Fundamentals of Privacy Engineering II

Riccardo Scandariato
Institute of Software Security, TUHH, Germany
ric***do . scanda***to @ tuhh.de

Master Course “Secure Software Engineering”
Summer Semester 2022 – Lecturer: Nicolás E. Díaz Ferreyra

Learning objectives

- Privacy as Contextual Integrity
- Privacy Impact Assessment (CNIL tool)
- Privacy Attacks using Targeted Ads

What is Privacy?

What is Privacy?

- **"The right to be let alone"** [Warren and Brandeis, 1890]
  - Focus on freedom from intrusion.
- **"Information self-determination"** [Westin, 1968]
  - Focus on control.
- **"The freedom from unreasonable constraints on the construction of one's own identity"** [Agre, 1999]
  - Focus on autonomy.
- **"An individual's right to determine how, when, and to what extent information about the self will be released to another person or to an organization"** [Hung and Cheng, 2009]
  - Focus on control and autonomy.

The landscape of PETs

Privacy is a multifaceted and complex concept.

⇒ Existing PETs rely on **different definitions** of privacy as well on social and technical **assumptions**.

Paradigms of Privacy Technology Research
1. Privacy as control: Technologies that provide means for control over information disclosure (e.g., *privacy settings*, *purpose-based access control*).
2. Privacy as confidentiality: Technologies that aim to create a sphere free from intrusions (e.g., *anonymous communication networks and protocols*).
3. Privacy as practice: It is hard to understand what information is available to others. These technologies aim to increase transparency in information flows (e.g., *P3P, a protocol informing about websites' data-collection practices*).

Violations to privacy?

Google's Street View site raises alarm over privacy

CALUM MacDONALD

Published on 4 Jun 2007

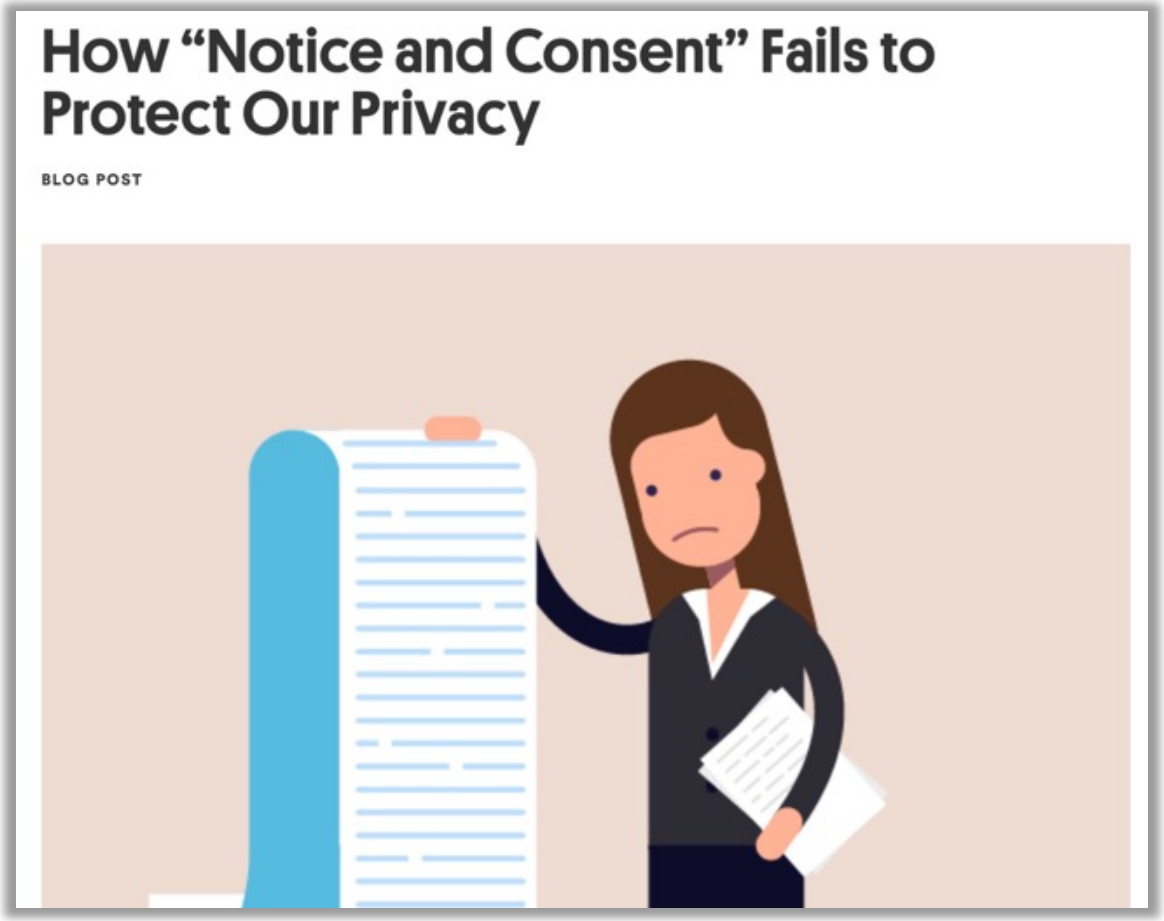
One man is seen picking his nose at a street corner, a couple are caught sunbathing in bikinis and another man is captured entering an adult book store.

- Privacy as **"freedom from intrusions"**
  ⇒ Imposes a public-private dichotomy.
  ✗ Intrusions in a public space?
- Privacy as **"information self-determination"**
  ⇒ Enhances control over personal information.
  ✗ Notice and consent?

Do these approaches **suffice** to analyze the **privacy implications** of socio-technical systems?

Violations to privacy?

Violations to privacy?



https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/

Privacy as Contextual Integrity

Current legislation is often grounded in traditional (and often narrow) views on people's privacy:

- Disruptive technologies have challenged the boundaries of privacy.
- Plenty of "legal vacuums" around privacy.

Contextual Integrity provides a framework to analyze the privacy implications of socio-technical systems by means of two core concepts:

1. Appropriateness: Privacy is about appropriate flow of information.
   - It conforms with *legitimate* norms/rules (they are worth defending and are morally justifiable).
2. Flow of information: Appropriate exchange of private information **depends on the context** in which such exchange is being conducted.

Privacy as Contextual Integrity

The exchange of personal data is at the core of any social interaction.

- Privacy is not about NOT SHARING personal data!

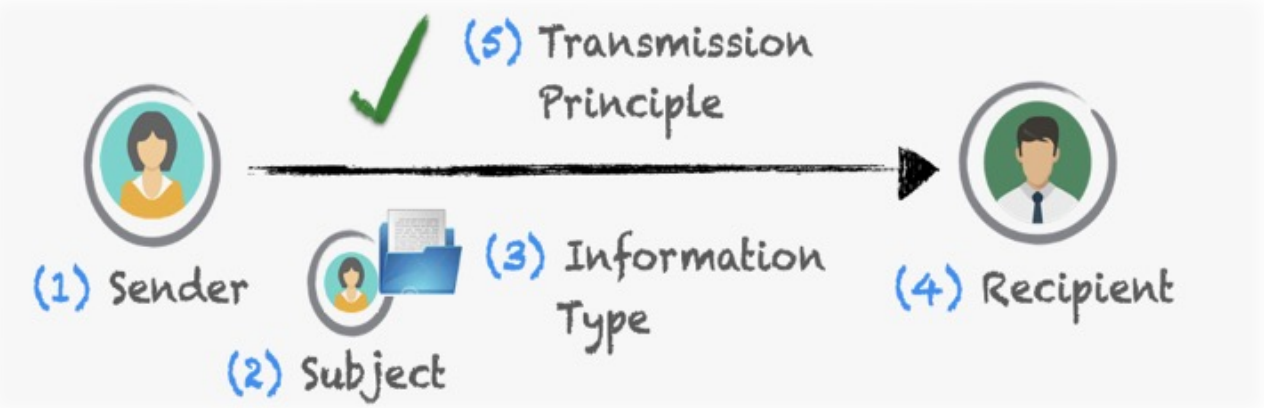
Any **social context** (work, healthcare) defines – more or less explicitly – a **social norm** (i.e., an appropriate behavior that is to be expected)

⇒ Contextual Integrity gives a framework to reason about the norms that apply, in a given social context, to the flows of personal data.

"In a context, the flow of information of a certain type about a subject (acting in a particular capacity/role) from one actor (could be the subject) to another actor (in a particular capacity/role) is governed by a particular transmission principle" [Nissenbaum, 2004]

The CI Tuple: 5 Parameters

- **Actors (*sender*, *subject*, *recipient*):** Physician, bank, merchant, police, advertiser, FBI, CIA, mother, spouse, neighbor, friend, student, …
- **Information type**: Age, gender, salary, address, medical diagnosis, …
- **Transmission principle**: Consent, coerce, compel, steal, buy, sell, in confidence, with notice, with a warrant, with authorization, …
  - *Constraint under which the information should flow!!*



Examples

- In a job interview, a recruiter **[REC]** is forbidden from asking **[TP]** about a candidate's **[SEN, SUB]** religious affiliation **[IT]**.
- Travelers **[SEN, SUB]** are obliged to show **[TP]** their vaccination status **[IT]** to the cabin crew **[REC]** upon request **[TP]**.
- A citizen of the U.S. **[SEN, SUB]** is obliged to reveal **[TP]** gross annual income **[IT]** to the Internal Revenue Service **[REC]**, under conditions of confidentiality except as required by law **[TP]**.
- Parents **[REC]** should monitor **[TP]** their children's **[SUB]** academic performance **[IT]** with or without the child's consent **[TP]**.

Contextual Integrity: Implications

Contextual Integrity **holds** when context-relative informational norms are respected, and it is and **violated** when they are breached.

- When people claim their privacy is being violated, then look for Contextual Integrity violations!
- Privacy is not about secrecy, but appropriate information flows.

Privacy Impact Assessment (PIA)

GDPR - Article 35: *"Where a **type of processing** in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to **result in a high risk to the rights and freedoms of natural persons,** the **controller** shall, prior to the processing, carry out an **assessment of the impact of the envisaged processing operations** on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks".*

PIA Goals and Objectives

An iterative methodology, which should guarantee a **reasoned**, **reliable use of personal data** during processing:

- ✓ To ensure that data handling conforms to applicable legal, regulatory, and policy requirements (compliance).
- ✓ To determine the risks and effects of *collecting*, *storing*, and *disseminating* information in a particular system.
- ✓ To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
- ✓ Performed in principle by a **data controller** to build and demonstrate the implementation of privacy protection principles.

Data Processors and Controllers

⇒ **Data Controller**: Determines the *purposes* for which and the *means* by which personal data is processed.

⇒ **Data Processor**: Processes personal data only *on behalf* of the controller. It is usually a 3rd party external to the company.

Example: A brewery has many employees. It signs a contract with a payroll company to pay the wages. The brewery tells the payroll company when the wages should be paid, when an employee leaves or has a pay rise, and provides all other details for the salary slip and payment. The payroll company provides the IT system and stores the employees' data. The brewery is the data controller, and the payroll company is the data processor.

PIA Methodologies

- ISO standard for conducting PIAs: ISO 29134
- Vast majority of PIAs in the industry: home-cooked templates.
- Some of methodologies/tools supporting PIAs:
  - LINDDUN (KU Leuven)
  - CNILs PIA Framework ☺

CNIL: How is a PIA carried out?

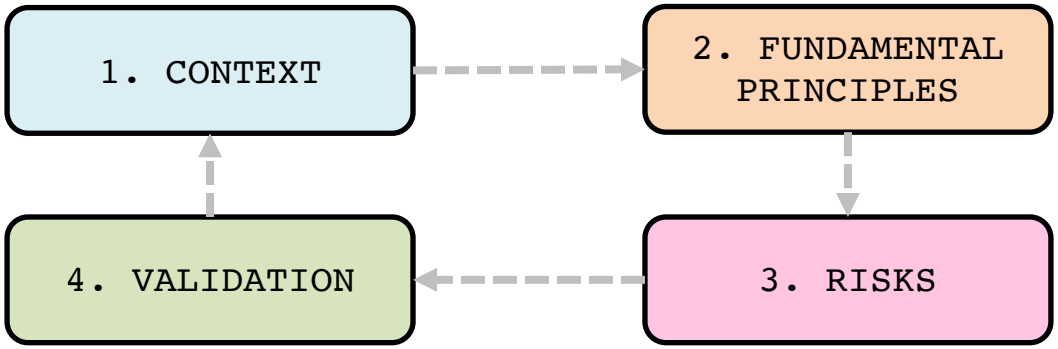
Compliance approach of a PIA is based on two pillars:

i. **Fundamental rights and principles**, which are "non-negotiable", established by law and which must be respected, regardless of the nature, severity and likelihood of risks (e.g., *limited storage duration*; *right of access*, *to object*, *rectification and erasure*).

ii. **Management of data subjects' privacy risks**, which determines the appropriate technical and organizational controls to protect personal data.

How is a PIA carried out?

1. *Define the context of the processing of personal data under consideration.*
2. *Analyze the controls guaranteeing compliance with the fundamental principles.*
3. *Assess privacy risks associated with data security and ensure they are treated.*
4. *Document the validation of the PIA in view of the previous facts to hand or decide to revise the previous steps.*



The approach should be implemented **as soon as a new processing** of personal data is designed

1. Study of the context

- Present a **brief outline** of the processing under consideration, its nature, scope, context, purposes and stakes:
  - *"What are the expected benefits (for the organization, for the data subjects, for society in general, etc.)?"*
  - The *personal data* concerned, their *recipients* and *storage durations*.
  - Describe the whole life cycle: From *collection* to *erasure*.
- Identify the **data controller** and any **processors**.
- List the **references applicable** to the processing, which are necessary or must be compiled with (e.g., specific GDPR Articles).

Generally carried out by the project owner[6], with the help of a person in charge of "Data protection" aspects[7].

Aim: gain a clear overview of the personal data processing operations under consideration.

2. Study of the fundamental principles

(i) Explain and justify the necessity of processing personal data:

- purpose(s): specified, explicit and legitimate (GDPR Art. 5.1-b).
- basis: *lawfulness* of processing, prohibition of misuse (GDPR Art. 6).
  - ✓ Consent: the individual has given clear consent for you to process their personal data for a *specific purpose*.
  - ✓ Vital interests: the processing is necessary to protect someone's life.
  - ✓ Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- data minimization: adequate, relevant and limited (GDPR Art. 5-c).
- quality of data: accurate and kept up-to-date (GDPR Art. 5-d).
- storage periods: limited (GDPR Art. 5-e).

2. Study of the fundamental principles

(ii) Select and describe controls to comply with the following **requirements**:

- Inform data subjects – fair/transparent processing (Articles 12, 13, 14).
- Obtain **explicit** and **unambiguous** consent (Articles 7, 8).
  - Explicit: The subject must explicitly agree to the processing of her *sensitive data* (Article 9). It is obtained through a statement.
  - Unambiguous: Consent for regular, non-sensitive personal data doesn't necessarily need to be explicit (e.g., providing your e-mail address to receive advertisement → no need for "I Consent").
- Guarantee the right of **access and data portability** (Articles 15, 20).
- Guarantee the rights to **rectification and erasure** (Article 16, 17).

Objective: build the system that ensures compliance with privacy protection principles.

3. Study of the risks

(i) Assessment of existing or planned controls: Gain a good understanding of the controls that contribute to *security*:

- Identify or determine the existing or planned controls.
- Check that improving each control is either not necessary or not possible.
- If applicable, review or propose additional controls.

(ii) Risk assessment: Gain a good understanding of the causes (potential privacy breaches) and consequences of risks.

i. For each feared event (*illegitimate access to personal data*, *unwanted change of personal data*, and *disappearance of personal data*):

   ⇒ (1) determine potential impacts, (2) estimate its severity, (3) identify the threats, and (4) estimate its likelihood.

ii. Determine whether the risks identified in this way can be **considered acceptable** in view of the existing or planned controls.

4. Validation of the PIA

1. Consolidate and present the study's findings:

- Visually present of the controls selected to (i) ensure compliance with the **fundamental principles**, (ii) contribute to **data security**.
- Visually map the **risks** (*initial* and *residual* where applicable).
- Outline an **action plan** for the additional controls identified in the previous steps (person responsible for their implementation, costs, and timeframe).

2. Formally document the consideration of stakeholders.
3. Decide whether the controls, residual risks and action plan are acceptable.

   ⇒ The PIA may be **validated**, **conditional on improvement**, or **refused**.

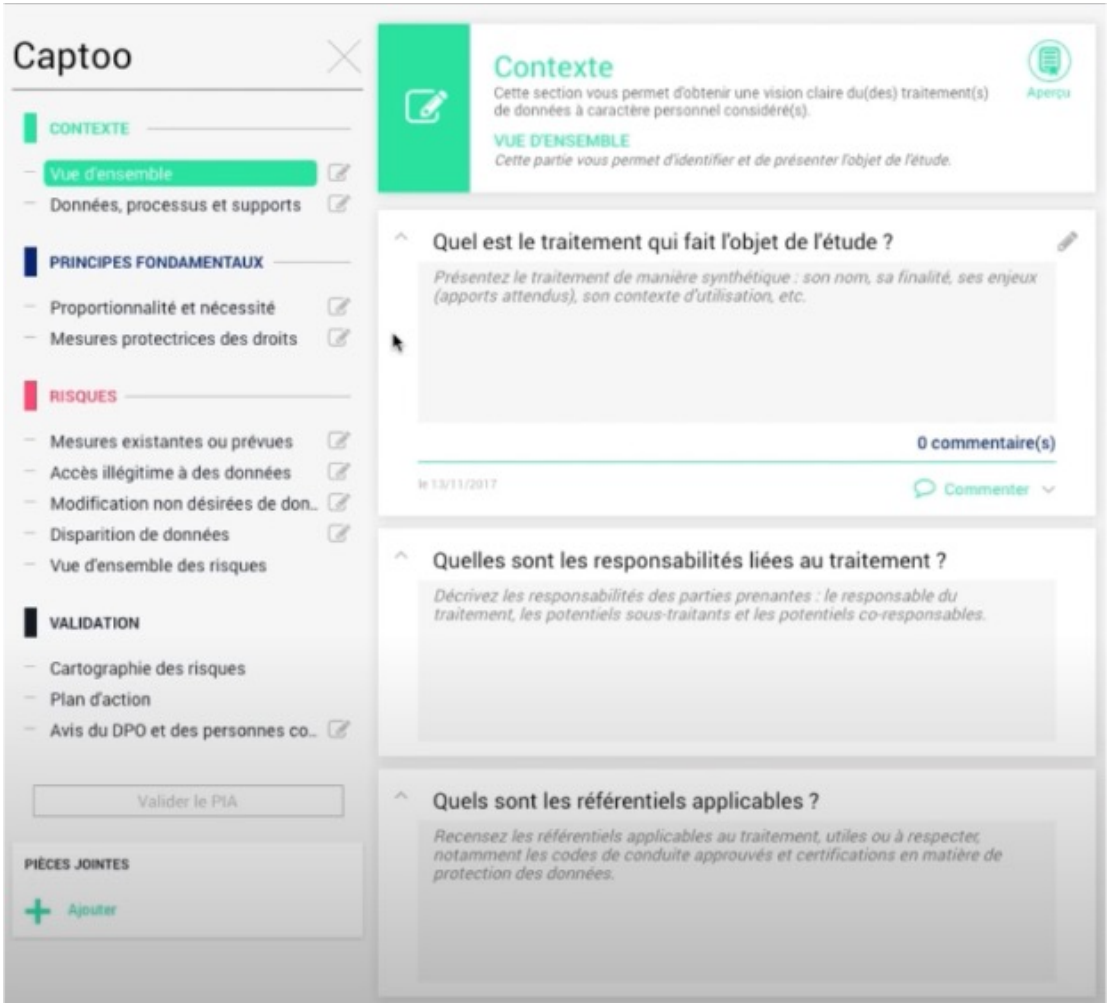
4. If necessary, repeat the previous steps so that the PIA can be validated.

CNIL Tool

Create new PIA

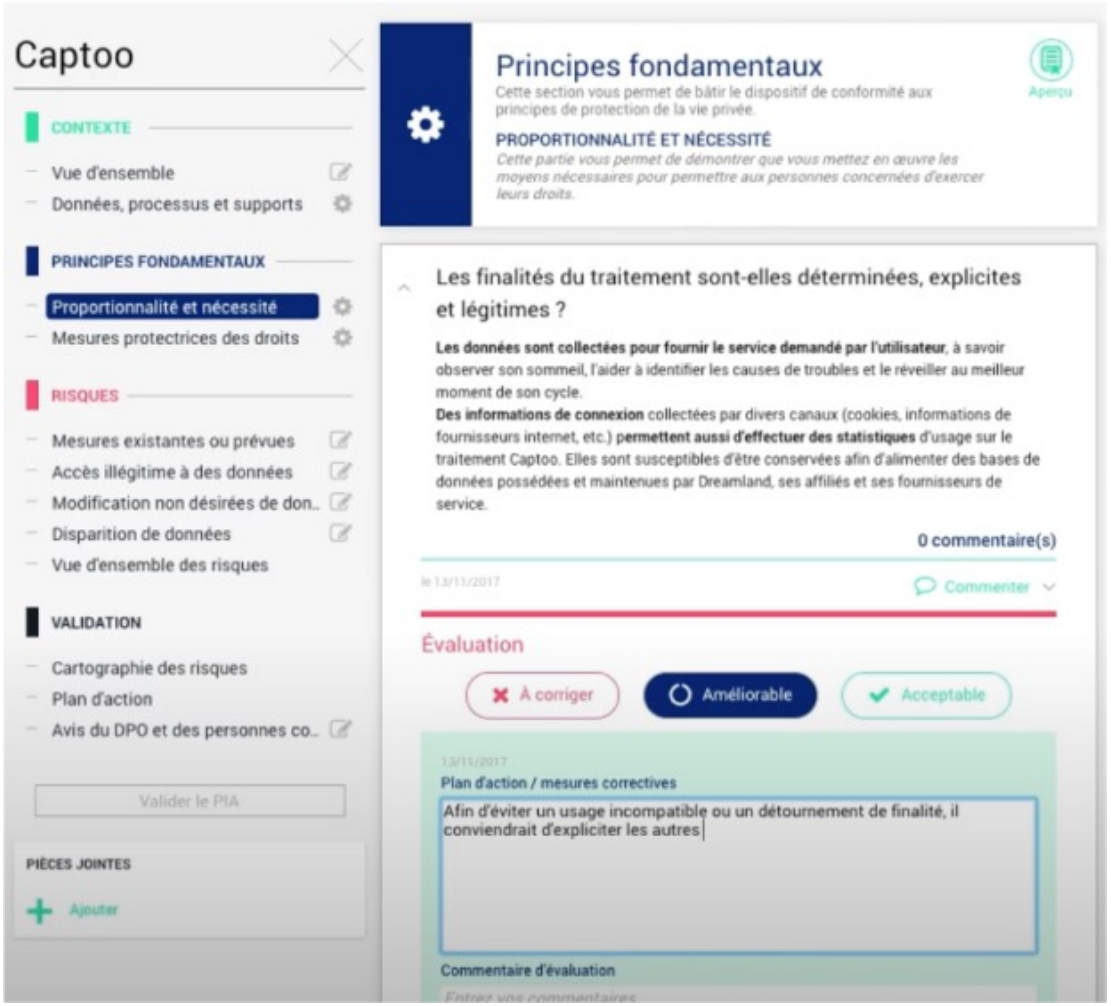
CNIL Tool

Update the PIA

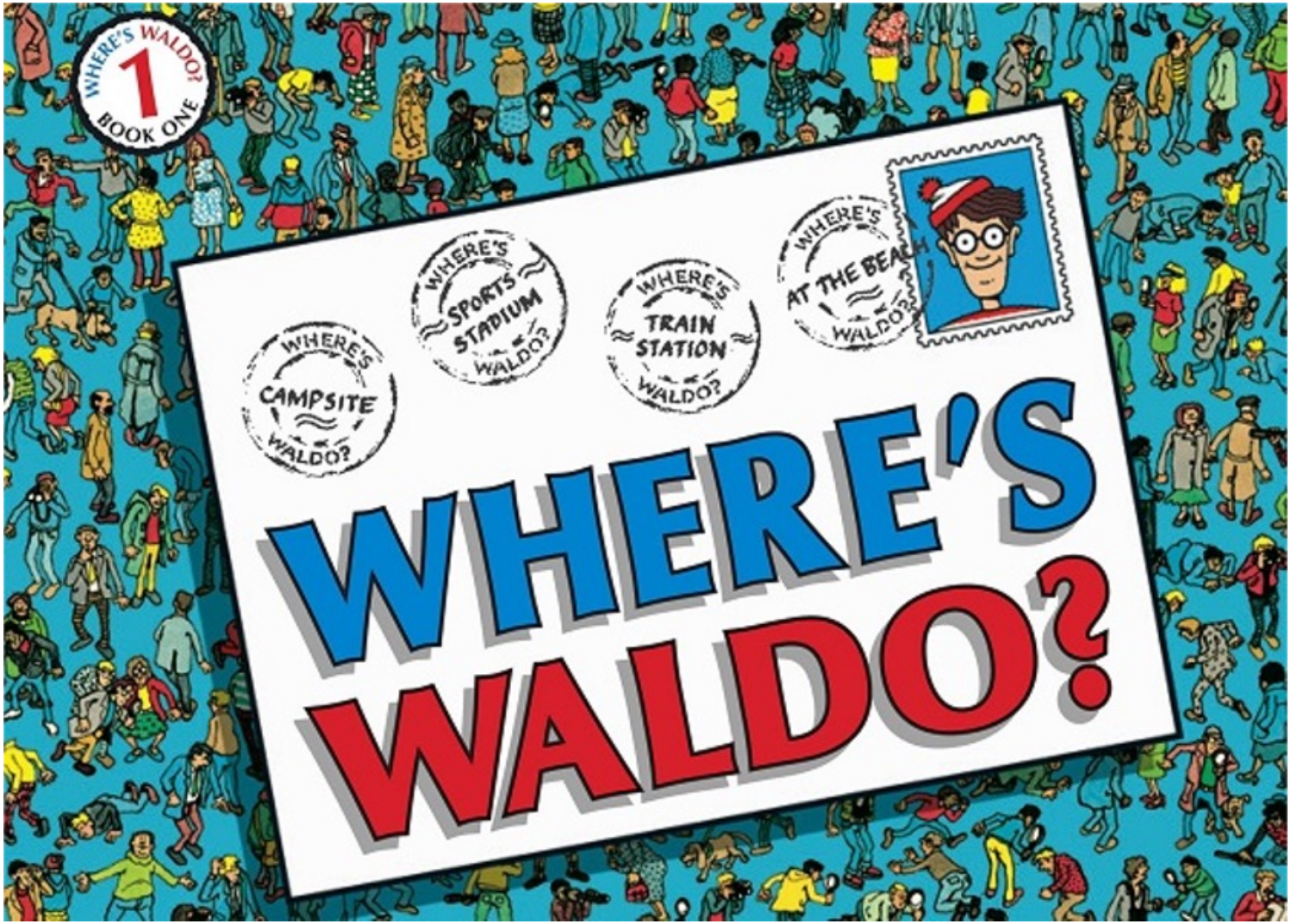


CNIL Tool

Evaluate the PIA



Privacy Attacks
Using Targeted Advertising


WHERE'S WALDO?
1
BOOK ONE
WHERE'S CAMPSITE WALDO?
WHERE'S SPORTS STADIUM WALDO?
WHERE'S TRAIN STATION WALDO?
WHERE'S AT THE BEACH WALDO?
WHERE'S WALDO?

Finding Waldo can take a very long time...

Targeted Advertisement: Ubiquity

Over the last decades, online advertisements (a.k.a “ads”) have become more and more **ubiquitous** and **personalized**

Targeted Advertisement: Ubiquity

Targeted Advertising (TA) is currently the most effective and profitable form of online marketing:

⇒ Allows to deliver personalized ads by effectively *selecting* and *directing* information to the right potential customers.

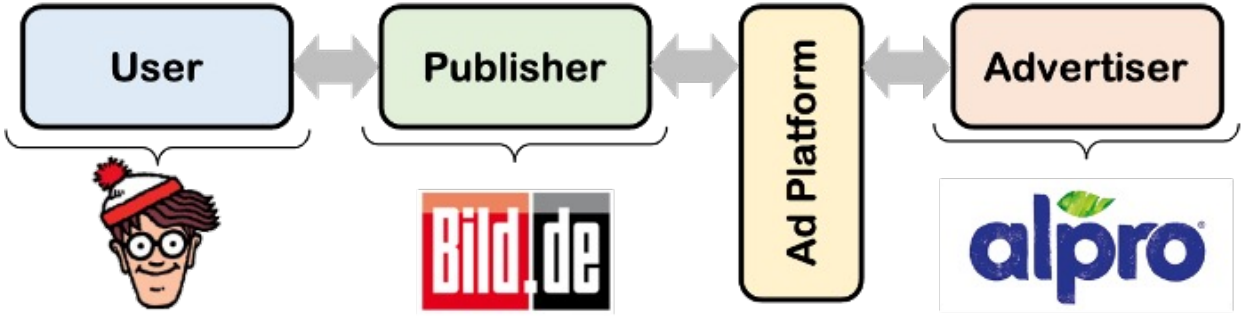
TA relies on an intricate structure composed by a variety of **intermediary entities** and **technologies**

Online Advertising Ecosystem

⇒ **Advertiser:** Entities interested in promoting a brand or a product through targeted ads and are willing to pay for it.

⇒ **Publisher:** Entities which provide online content through a webpage (e.g., blogs, newspapers, search engines).

⇒ **Ad Platform:** Group of entities that connect advertisers with publishers through their demand and supply-side interfaces.



Overall, there are two main technological solutions for Ad Platforms:
Ad Networks and **Ad Exchanges**

Ad Networks

Ad Networks were the most traditional approach in the early days:

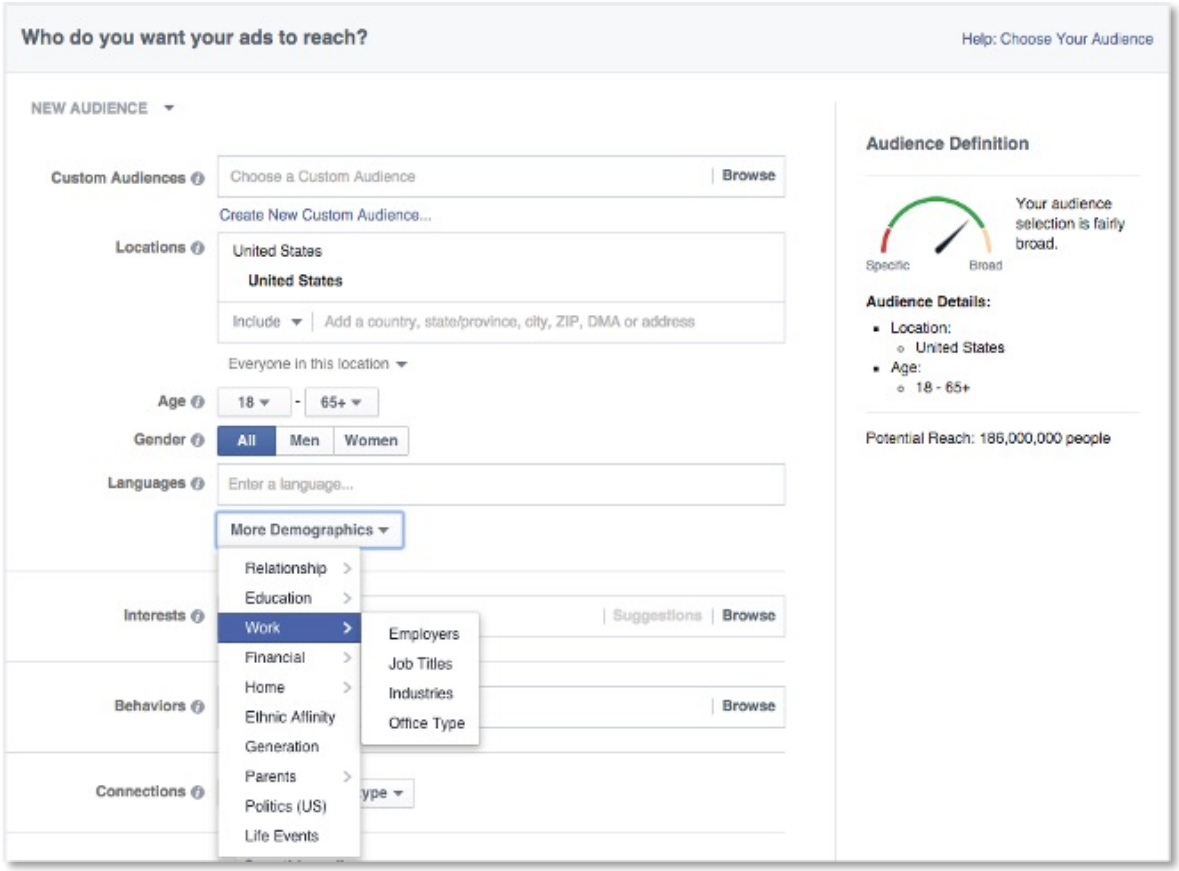
- Act as a **middleman** between publishers and advertisers.
- Collect and aggregate publishers' **inventory** (i.e., space for displaying ads) into **audience segments**.
- Advertisers can set-up campaigns for specific **market segments** (e.g., automotive, fashion).

⇒ Cost per Mille (**CPM**): Inventory is sold per blocks of 1000 **impressions** (views of ads).

⇒ Cost per Click (**CPC**): Advertisers pay a small fee when a user clicks their ad.

Advertisers can only buy impressions from a **limited** and **selected** number of publishers (price not transparent).

Ad Networks



Some Ad Platforms still incorporate Ad Network features (e.g., Facebook Ads).

Ad Exchanges

Over time, Ad Networks have *evolved* into Ad Exchanges:

- Follow an auction-based approach where publishers and advertisers transact impressions in **real time**.

⇒ Real Time Bidding (RTB):

✓ Advertisers bid on **individual impressions** (not inventories) based on users' *behavioural data* and *contextual information*.

✓ Bids are set based on the **amount of information** an advertiser has on a particular user (more information, higher the bid).

✓ The **winner** of the auction is allowed to display an ad to that user.

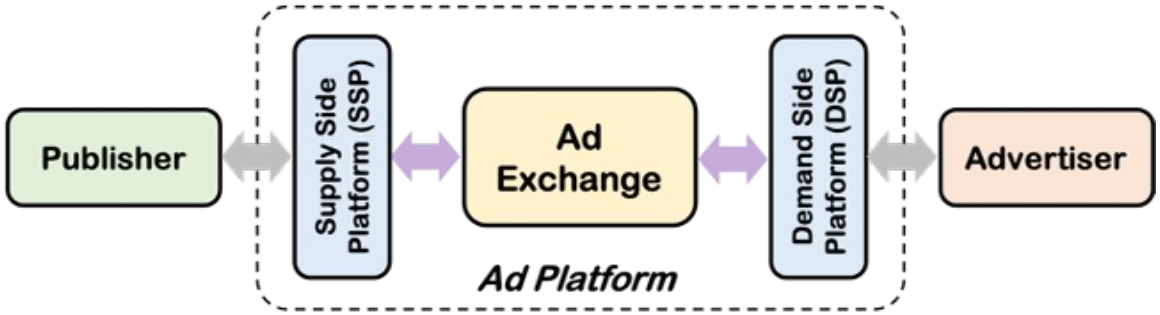
Advertisers can buy impressions from **the whole Internet**. The price is given by the **competition** in the market (more transparent)

Demand and Supply Side Platforms

Publishers and advertisers rarely interact with Ad Exchanges directly:

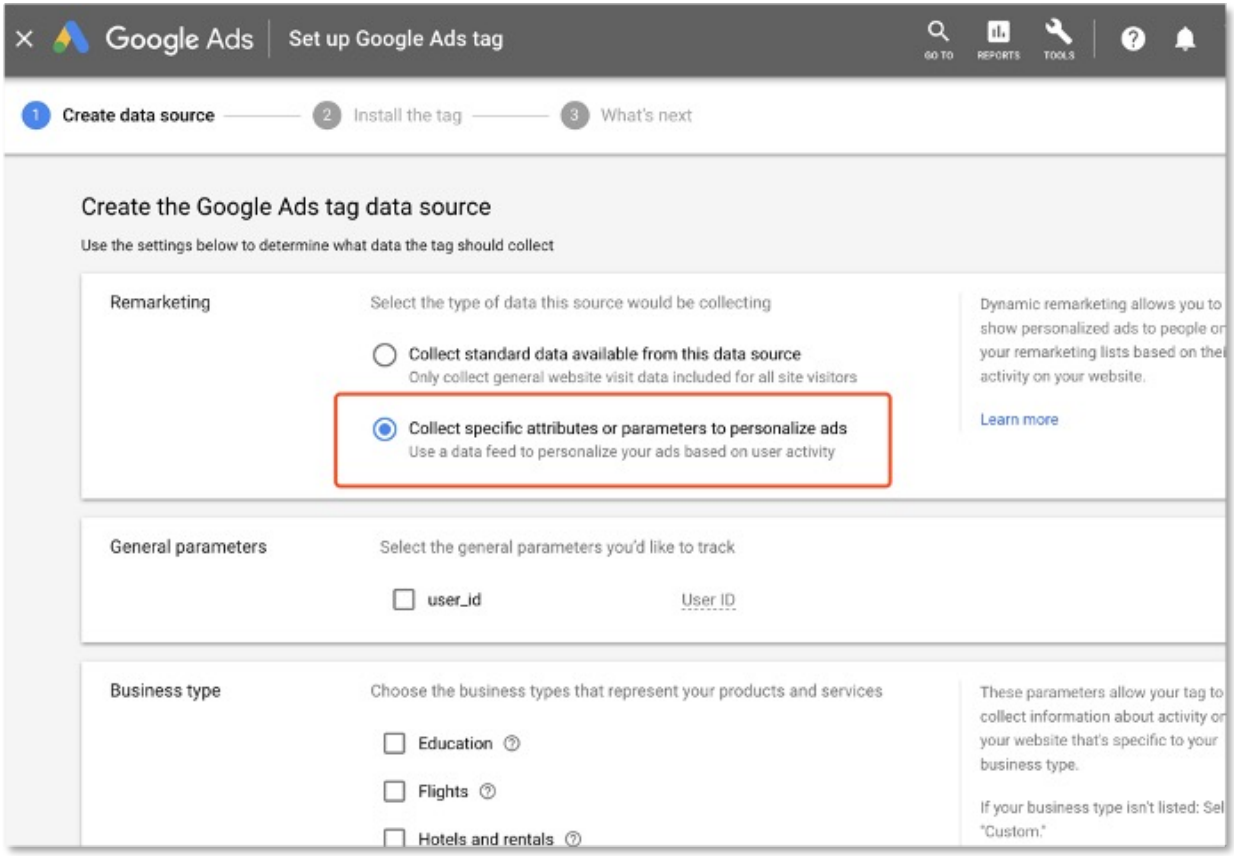
- Demand-Side Platforms (**DSP**): Work on behalf of advertisers by optimizing the process of buying impressions.
- Supply-Side Platforms (**SSP**): Work on behalf of publishers by coordinating, managing and distributing their ads inventory.

⇒ Both, DSPs and SSPs, can operate with different Ad Exchanges.



The line between DSPs, SSPs, and Ad Exchanges has become blur over the years (e.g., Google AdWords and Google AdSense)

Ad Exchanges



Targeted advertisement is delivered to Internet users thanks to a process called **Cookie Matching/Syncing**

1st and 3rd Party Cookies

Cookies are randomly generated strings of text used by web servers to **recognize users** in subsequent visits:

- Can contain a wide range of information including personal data.
- 1st-Party Cookies: Created by the domains a user **directly visits** to deliver a customized experience (e.g., preferred language).
- 3rd-Party Cookies: Created by a domain **different** than the one the user is visiting (e.g., a DSP) mainly for tracking purposes.

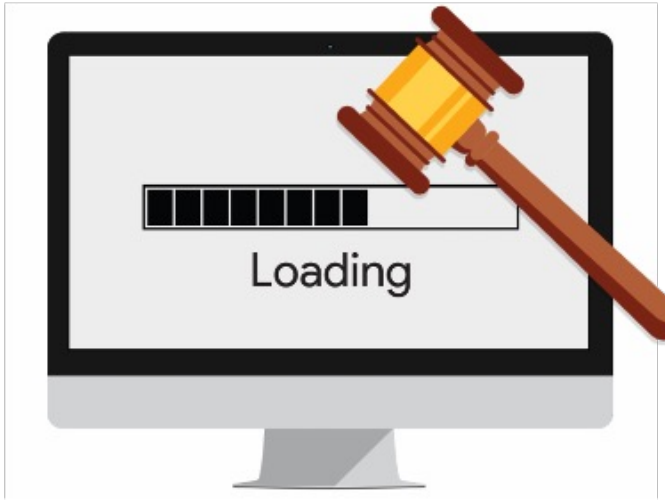
Cookies are **domain specific** and can only be accessed by the domain who created them ⇒ **Same-Origin Policy**

Cookie Matching

When the user enters the publisher's website, the website **automatically calls** the **Ad Exchange**:

⇒ Ad Exchange drops a 3rd-Party cookie on the user's browser.

⇒ The Ad Exchange puts the user's impression to **auction**.



The auction process takes a fraction of a second!!

Cookie Matching

During an auction, the Ad Exchange sends **their cookie** (user id + contextual information) to the prospective bidders/DSPs:

✗ Since bidders have no direct access to the website, they **cannot read** their own cookies before winning the auction (in theory).

✗ The cookieID of the Ad Exchange is **different** from the one of DSPs, and therefore they cannot parse it (*different domains!*).

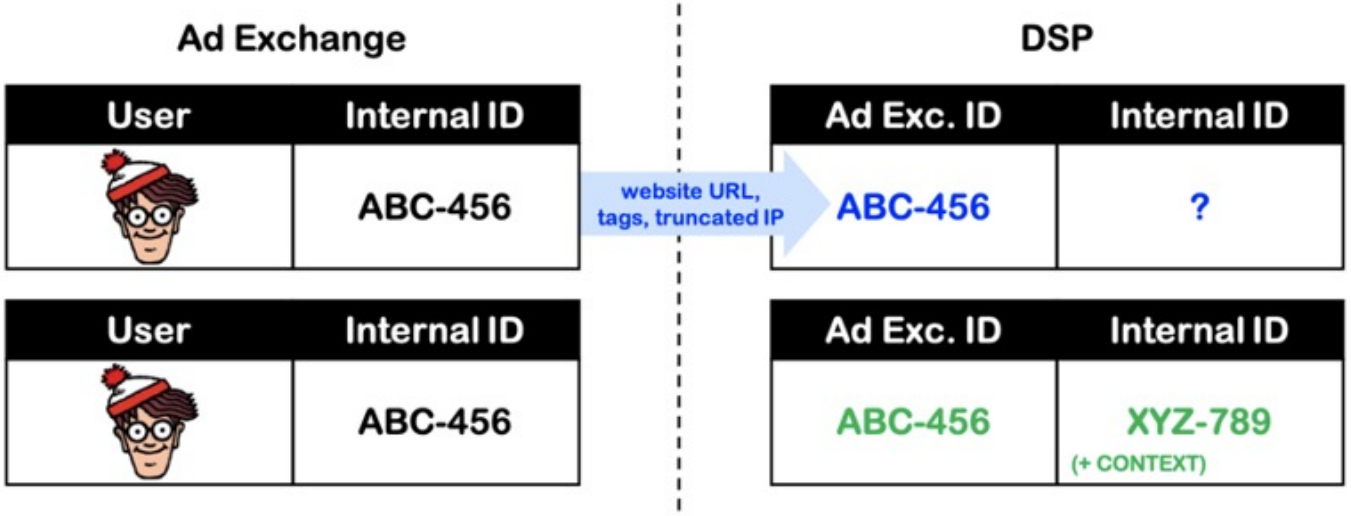
⇒ How can a DSP determine if this is a **known user** and bid higher?

User	Ad Exchange	DSP
	ABC-456	XYZ-789

A **Cookie Matching Table** allows bidders and Ad Exchanges to **match the identifiers** (cookies) they have about a single user.

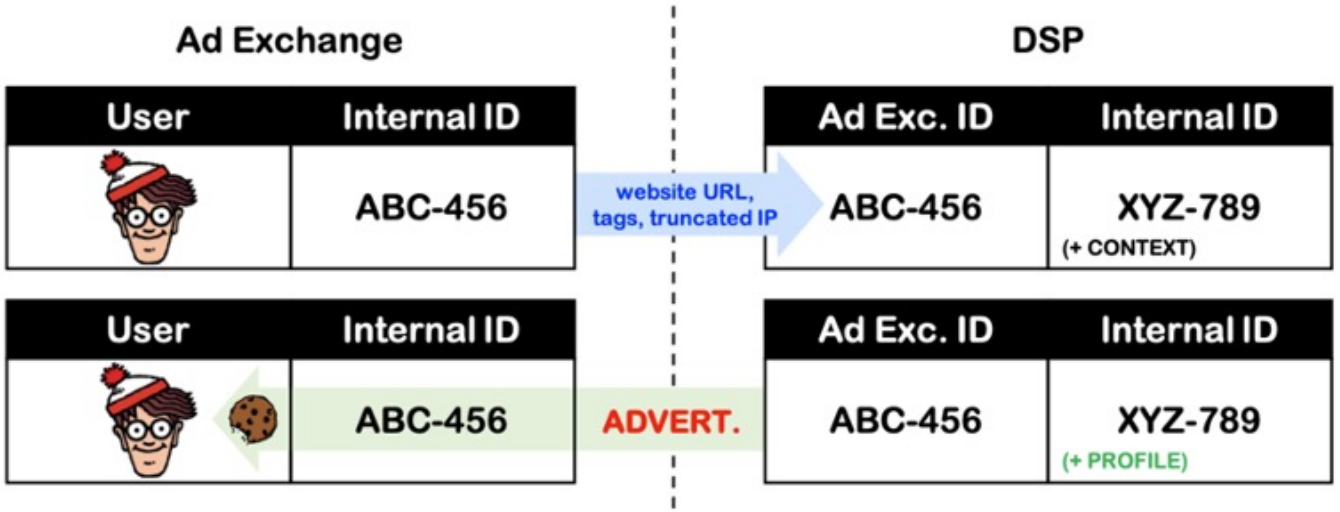
Cookie Matching: Unknown User

1. The Ad Exchange sends the cookie id=**ABC-456** to the DSP along some contextual information (e.g., website URL).
2. There is **no prior registry** of user ABC-456 at the DSP ⇒ The DSP creates their own id=**XYZ-789** for ACB-456.
3. The bid is low, so the DSP **loses the auction** and cannot store their cookie on the client's side.

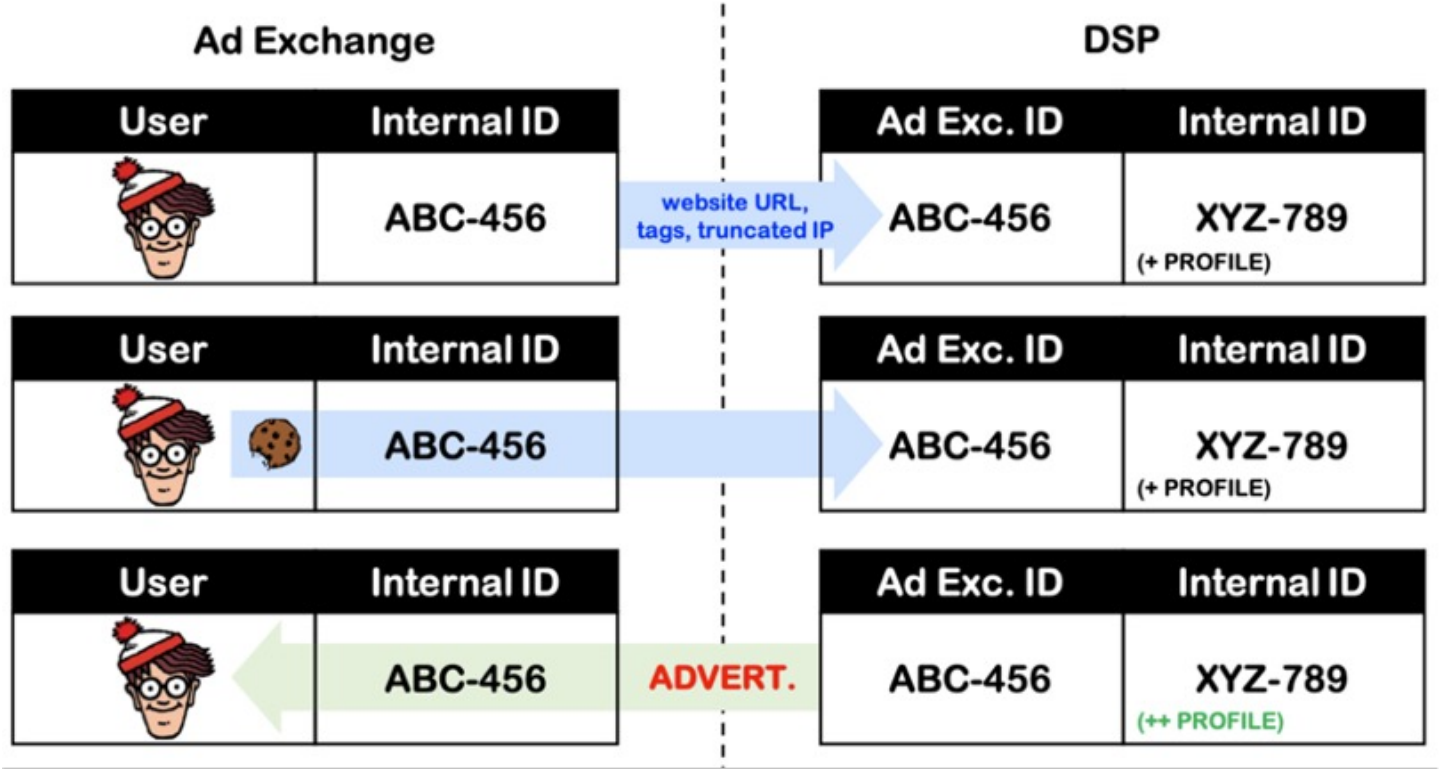


Cookie Matching: Create Cookie

1. The Ad Exchange sends the cookie id=**ABC-456** to the DSP along some contextual information (e.g., website URL).
2. There is an **internal ID** and contextual information for user ABC-456 at the DSP ⇒ The DSP **bids higher**
3. The DSP **wins the auction** and stores their cookie on the client's side (her browser) ⇒ **The DSP can start tracking!**



Cookie Matching: Existing Cookie



By showing more ads to the user, the DSP also gathers more information for **tracking** and **profiling**.

Privacy Threats

The current approach to targeted advertising can certainly posit **threats** to people's privacy:

- ✗ All entities with access to user data can be considered as **potential attackers** (e.g., SSP, DSP, Ad Exchanges).
- ✗ Private information can be **leaked** and **misused** at different stages of the ad targeting process (e.g., during RTB).

⇒ An attacker could infer *sensitive information* about the user such as her *political affiliation, sexual orientation, religion, and race*.

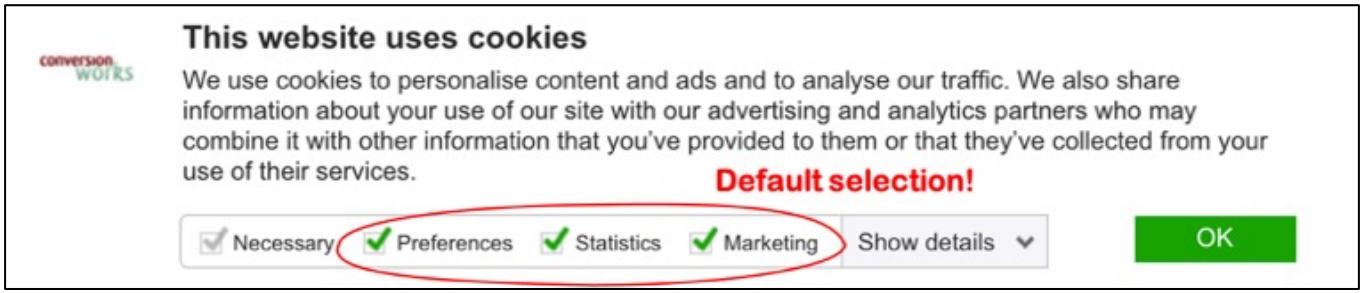
⇒ Such information be used against her and lead to **unjustified discrimination** and **targeted surveillance** scenarios, among others.

What can we do as users to protect our privacy online?

Countermeasures

In principle, users could protect themselves by systematically **deleting 3rd-party cookies** and using **ad-blocking software**:

- Users often **lack awareness** (risks are not evident) ⇒ won't take action.
- Some of them lack **technical knowledge** to understand the logic behind protection mechanisms (“why delete cookies?”).
- More pervasive tracking mechanisms such as **flash cookies** and **fingerprinting** can impair users’ privacy-protection efforts.



March ’18: **GDPR gets effective** ⇒ trackers must ask for consent!

Dark Patterns

Developers' decisions about defaults can have implications for users' privacy:

- People **rarely change** default configurations (status quo bias).
- Developers also tend to keep defaults and standards set by large tech companies **without reflecting** much on the consequences.

> Technological designs that leverage human biases for deceptive purposes are referred as **dark patterns**

⇒ The use of dark patterns should be discouraged among developers!

*"Machines themselves are **empty gloves** into which a **hand**, either cold and excessively bony, or warm, full-fleshed, and gentle, can be inserted. The hand is always the **hand of man**, and the hand of man can be **good or evil**, while the **gloves** themselves **remain amoral**."* Ray Bradbury (1953).

Questions ?