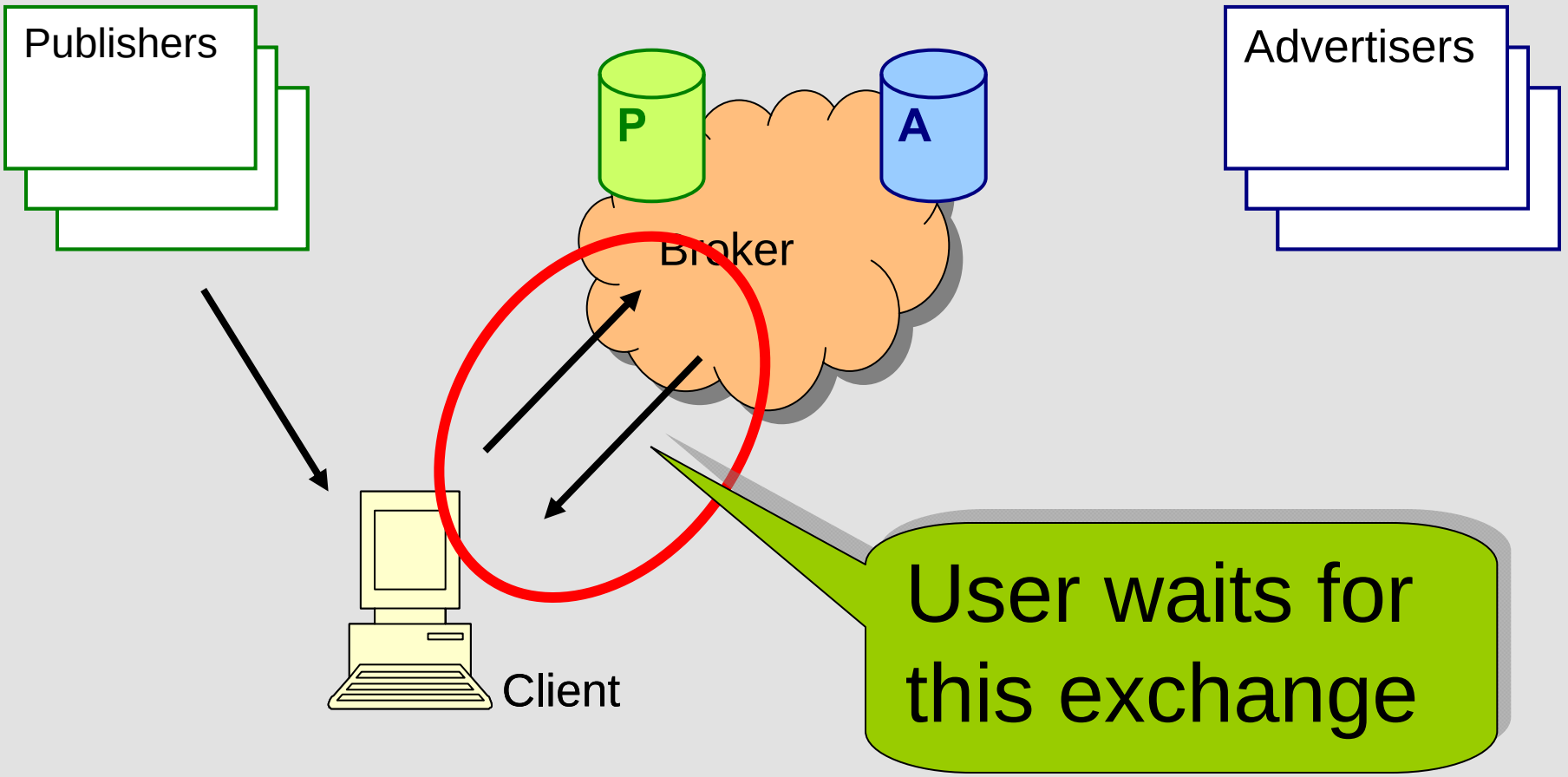
Today's advertising model

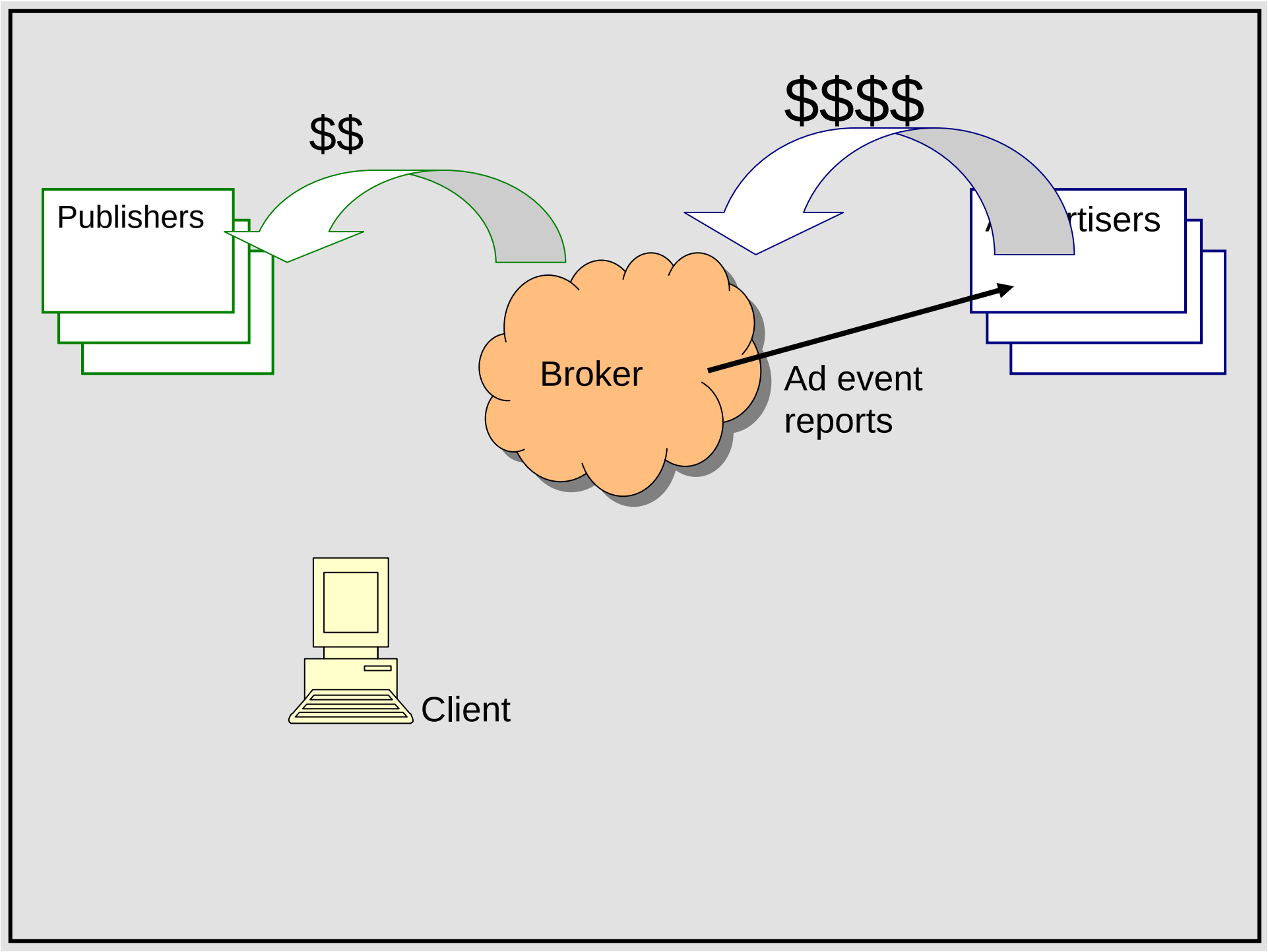


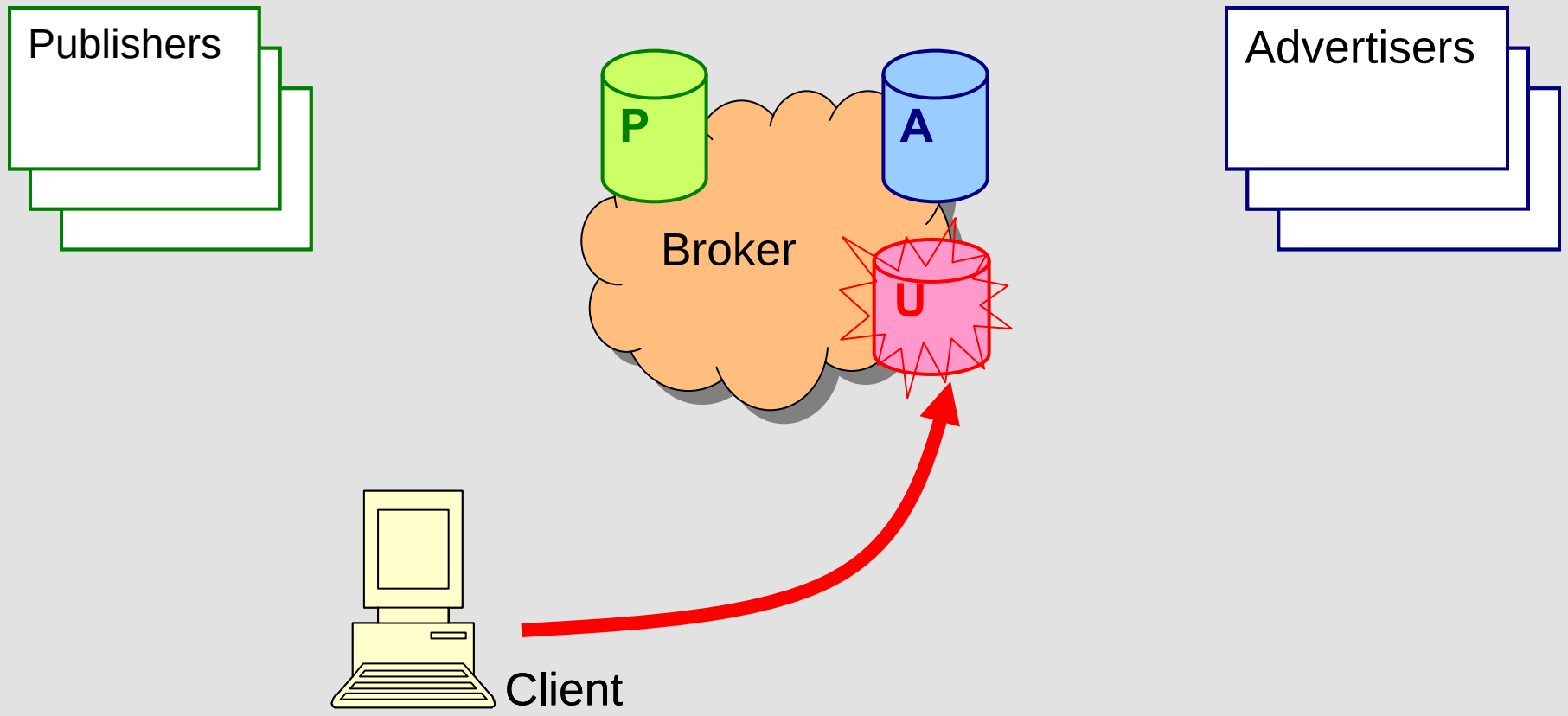
Today's advertising model



Today's advertising model

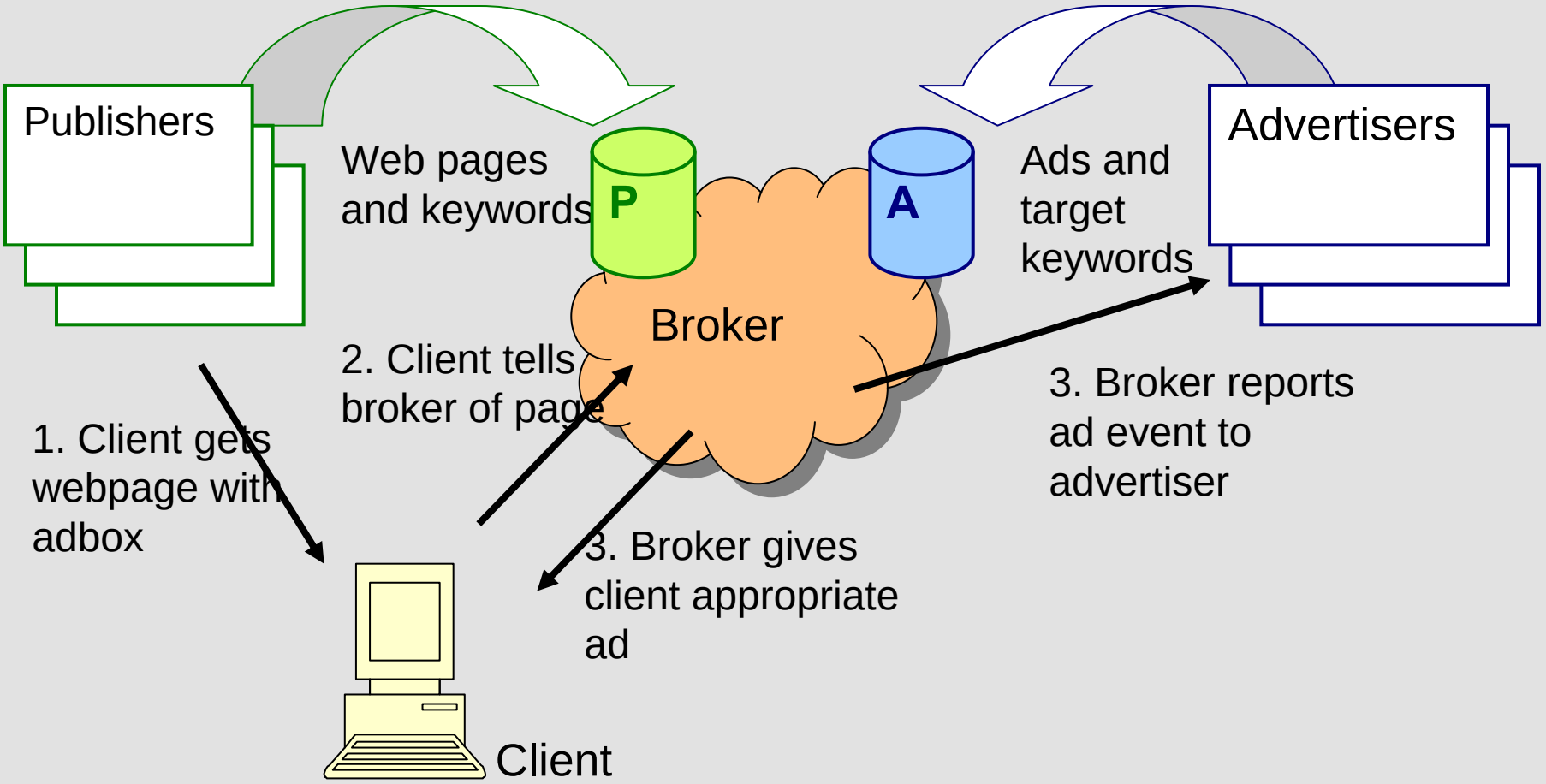



$$
$$$$
Publishers
rtisers
Broker
Ad event
reports
Client



Increasingly, the Broker stores information about the user

Today's advertising model



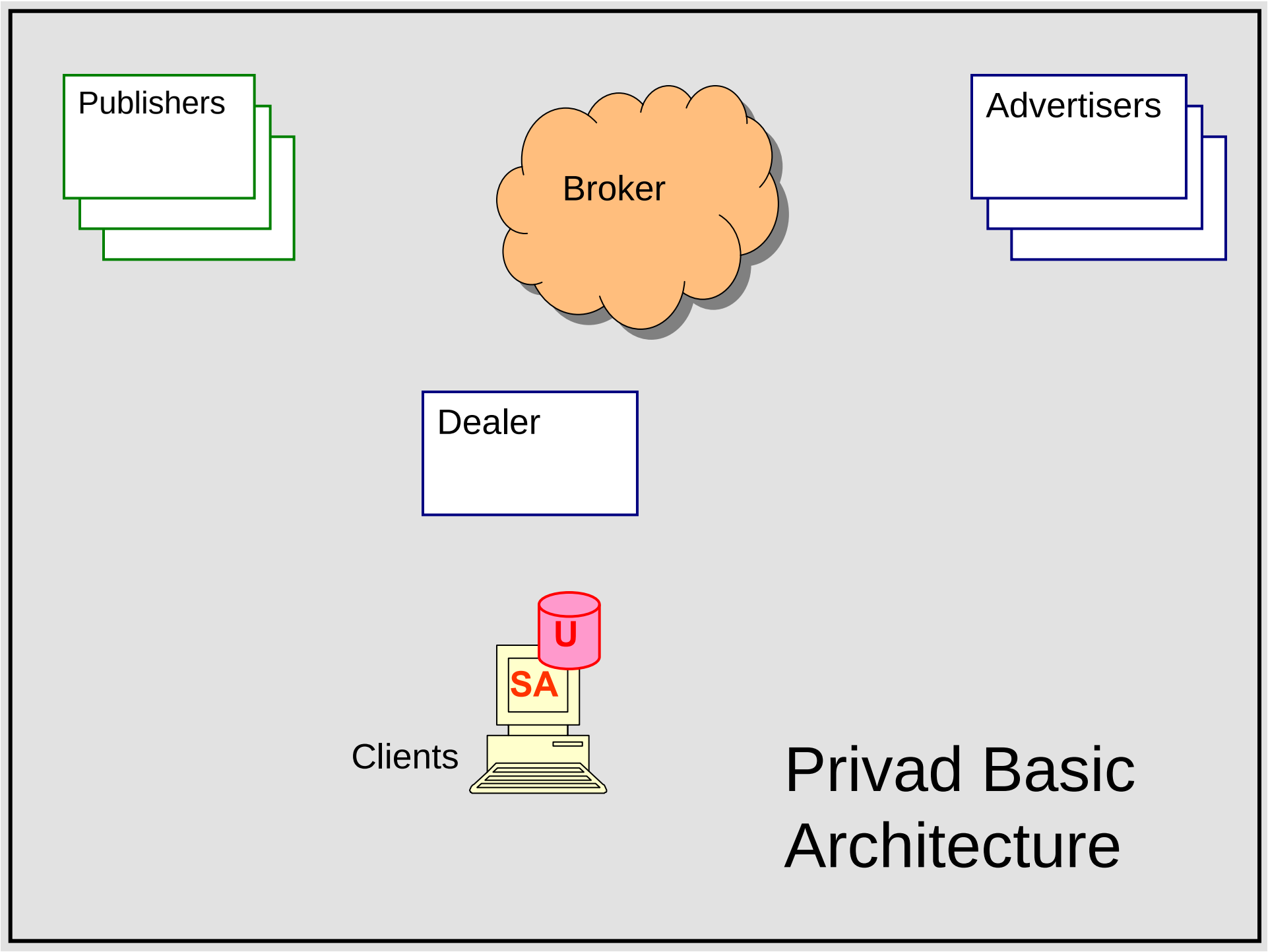
Privad: Basic Approach

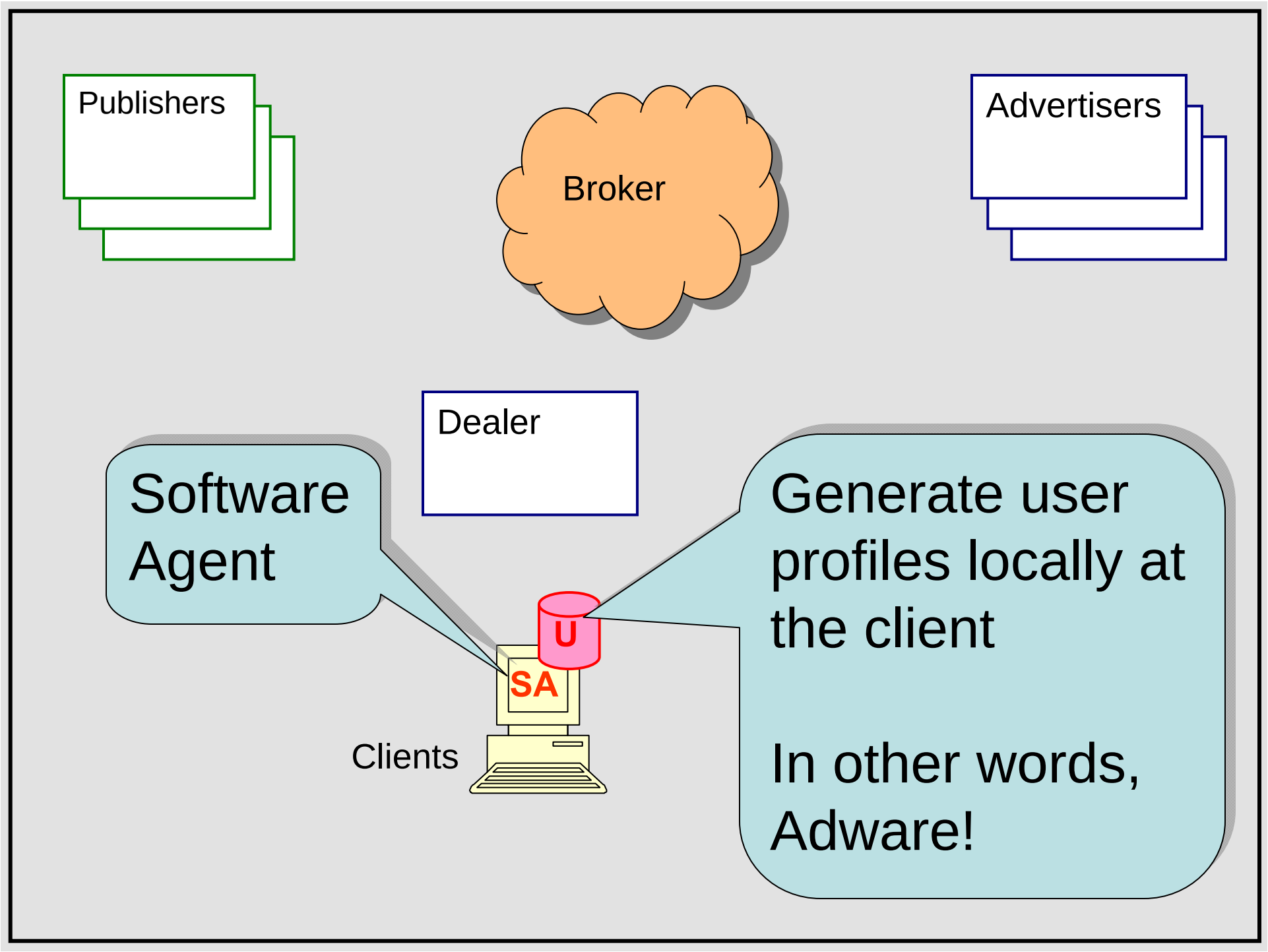
Run profiling on the client

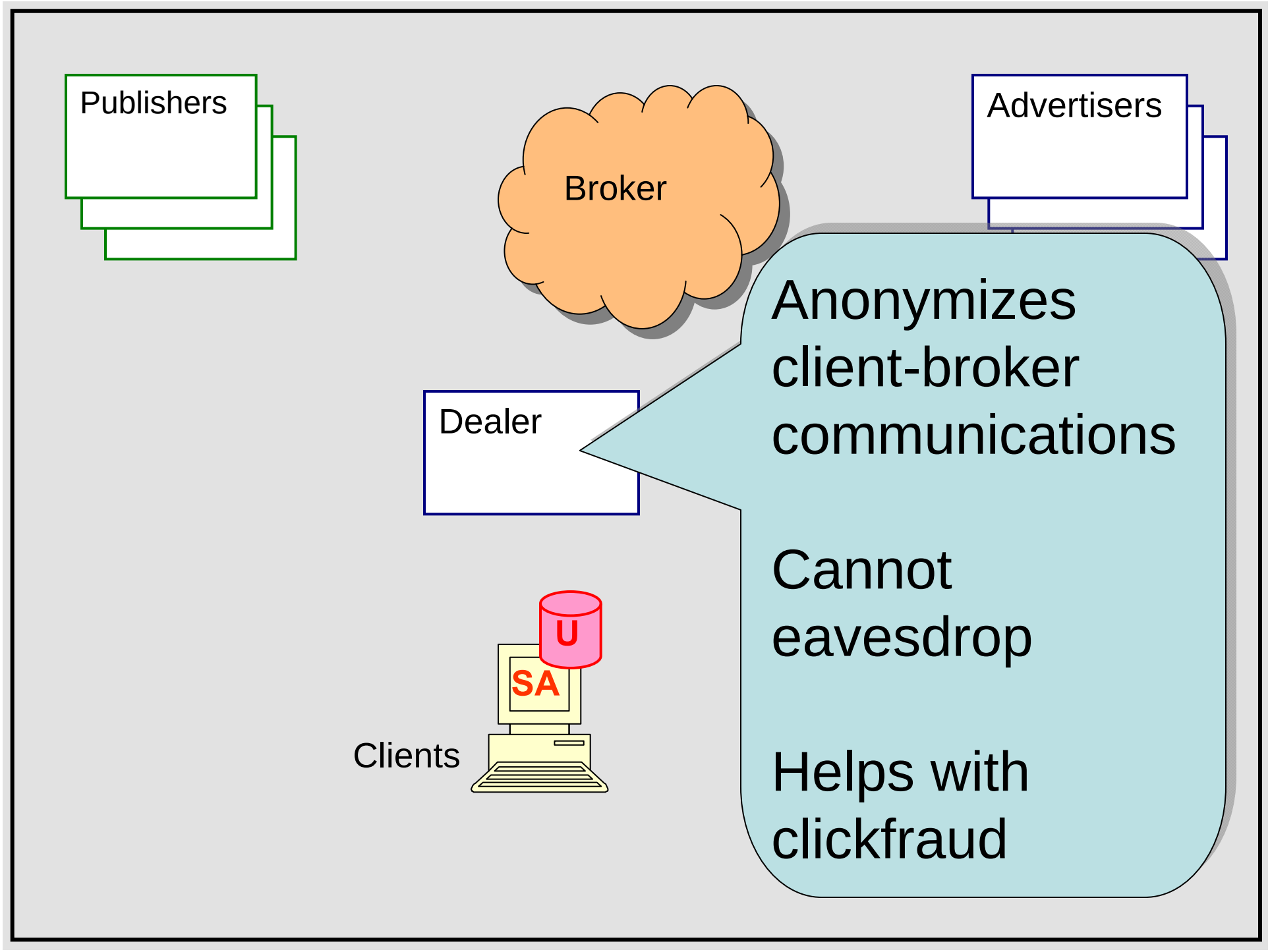
In other words, adware!

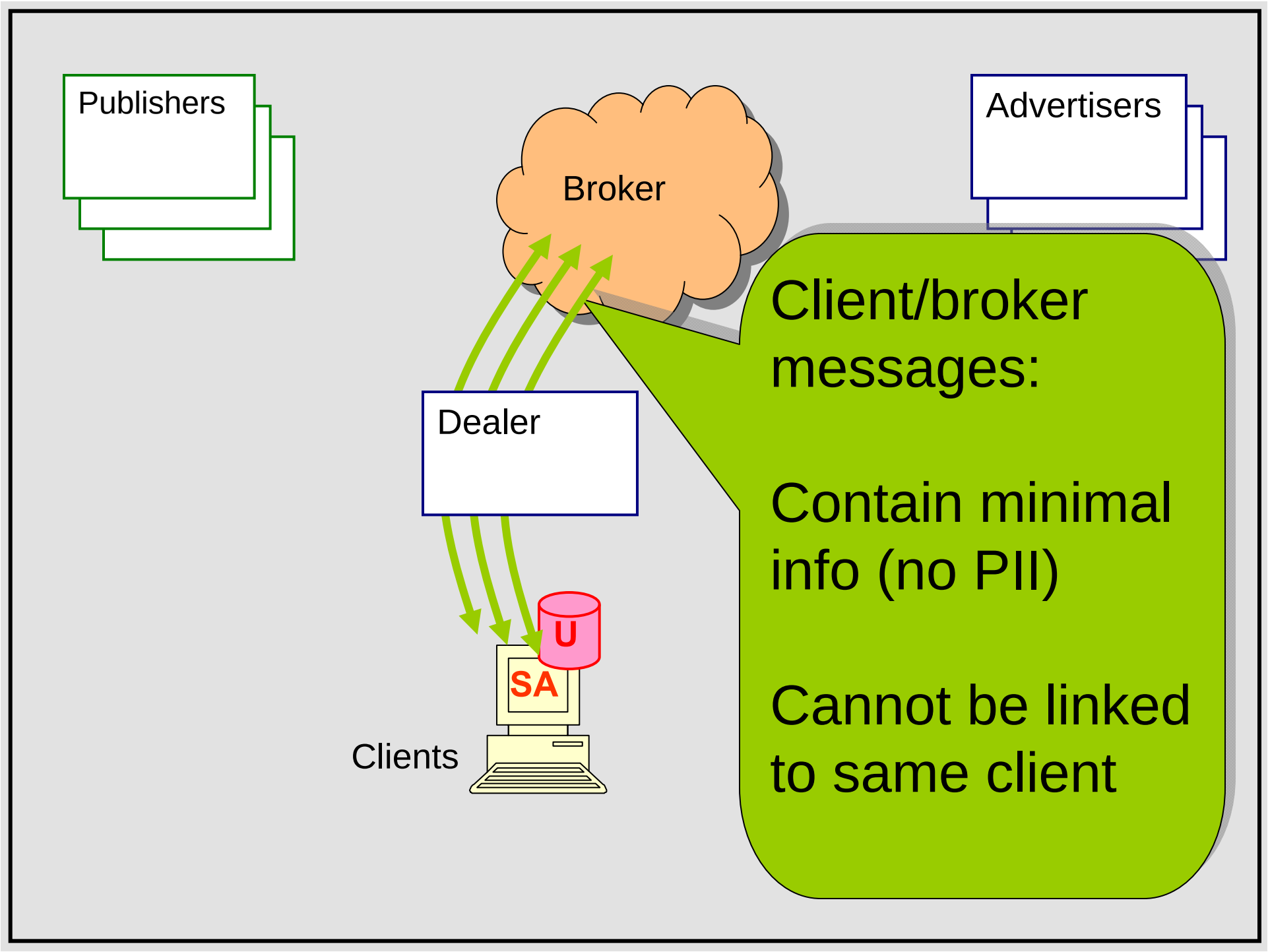
Push ads to clients, let client locally select ads to show

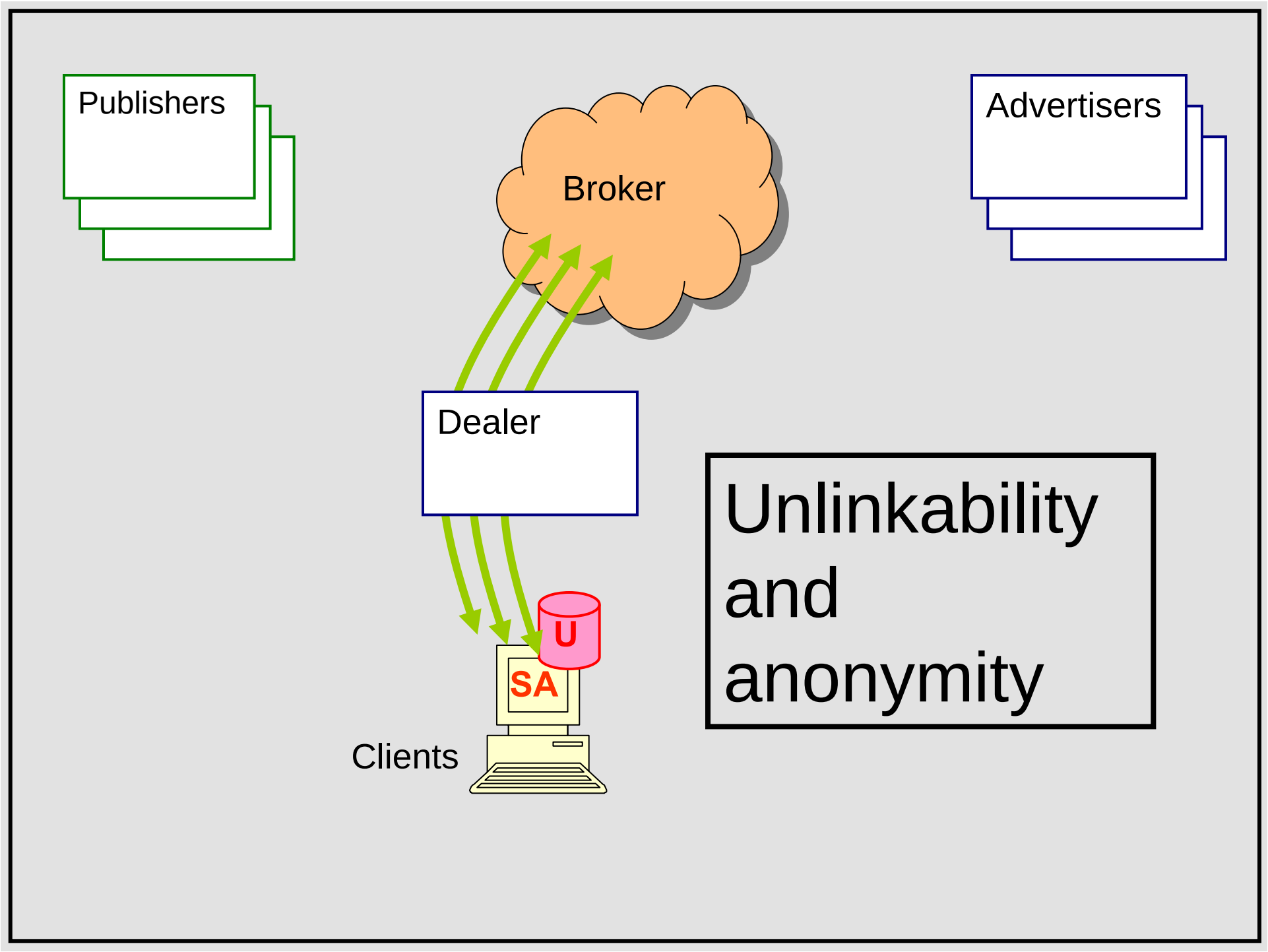
Clients anonymously report ad events, request classes of ads

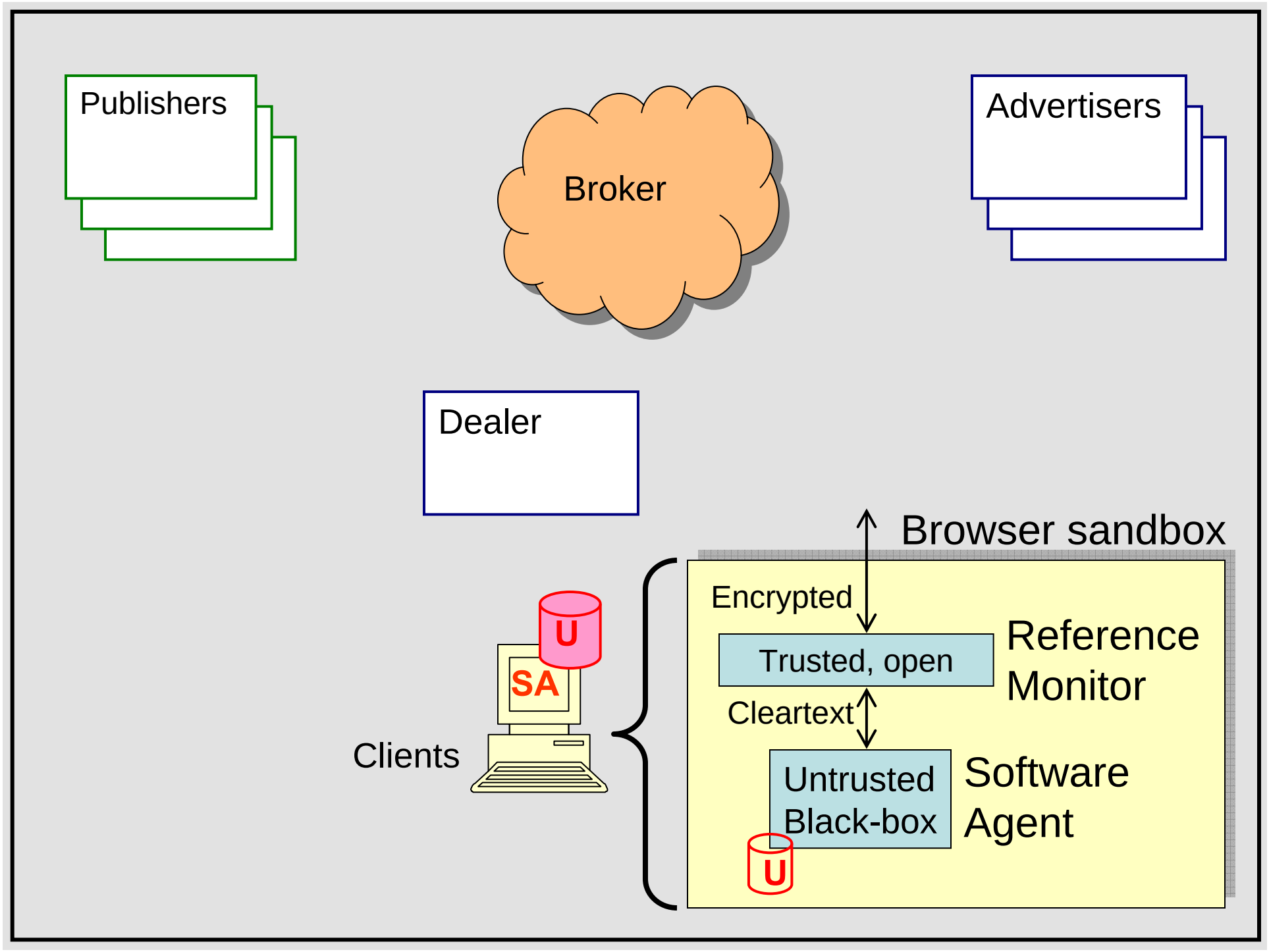

Publishers
Broker
Advertisers
Dealer
U
SA
Clients
Privad Basic Architecture

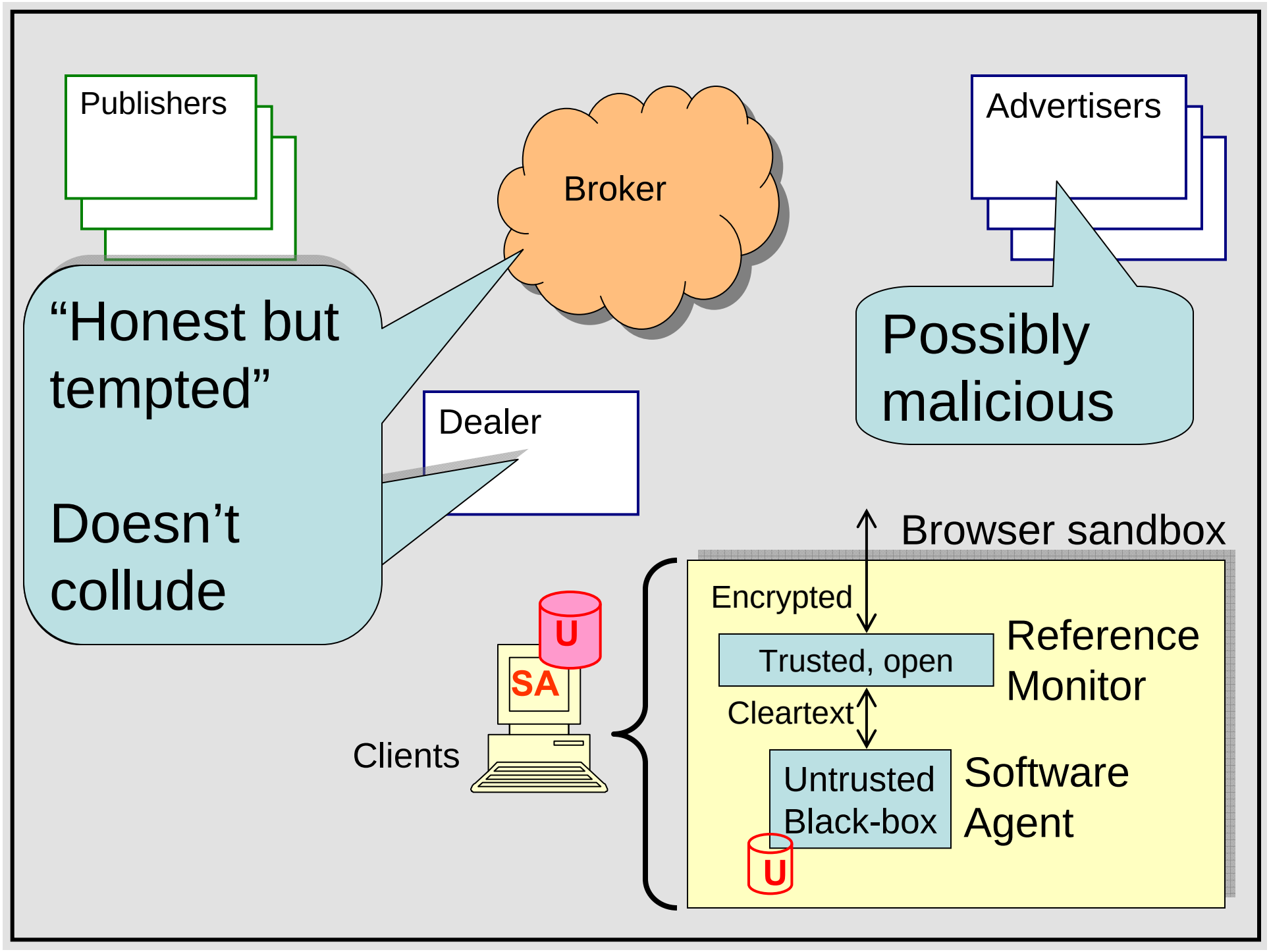

Publishers
Broker
Advertisers
Dealer
Software Agent
U
SA
Clients
Generate user profiles locally at the client
In other words, Adware!

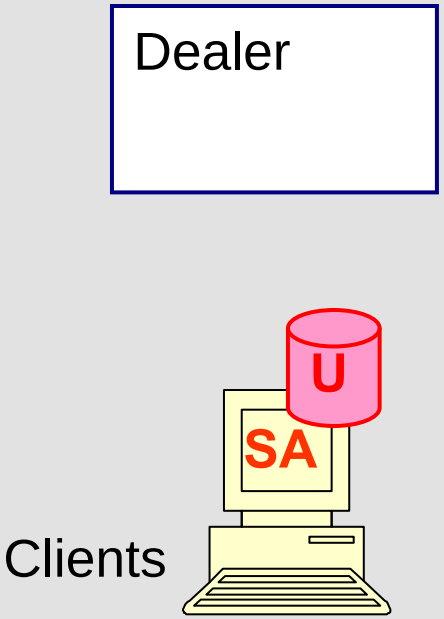

Publishers
Broker
Advertisers
Dealer
Anonymizes client-broker communications
Cannot eavesdrop
Helps with clickfraud
U
SA
Clients


Publishers
Broker
Advertisers
Client/broker messages:
Contain minimal info (no PII)
Cannot be linked to same client
Dealer
U
SA
Clients


Publishers
Broker
Advertisers
Dealer
U
SA
Clients
Unlinkability and anonymity

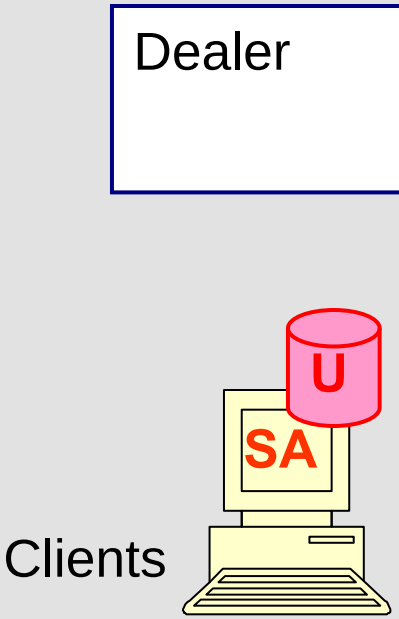

Publishers
Broker
Advertisers
Dealer
Browser sandbox
Encrypted
Trusted, open
Reference Monitor
Cleartext
Untrusted Black-box
Software Agent
U
SA
U
Clients


Publishers
Broker
Advertisers
"Honest but tempted"
Doesn't collude
Possibly malicious
Dealer
Browser sandbox
Encrypted
Trusted, open
Reference Monitor
Cleartext
Untrusted Black-box
Software Agent
U
SA
Clients
U



Dealer and Software Agent are new components

How are they incentivized?



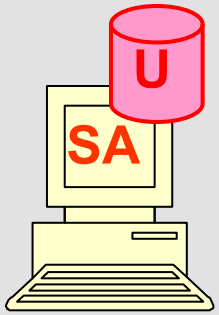
Dealer:

Legally bound to follow protocols, not collude

Execute open-source software, open to inspection

Dealer

Clients



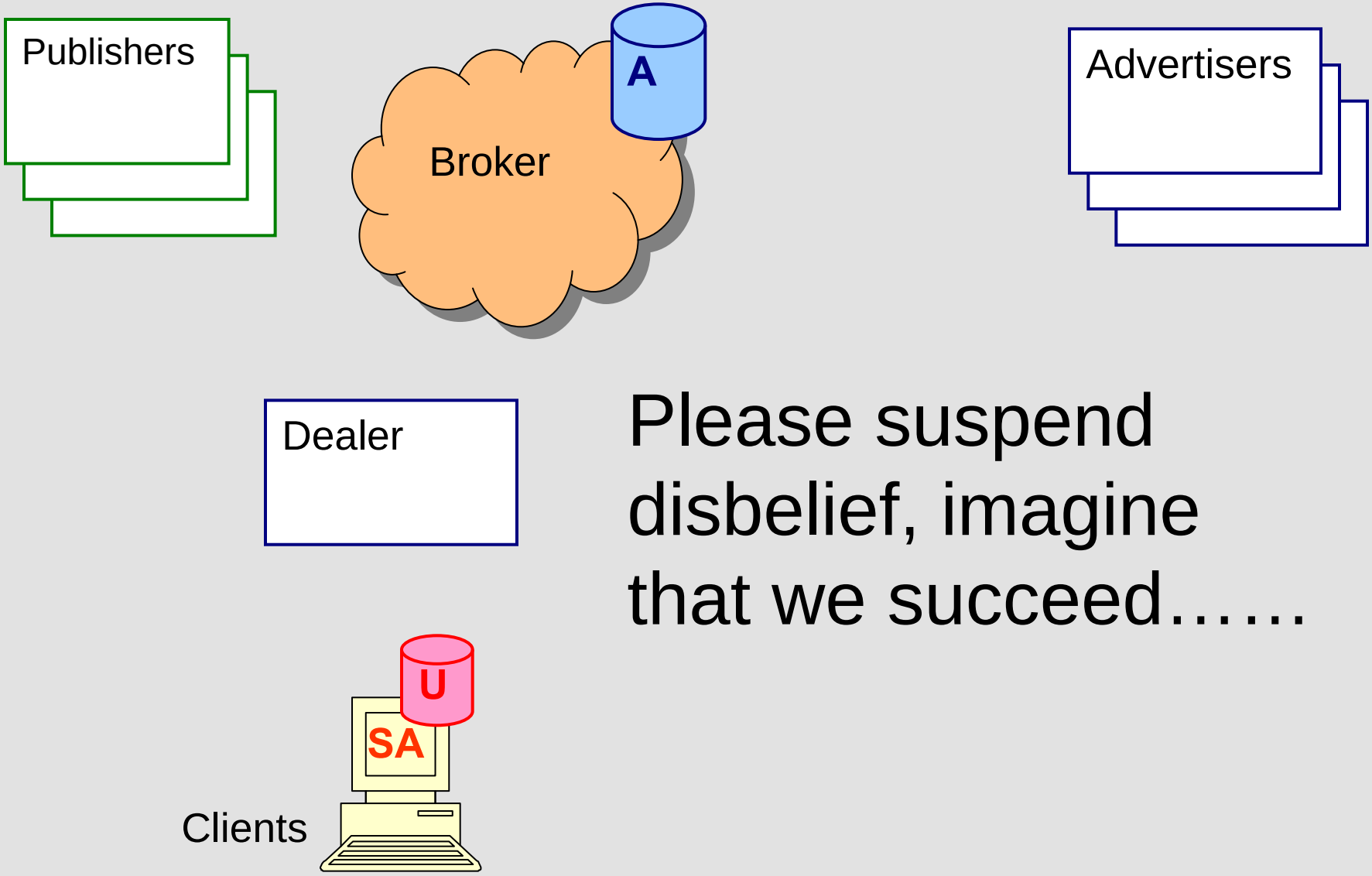
Client:

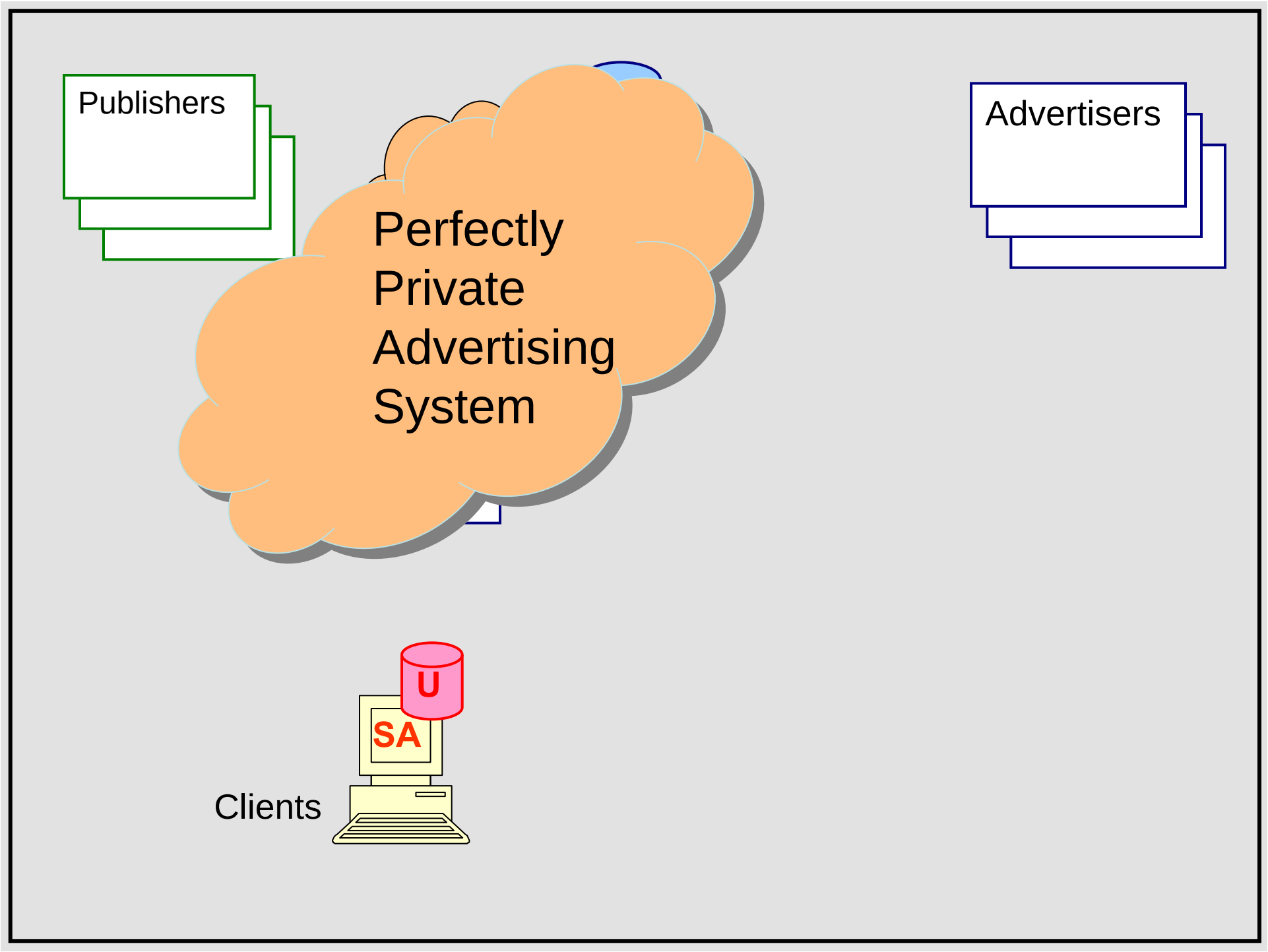
Various options:

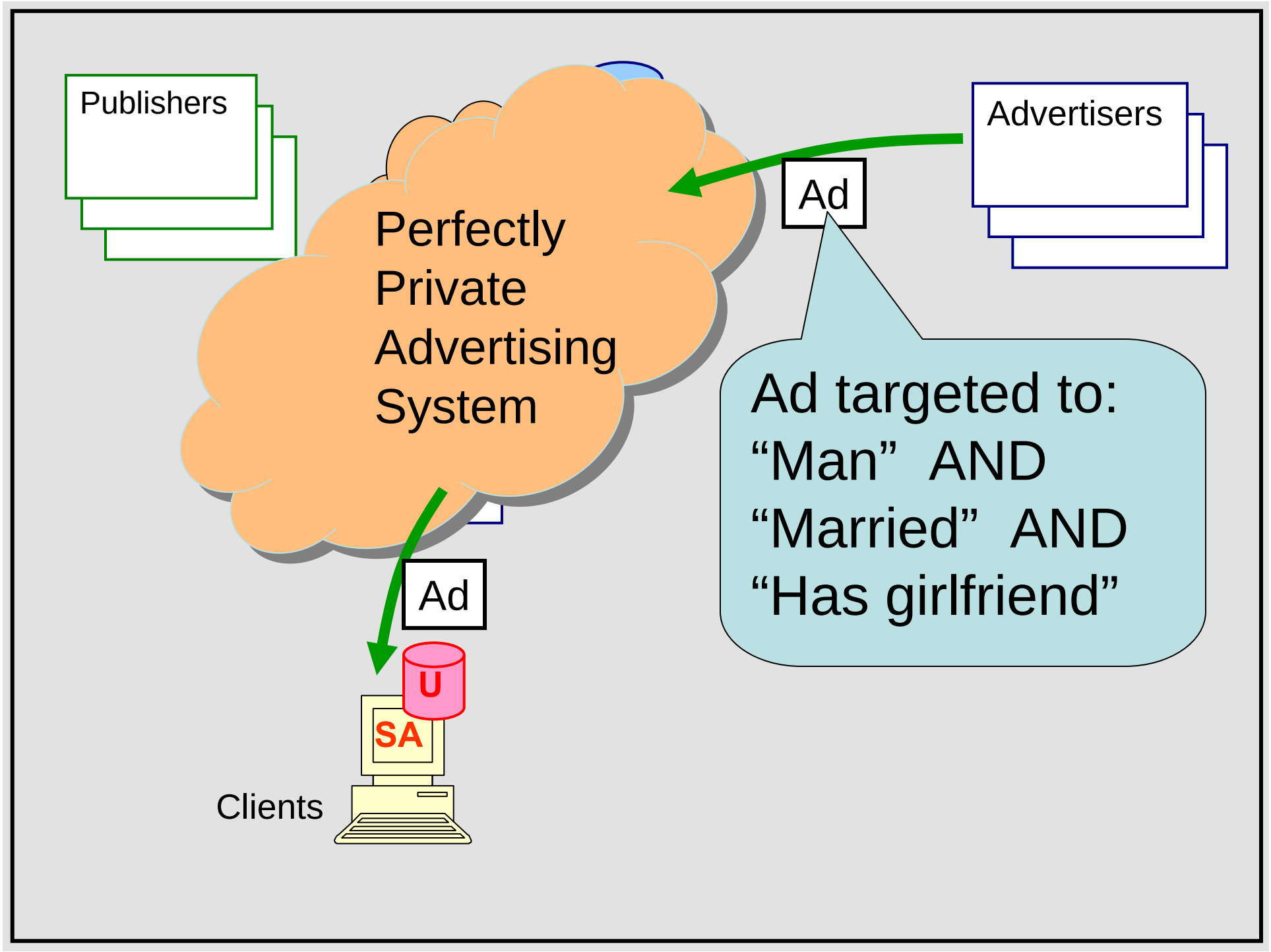
Provide benefit: free software, content, …..

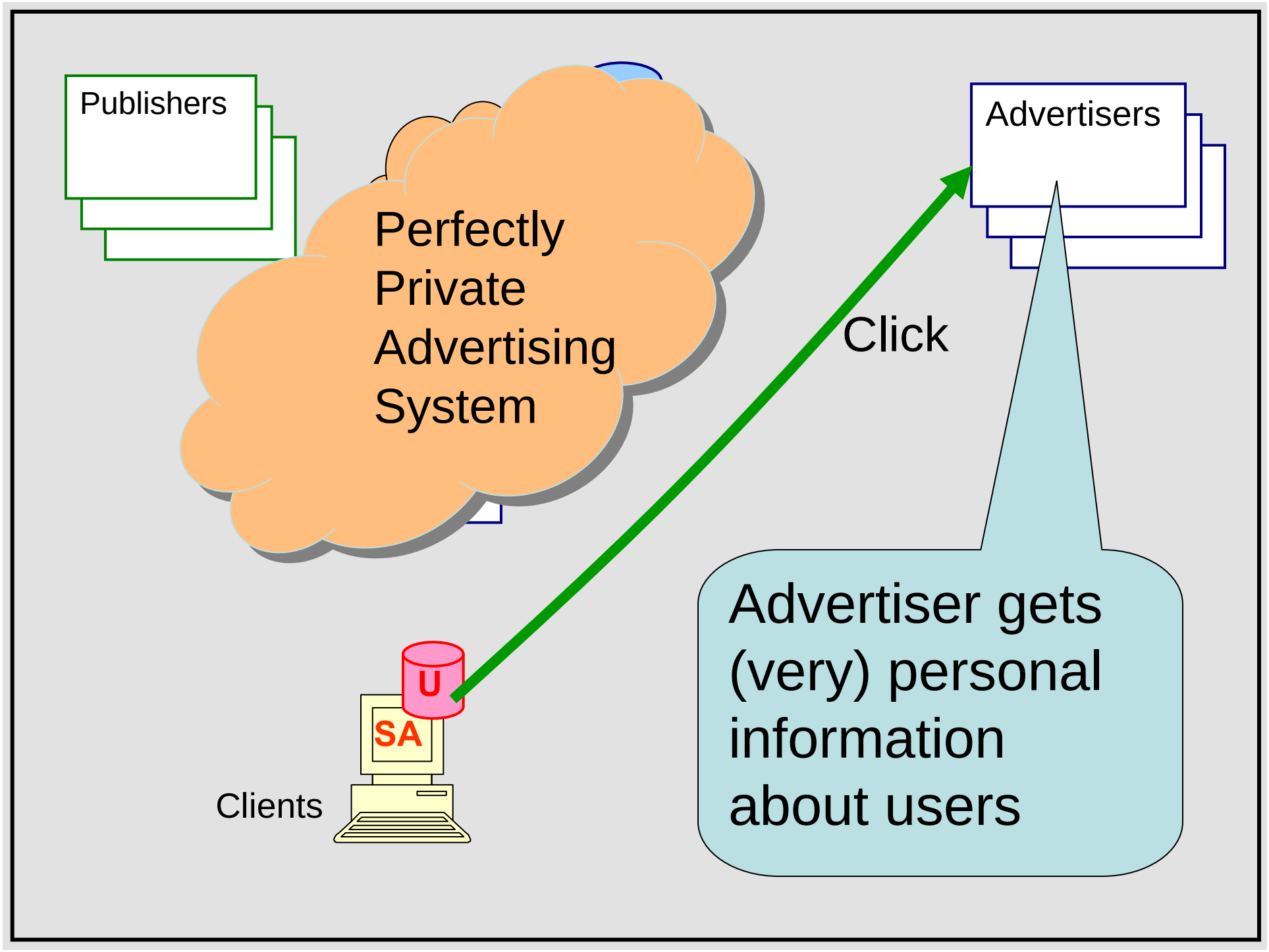
Like adware!

Bundle with browser or OS

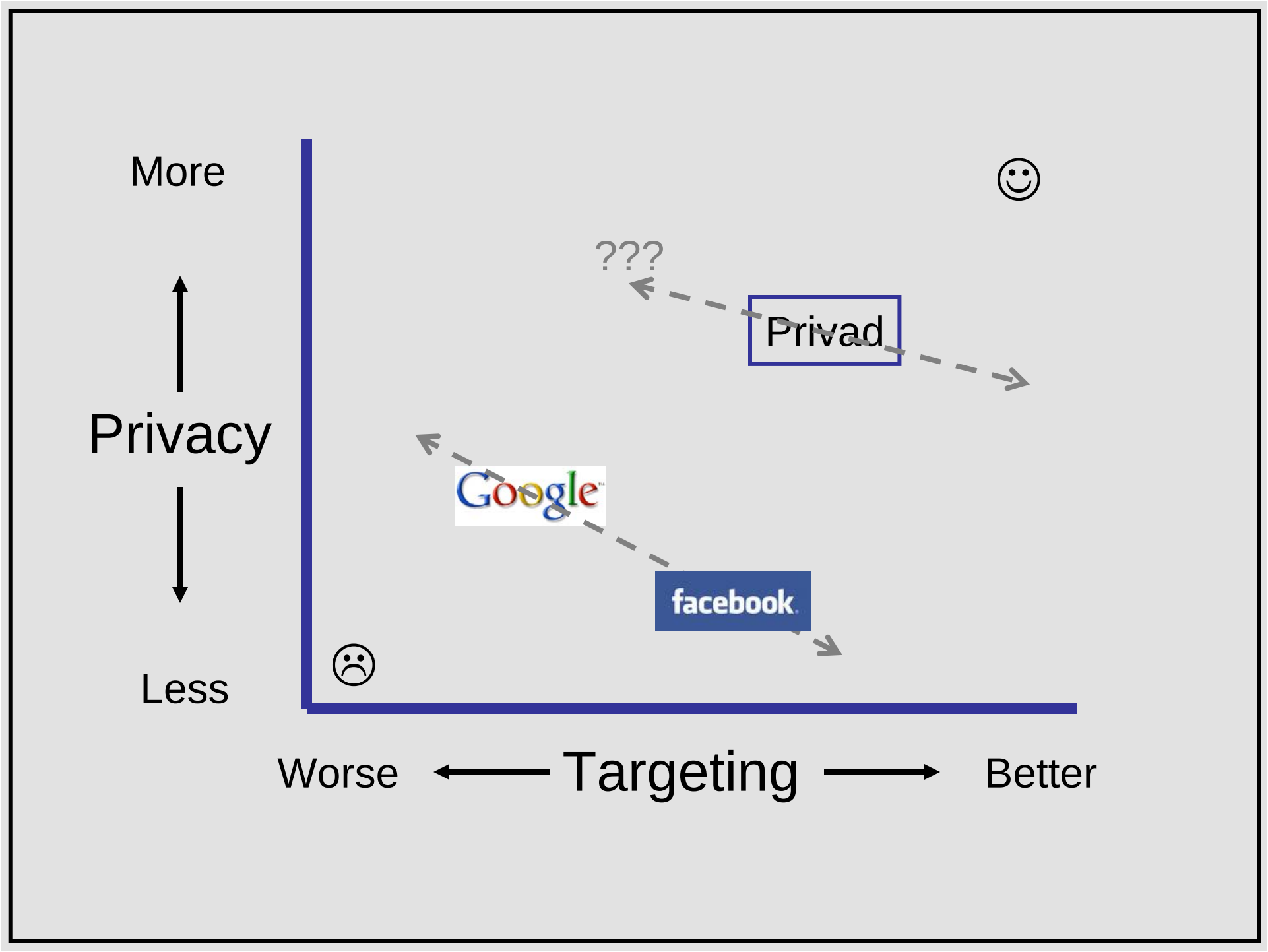

Publishers
Broker
A
Advertisers
Dealer
Please suspend disbelief, imagine that we succeed……
U
SA
Clients


Publishers
Perfectly
Private
Advertising
System
Advertisers
U
SA
Clients


Publishers
Advertisers
Perfectly
Private
Advertising
System
Ad
Ad targeted to:
“Man” AND
“Married” AND
“Has girlfriend”
Ad
U
SA
Clients


Publishers
Perfectly
Private
Advertising
System
Advertisers
Click
U
SA
Clients
Advertiser gets
(very) personal
information
about users


Honey, why are you getting ads for sexy lingerie?

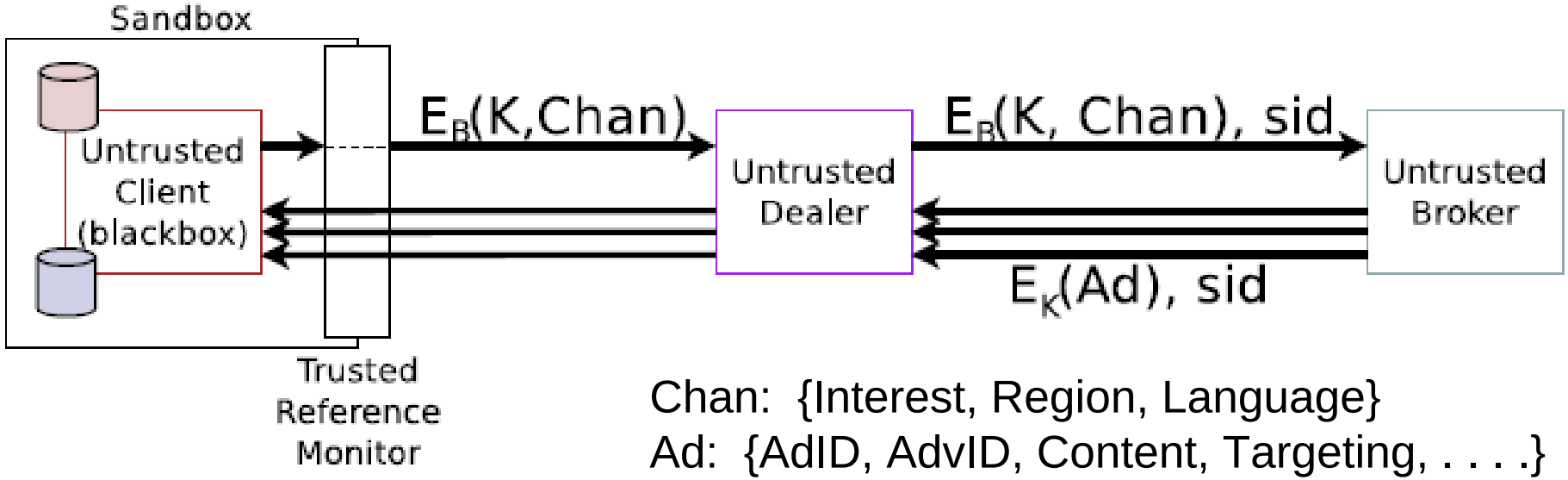

More
Privacy
Less
???
Privad
Google
facebook
Worse
Targeting
Better

Privad: Basic Operation

Before ad view	Client pulls (some set of) ads from Broker
At ad view	Client locally puts (a subest of) ads in adboxes
After ad view	Client reports views/clicks to Broker

Client pulls ads from Broker

- Client determines user interest
  - Currently we look at searches and browsing on shopping sites
  - Pre-defined interest categories
- Client requests ads related to interest
  - Client may reveal language and region, but no other demographics



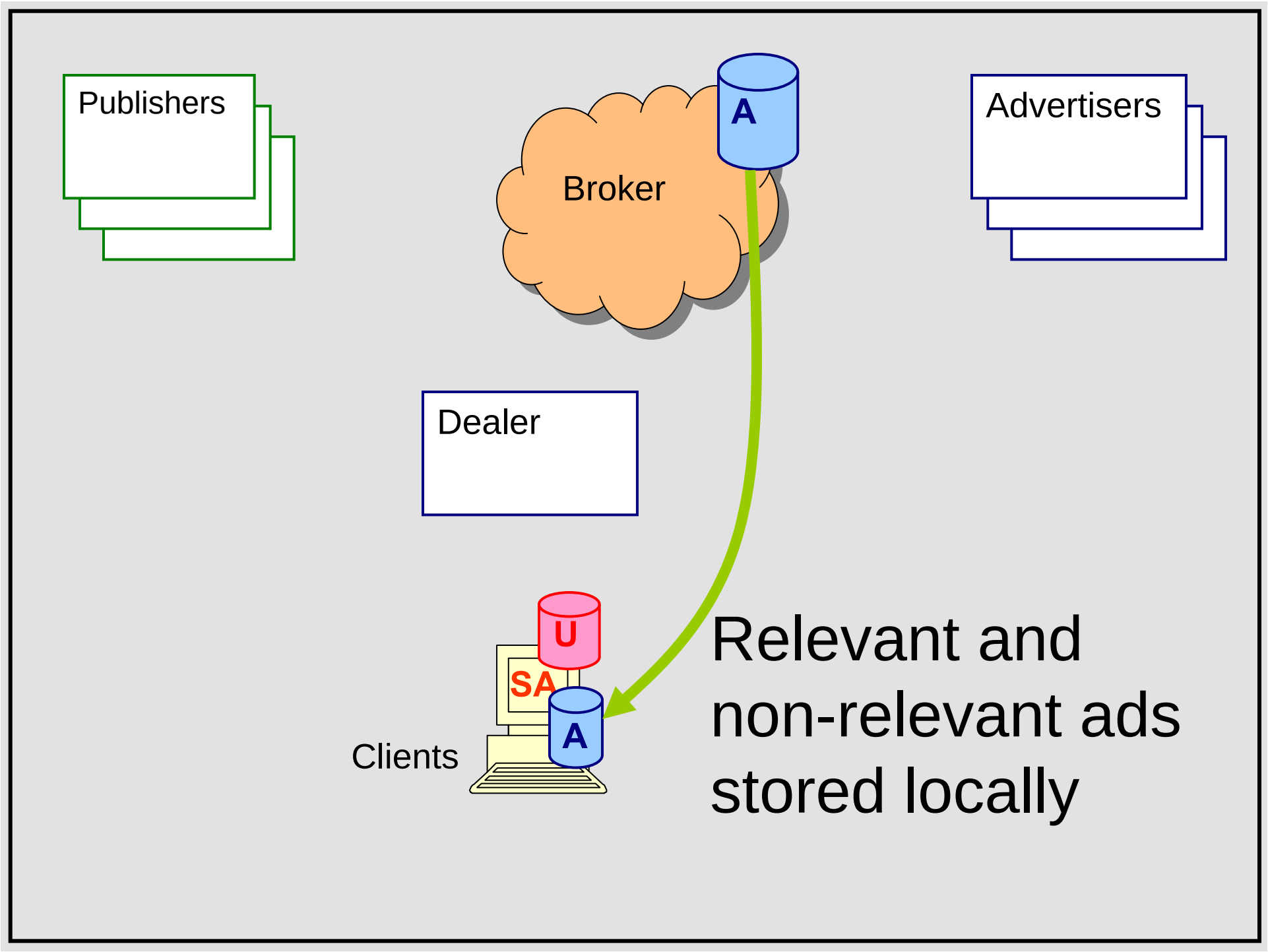
Chan: {Interest, Region, Language}
Ad: {AdID, AdvID, Content, Targeting, ...}

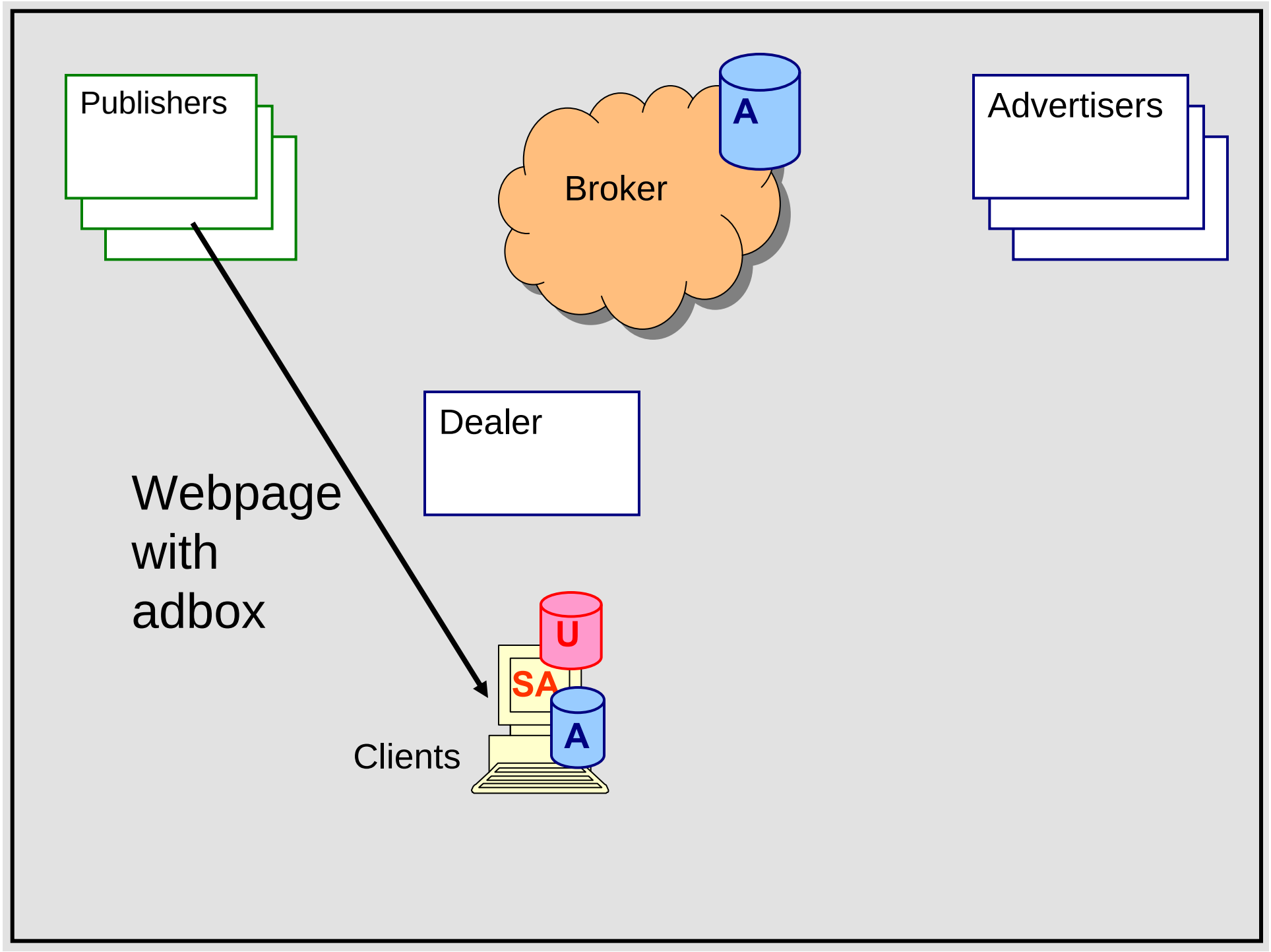
Key K unique to this request

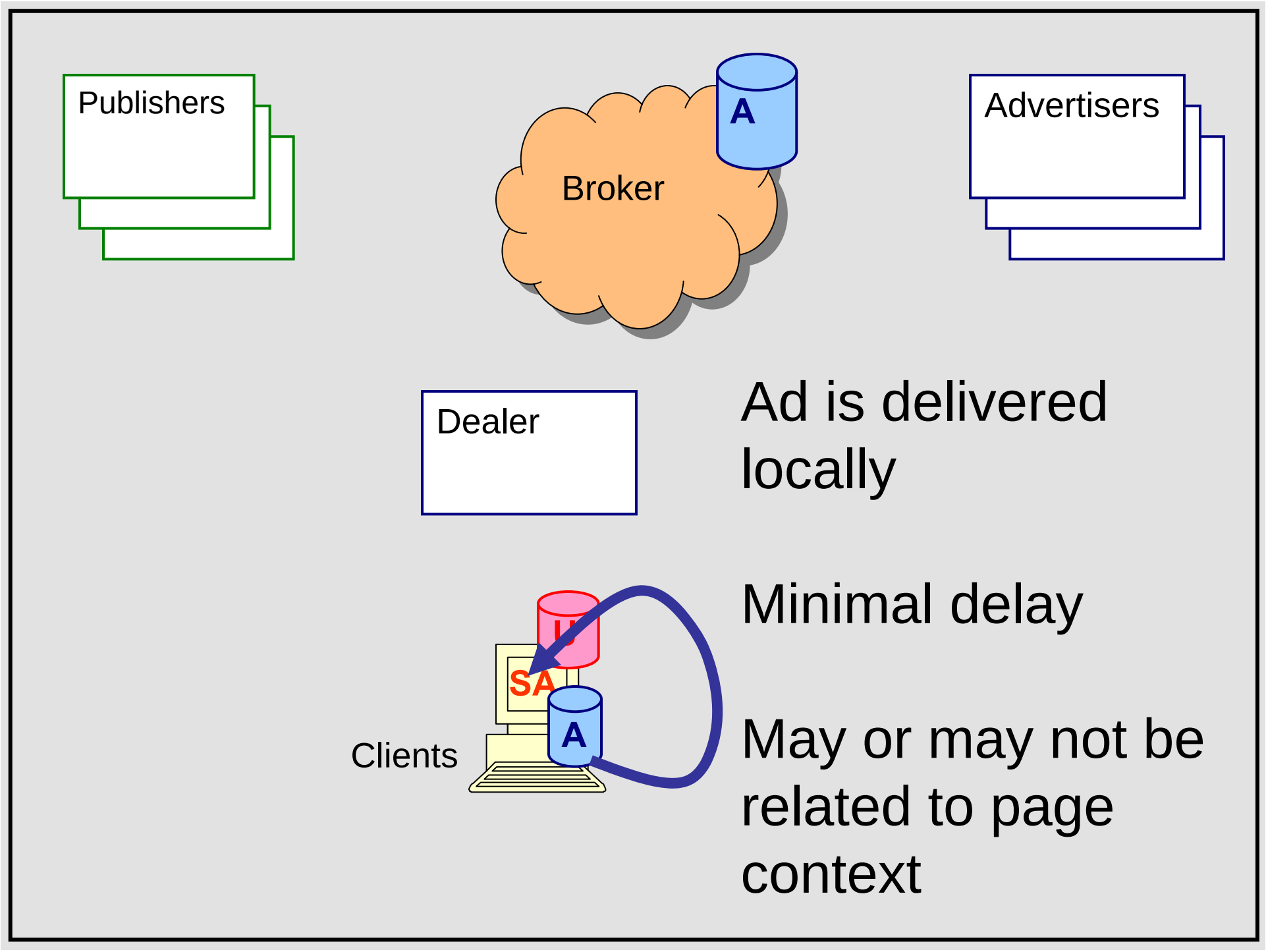
Dealer knows Client requests *some* channel

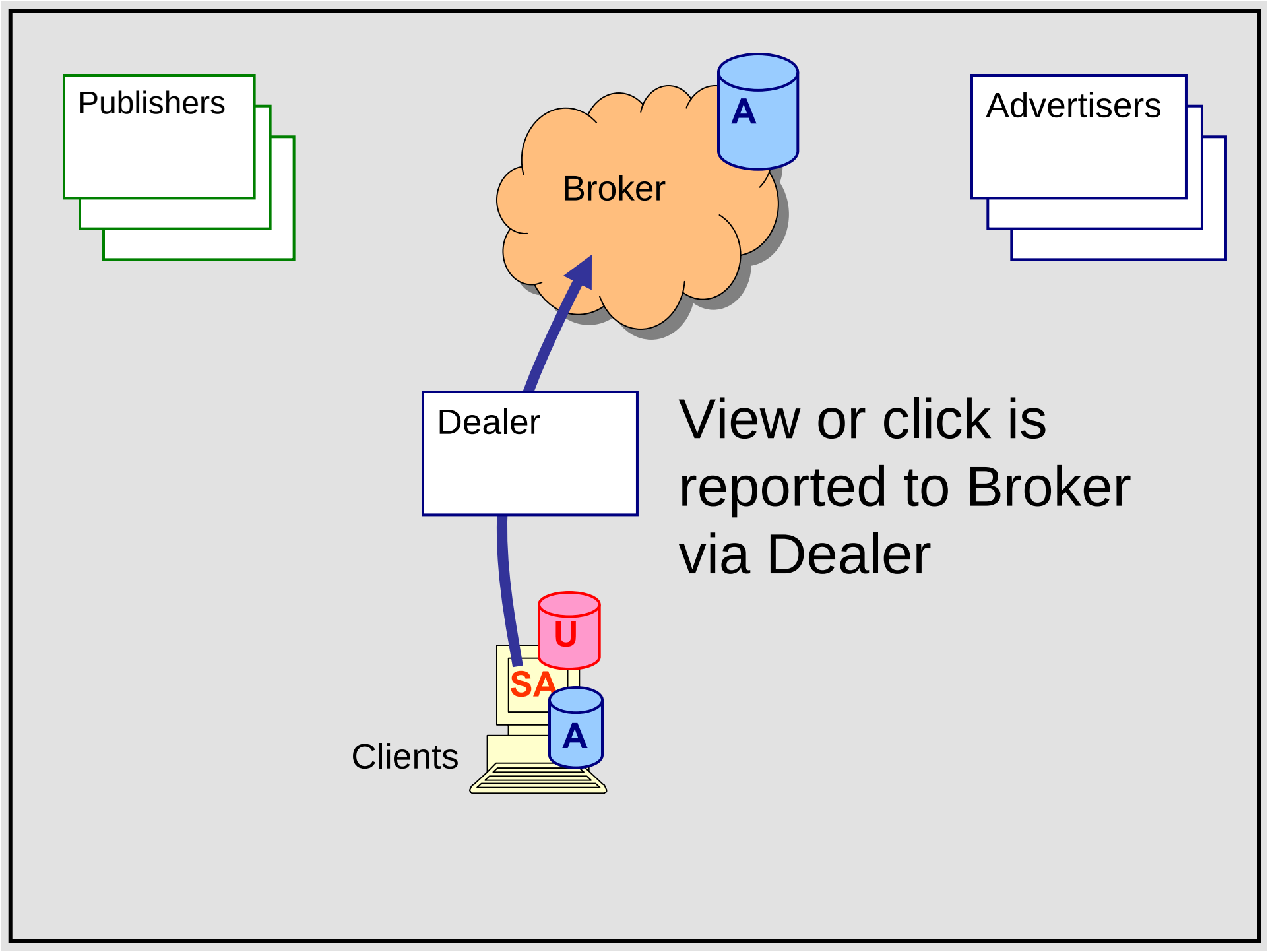
Broker knows *some* Client requests this channel

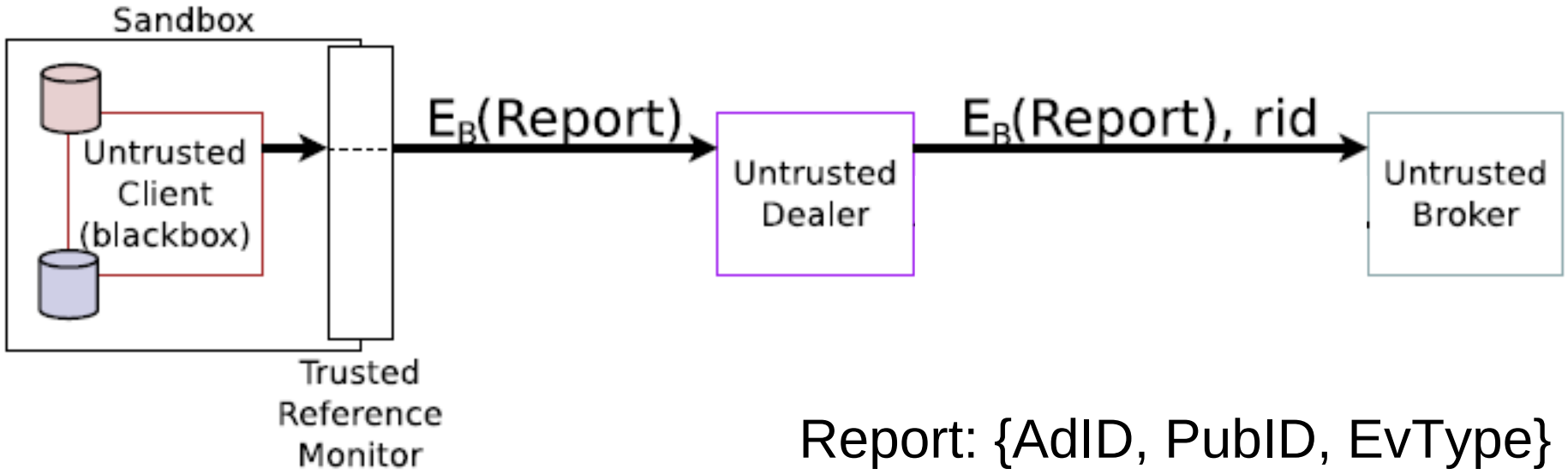
Dealer cannot link requests


Publishers
Broker
A
Advertisers
Dealer
U
SA
A
Clients
Relevant and
non-relevant ads
stored locally


Publishers
A
Broker
Advertisers
Dealer
Webpage
with
adbox
U
SA
A
Clients


Publishers
A
Broker
Advertisers
Dealer
Ad is delivered locally
Minimal delay
IP
SA
A
Clients
May or may not be related to page context


Publishers
Broker
A
Advertisers
Dealer
View or click is reported to Broker via Dealer
U
SA
A
Clients

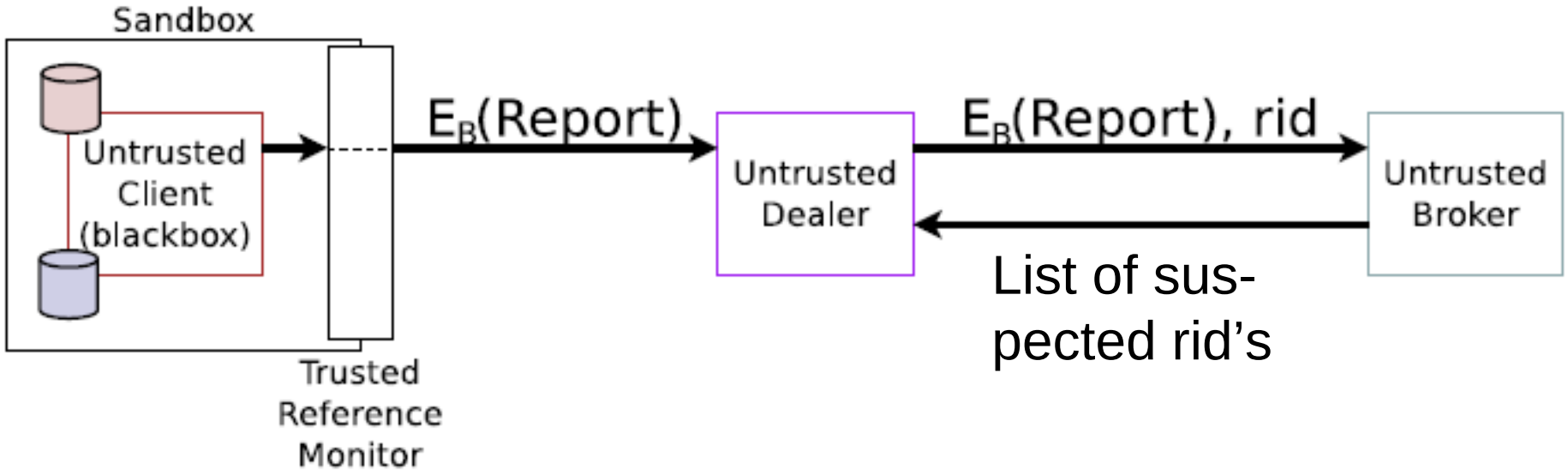


Report: {AdID, PubID, EvType}

Dealer learns client X clicked on *some* ad

Broker learns *some client* clicked on ad Y

At Broker, multiple clicks from same client appear as clicks from multiple clients



rid: Report ID

- Unique for every report

Used to (indirectly) inform Dealer of suspected attacking Clients

- Dealer remembers rid↔Client mappings
- Client with many reported rid's is suspect

Click Fraud

Thresholds: Dealer flags Clients with high subscriptions, clicks, views, CTR

- Forces attacker to use botnet
- Hard to use same botnet for multiple attacks

Blacklists: Dealers use lists of known bots (from antivirus or network telescope). Dealers share list of banned clients

- Limits time that botnet is valid

Click Fraud

Historical Statistics: Broker looks for deviations from normal advertiser or publisher activity

- Use this to flag suspected reports
- Forces gradual attacks

Honey-farms, Charge per action (not clicks), “bait” ads, ...

Crypto Overhead

One public-key operation per view etc.

We can offload these to Clients:

1. Clients create public keys
2. Distribute keys to other Clients (via Broker and Dealers)
3. Encrypted messages delivered back to key-generating Clients for decryption

Other Challenges: Auctions

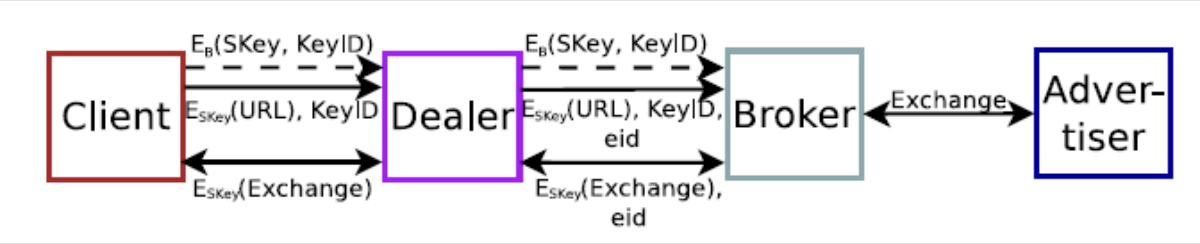
Privad auction is distributed

- Broker has some information (advertiser bid, budget, CTR), Client has other information (user preferences)

Must consider advertiser privacy

- Advertiser doesn’t want to reveal bid, budget, or CTR

Other Challenges: Privacy from advertisers



To an extent, can hide Client from advertiser

- But ultimately user may reveal himself (i.e. through purchase)

Even a view report can reveal information

Must limit level of targeting, and avoid really sensitive advertising

Other Challenges: User Statistics

Broker and advertiser want to know deep *statistical* information about users

- What kind of targeting works best?
- When should ads be shown?
- Are users interested in A also interested in B?
- How can conversion rates be improved?

Centralized systems have full knowledge

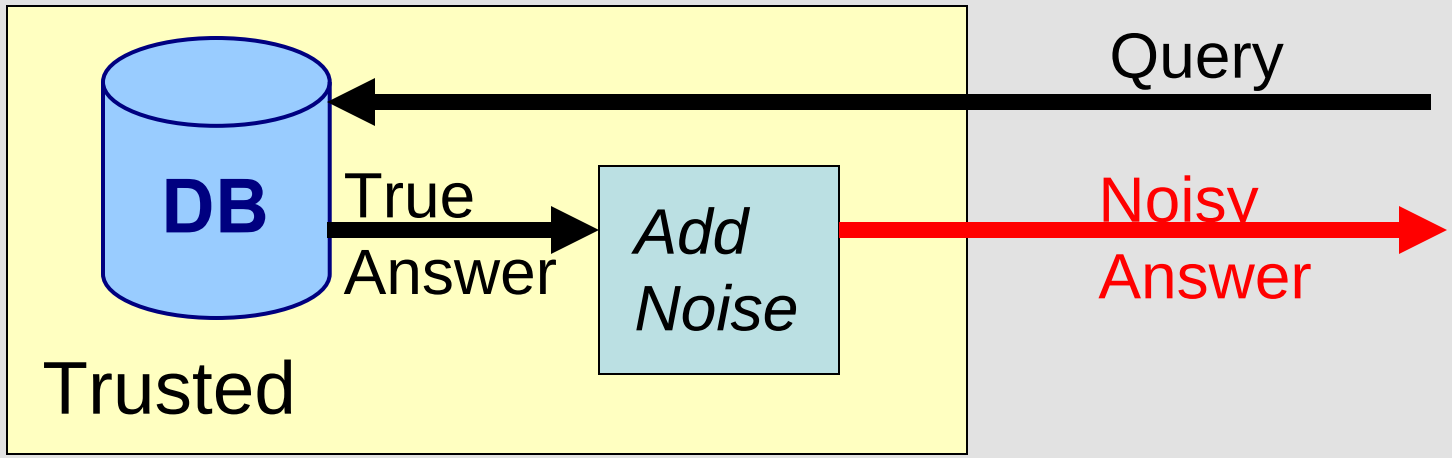
How can Privad privately provide this information?

Differential Privacy

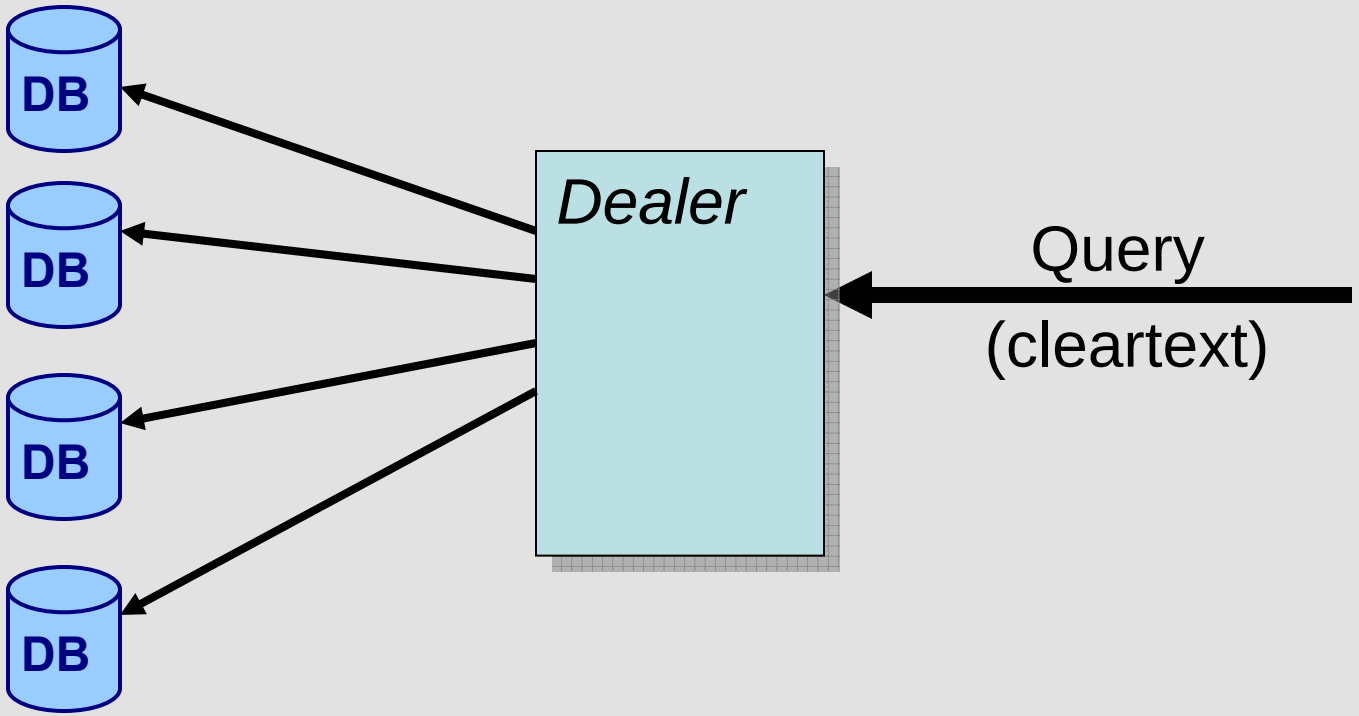
Differential Privacy adds noise to answers of DB queries

Such that presence or absence of single DB element cannot be determined

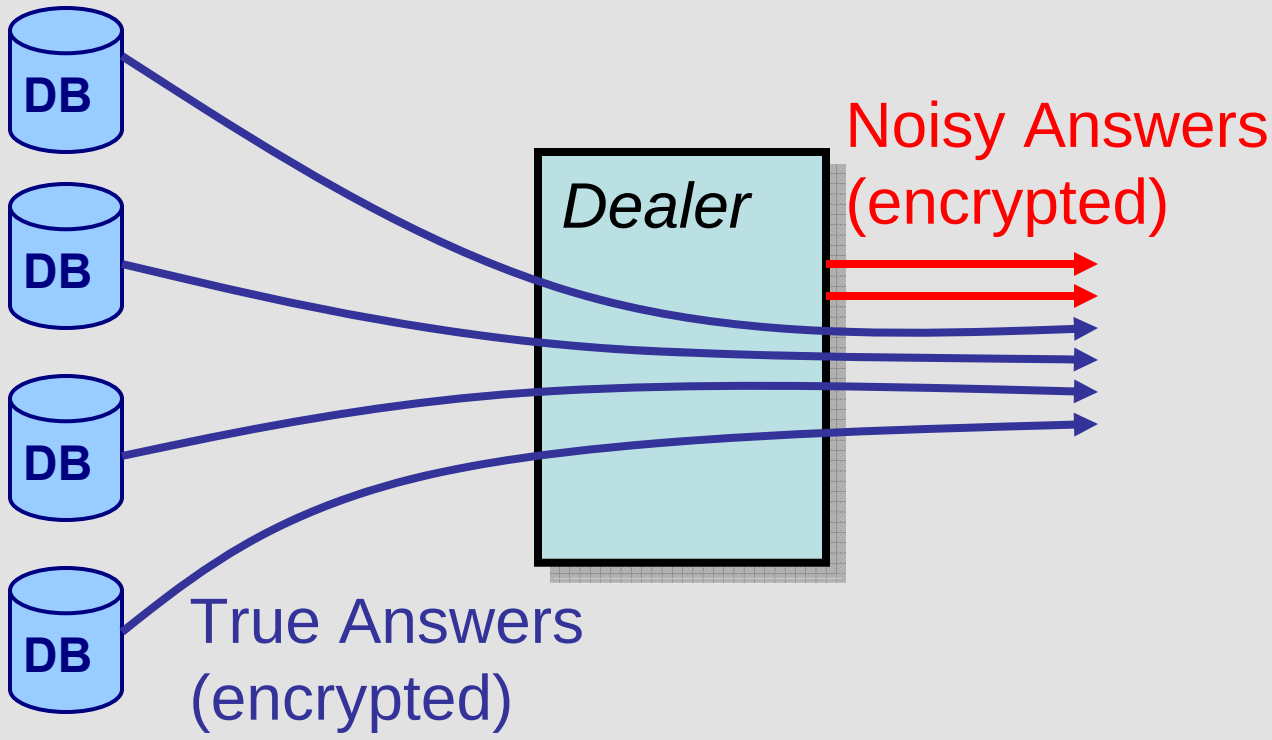
Normally modeled as a single trusted DB



Distributed Differential Privacy



Distributed Differential Privacy



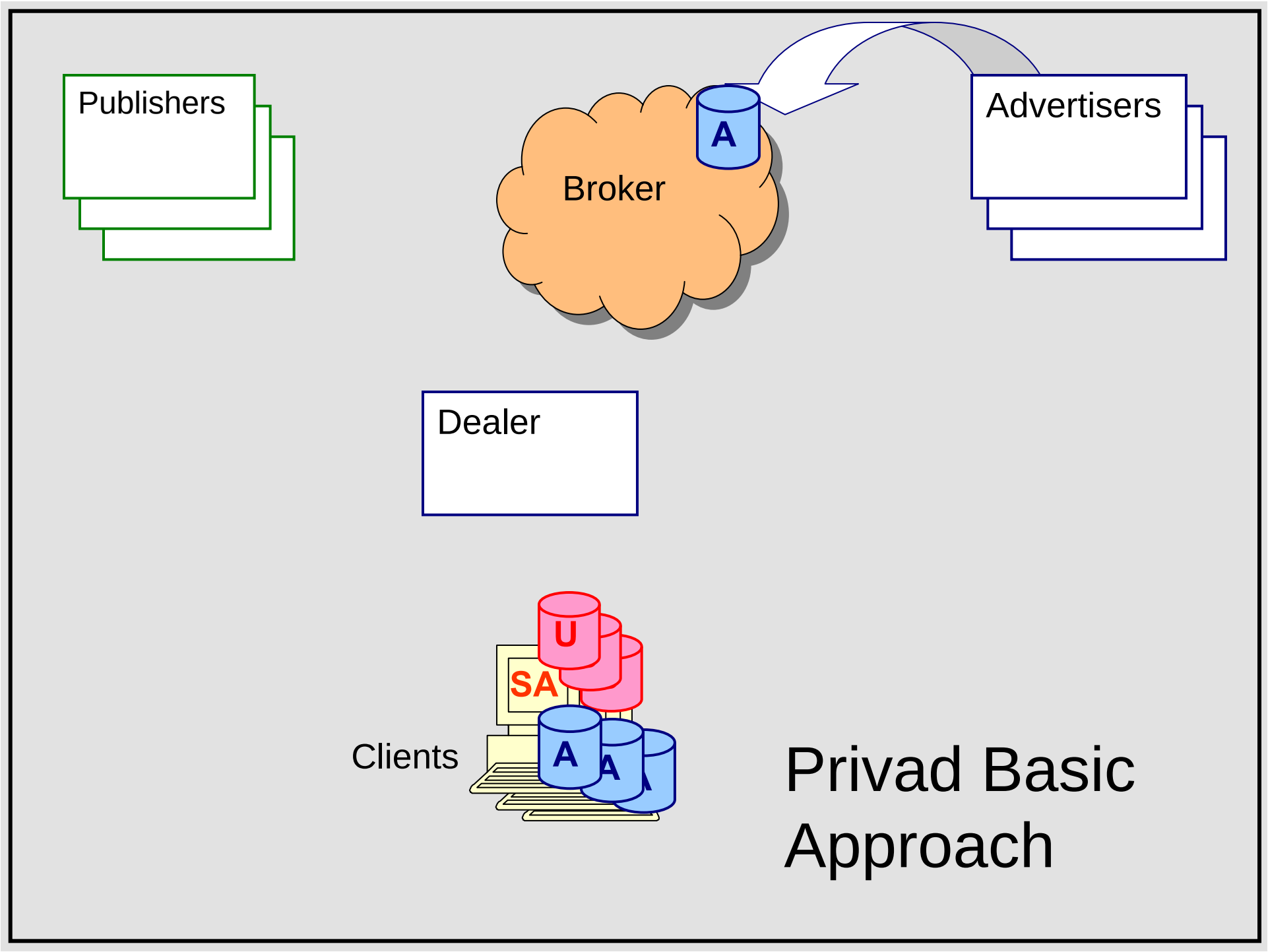
Privad Project Status

Developing large-scale experiment

- 10,000's of Firefox clients
- Ads derived from Amazon product API
- Detect user interest from searching/browsing on shopping web sites
- No user demographics

Hope to show better CTR, scalability

adresearch.mpi-sws.org


Publishers
Broker
A
Advertisers
Dealer
Clients
U
SA
A
A
Privad Basic Approach