# Ad Tech: How to Manage Compliance in a New First Party (or NO) Cookie World

*Julia Shullman, General Councel and Chief Privacy Officer, TripleLift*
*Fiyinfoluwa Adeleke, Assistant General Counsel, Yahoo*
*Lore Leitner, Partner, Goodwin Procter (UK)*

**March 24, 2022**

GOODWIN

# Agenda

- Cookies and similar technologies
- The legal framework in the US and the EU, and the key requirements
- Five steps to global tracking compliance
- Recent developments

# What are cookies?

**What?**

Cookies are small files of letters and numbers that are stored on a browser or the hard drive of a computer. They contain information that is transferred to user's computer's hard drive

**How?**

When a user first accesses a website, the website may set cookies in the user's terminal equipment

During following visits, the browser shares the cookies with the website, and the website may return personalized content

**Why?**

Cookies allow websites to adapt to users' preferences and choices (e.g., if they add a product to the shopping cart)

GOODWIN

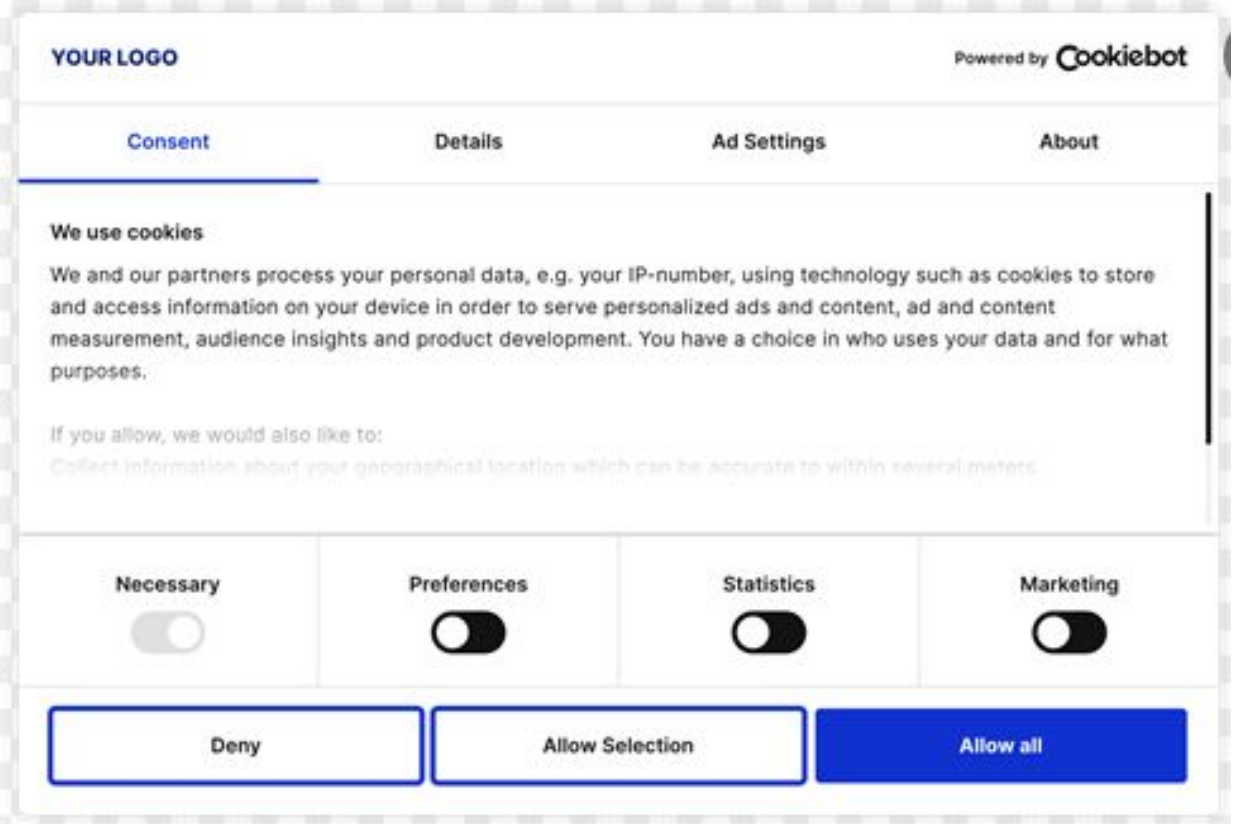
# What are similar technologies?

- The laws do not just apply to "cookies"
- EU concept covers *"use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user"*
- Examples of other technologies:
  - Advertising IDs
  - Pixels
  - SDKs
  - Flash / Local Shared Objects
  - LocalStorage
  - Web beacons or bugs (including transparent or clear gifs)
  - Fingerprinting technologies
  - Social Plug-Ins

# Types of Cookies


GOODWIN

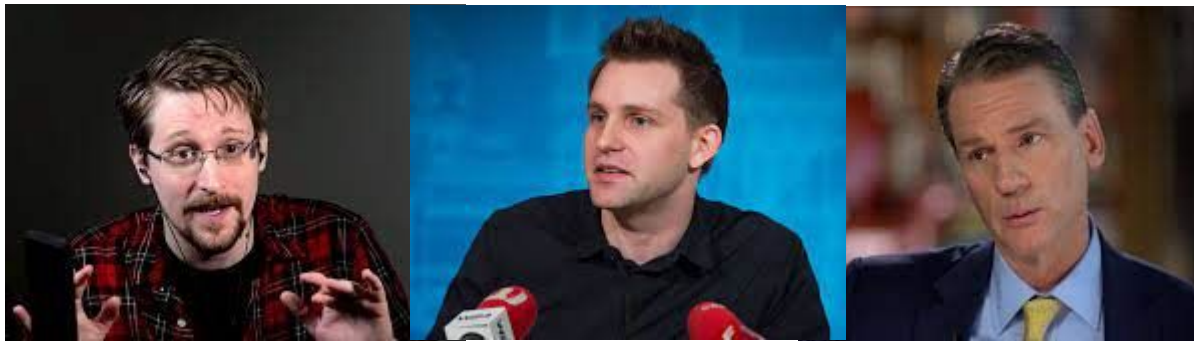
# Categories of Cookies




GOODWIN

# Brief history of OBA and tracking regulation efforts in the US

- **Late 90's** – FTC starts looking into data collection and advertising online
- **First half of 2000's**
  - Self-regulation with IAB, DMA, DMA (PII vs. Non-PII debate),
  - FTC recommends legislation, but dot-com bubble pauses debate
  - Congress enacts GLBA, COPPA



- **Second half of 2000's**
  - FTC issues self-regulatory principles, blurs PII/Non-PII distinction; principles demand transparency and choice
  - California updates CalOPPA, adding OBA disclosure requirements
  - Ghostery/Evidon plug-ins and integrations provide OBA choice (but not tracking choice)
- AdChoices program launches
- **2013** – Edward Snowden upends the world of privacy, FTC updates COPPA
- **May 2018** – GDPR
- **June 2018** – CCPA
- **2023** – CPRA, Virginia CDPA, Colorado CPA

GOODWIN

# US landscape, today

- **Tracking technology covered/regulated**
  - Sale of personal information
  - Sharing personal information with non-affiliates (fintech, insurtech)
  - Collecting PI from children under 16
  - iOS IDFA
  - Sharing PI with non-affiliated third parties for "cross-context behavioral advertising
  - Displaying targeted advertising based on personal information collected from non-affiliated third parties
- **Tracking technology not regulated**
  - First-party - where targeting is based solely on data from a consumer's interaction w/ service
  - Tracking by service providers, e.g., analytics
- **Choices**
  - Generally: **opt-out**
  - Fintech, insuretech, kids under 16, sensitive pi: opt-in
- **Plan of action**
  - Understand tracking landscape - tech you use to track, advertise - and what the tech does specifically with data
  - Verify all settings, in analytics, SDK and other implementations, presence of service provider language
  - Explain tracking and sharing in the privacy policy, **high-level**
  - Make sure you don't use advertising/tracking without opt-in, if required
  - Decide what opt-outs you need to offer based on use of tech
  - Implement opt-out: automated or vendor or self-help via instructions
- **Understand how you store tracking data for privacy rights compliance**

GOODWIN

# Key Differences US v. Europe

- **Mostly opt-in**
- **Requires detailed explanation of tracking**
- **Divergent guidance across member states**

# GDPR vs ePrivacy


## E-Privacy Directive

- Contains "special rules" with respect to the processing of personal data in the electronic communication sector
- Explicitly limits the conditions under which traffic data, including personal data, of subscribers and users of a publicly available electronic communications service may be processed
- Requires user's opt-in consent for use of tracking/profiling cookies/technology except for cookies which are "strictly necessary"
- Take precedence over the (more general) provisions of the GDPR. However, where the processing of personal data is not specifically governed by the ePrivacy Directive (or where the ePrivacy Directive does not contain a "special rule"), the GDPR applies.
- Allows for national variation: directives requires national implementation, and does not have "direct effect"


## GDPR

- Consent should meet the standard of consent required under the GDPR, i.e. freely given and informed, withdrawable at any time in a manner which is as easy as giving consent.
- Privacy-by-design/by-default requires no pre-ticking of consent tick-boxes (*Planet 49*)
- Legal basis is needed for the subsequent processing of the personal data collected via the cookie consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioral advertisement, data-brokering, location-based advertising or tracking-based digital market research
- Does not regulate specific marketing channels/practices
- Applies to *all aspects of personal data processing for marketing purposes*, including collection and sale

GOODWIN

# Key EU Legal Requirements

## CONSENT

- Consent is required for all purposes except strictly necessary cookies
- Clear and positive action required
- Consent needs to be separate per purpose
- No cookies on pre-consent landing page

## NOTICE

- Types of cookies and purposes
- Third party cookies – who these parties are and how they will use the information
- How consent can be withdrawn
- No explicit need to have a cookie policy separate from privacy policy


## OPT-OUT

- Individual must be able to withdraw consent at any time
- Withdrawal must be as easy as giving consent

## LIFESPAN

- France: maximum cookie lifespan 13 months. The maximum retention period of the cookie data collected 25 months
- UK: proportionate to purpose and intended outcome
- Ireland: proportionate – session cookie with forever lifespan not proportionate.

GOODWIN

# Cookie Banner Design

## UK

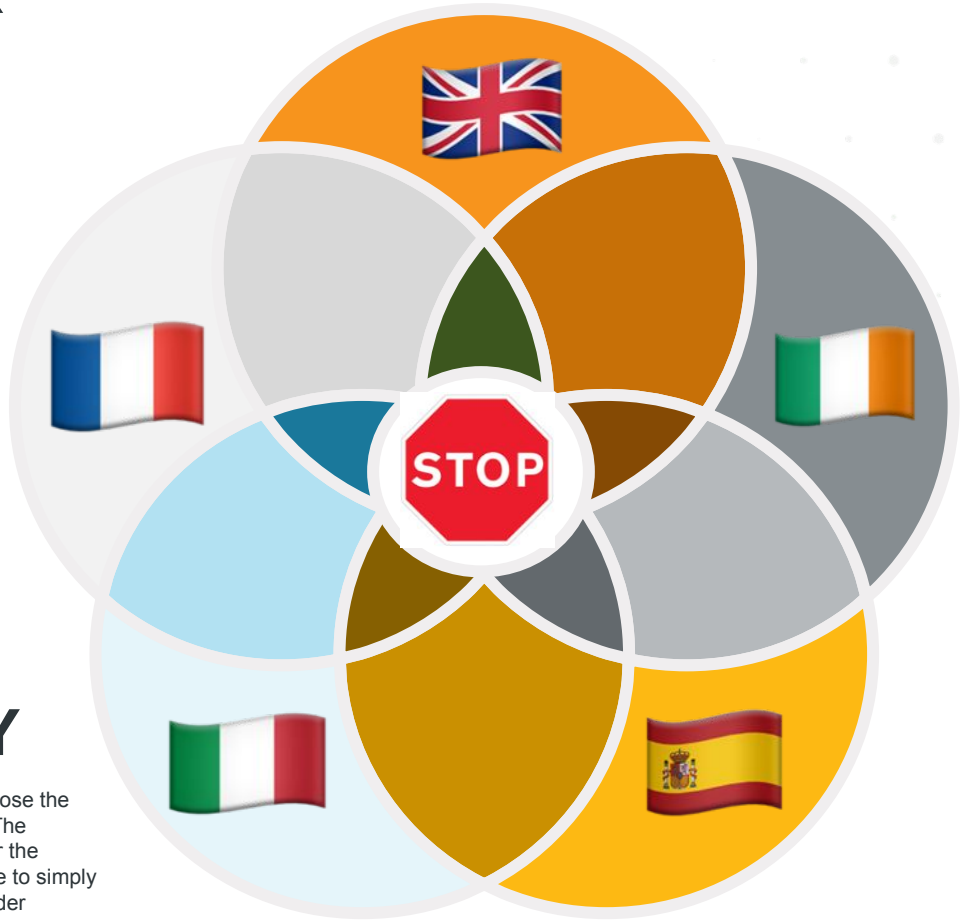
- No pre-ticked boxes (or equivalents such as ‘on’ sliders) for non-essential cookies.
- Emphasizing ‘agree’ or ‘allow’ over ‘reject’ or ‘block’ is not allowed, because this would be influencing users towards the ‘accept’ option.
- A “no-choice” consent mechanism is not allowed, even where the controls are located in a ‘more information’ section.
- The consent mechanism must have the technical capability to allow users to withdraw their consent with the same ease that they gave it.

## FRANCE

- Layered approach recommended.
- Equal prominence to be given to “accept” and “reject” buttons on the first layer of information. Specific granular consent per purpose and per cookies can be obtained through the second layer of information.
- Pre-checked boxes and pre-checked sliders are not allowed.
- Informed consent requires that prior to obtaining user consent, organizations must, at a minimum, provide to users (i) the identity of the data controller(s), (ii) the purpose(s) of the processing activities, and (iii) the existence of the right to withdraw consent
- CNIL strongly recommends certain types of banner design.

## ITALY

- The upper right corner of the cookie banner must contain an “X” to close the banner (in which case only strictly necessary cookies will be used). The Garante made a public statement that it favors the “X” approach over the “reject all button” approach. Its reasoning is that users should be able to simply close a cookie banner and browse a website without having to consider whether they want to accept or reject cookies.
- It must be clear that closing the banner is equivalent to a refusal to consent.
- The cookie banner must contain a link to a GDPR compliant privacy policy.




## IRELAND

- Nudging’ users into accepting cookies over rejecting them is not allowed. Equal prominence must be given to the “accept” option and the “reject” option, as well as the option to manage cookies and navigate to the second layer of information.
- Users must be presented with a link or a means of accessing further information about cookies and the third parties to whom data will be transferred.
- Wording which implies that “continued use of the website” – either through clicking, using or scrolling it - constitutes consent is not allowed.
- Pre-checked boxes and pre-checked sliders are not allowed.
- A “no-choice” consent mechanism is not allowed.

## SPAIN

- The cookie banner must include two buttons: one for accepting all cookies and one for rejecting all cookies. This option is especially advisable when there is a large number of different cookies involved.
- If the “keep browsing” method is adopted as a manner to obtain user consent, the relevant panel must include a “reject all” button.
- The “manage preferences” option must point users directly to setup panel and must be permanently accessible. This panel may be included in the second information layer.

GOODWIN

# Five Steps to Global Tracking Compliance

## Step 1

### Understand company's use of tracking

- Identify which cookies or other tracking technologies you use
- Understand what the tech does with data; sharing, own use, etc.
- Categorize cookies by (1) first/third party, (2) session or persistent, and (3) purpose (strictly necessary, essential, analytics, advertising)
- Check current regulatory and enforcement environment, market conditions

## Step 3

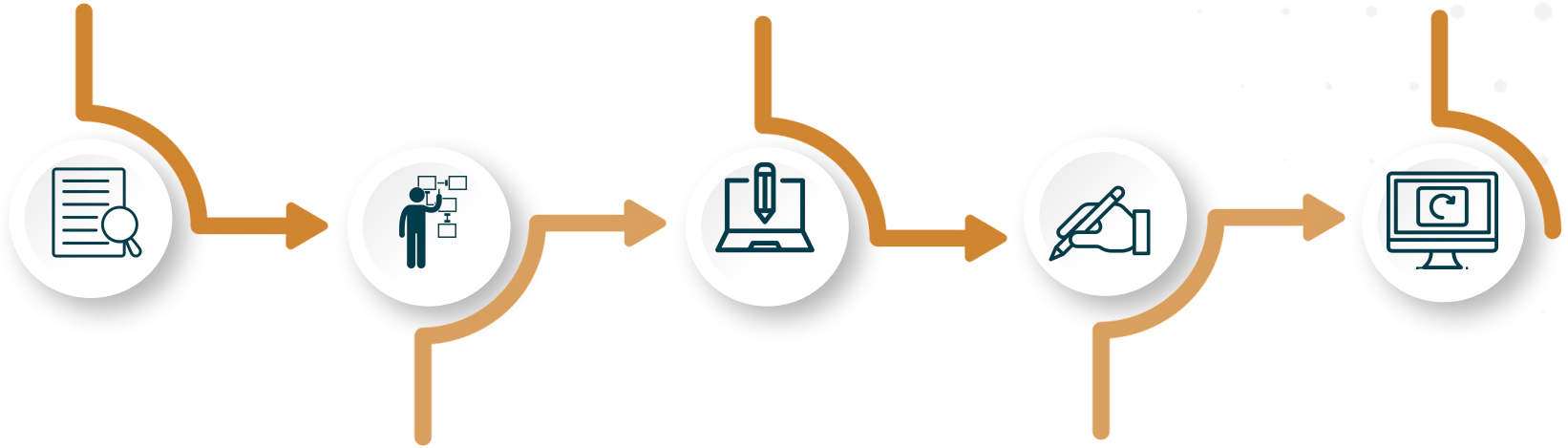
### Update user interfaces and choices

- Design privacy policy, cookie banner, considering current market practice, business needs, and local cookie guidance
- Opt-in choices via banners, pop-ups, operating system
- Opt-out choices via automated solutions or user instructions
- Add links for "sale," "sharing" or "tracking opt-outs"
- Set periodic consent and notice refresh

## Step 5

### Monitor market conditions

- Monitor tracking "chatter"
- Tech is evolving
- Regs are evolving
- Enforcement is evolving
- Market drives compliance posture



## Step 2

### Identify requirements relevant to you

- **Disclosure** - privacy policy, UI, cookie policy, banner, operating system
- **Consent** - opt-in, opt-out, timing
- **Contracts** - service provider language/DPA, based on intent of the relationship
- **Tech settings** - SDK, cookie, other tech settings on data collection, use and sharing, expiration periods
- **Data retention** - for privacy rights compliance

## Step 4

### Test implementation

- Verify that all notices and choices are available to users and work as intended
- Verify that all links work and cross-reference appropriately
- Consider that cookies are not dropped before consent
- Ensure consistency between your cookie and privacy policy on choices and effects of choices
- Verify data retention for privacy rights compliance

GOODWIN

# Recent developments

## Enforcement

- **Regulatory enforcement**, e.g. the **CNIL** has sent out a substantive number of letters to companies to force compliance
  - *December 31, 2021, the CNIL fined Google a total of 150 million euros (90 million euros for Google LLC and 60 million euros for Google Ireland Limited) because users of google.fr and youtube.com can't refuse or accept cookies as easily.)*
  - *December 31, 2021, the CNIL fined Facebook Ireland Limited 60 million euros because the users of the social network facebook.com residing in France can't refuse cookies as easily as to accept them.*

- **NOYB**, NGO founded by Max Schrems with a focus on privacy issues and privacy violations in the private sector

***noyb* files 422 formal GDPR complaints on nerve-wrecking "Cookie Banners"**

**As part of a one-year project on "deceptive designs" and "dark patterns", *noyb* aims to scan, warn and enforce the GDPR on up to 10.000 websites in Europe. After sending a written warning and a "draft complaint" to more than 500 companies on May 31st, 42% of all violations were remedied within 30 days. However, 82% of all companies have not fully stopped violating the GDPR. Accordingly, *noyb* filed 422 complaints with ten data protection authorities today.**

GOODWIN

# Recent developments

## Industry response

- **IAB Europe's TCF 2.0**: in 2018, IAB Europe and industry players created the Transparency and Consent Framework (TCF): a framework for complying with GDPR and providing a way to transmit consent from users to third party vendors. In August 2019, it launched a second iteration to address public and regulatory concern.

- At the start of 2022, the Belgian DPA found that the IAB Europe is a joint controller joint controller for profiling and other data processing done by TCF vendors in the context of OpenRTB. It also found that the information provided to users through the CMP interface is too generic and vague to allow users to understand the nature and scope of the processing, especially given the complexity of the TCF. Therefore it is difficult for users to maintain control over their personal data.

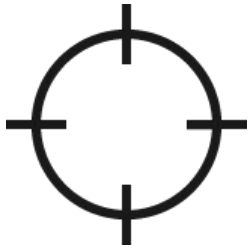
- **Apple** has made numerous changes, e.g. in June 2018 it blocked third party cookies in Safari, in May 2021 it released its app tracking transparency, etc.

- **Google** announced in January 2020 that it would block third party cookies in Chrome by 2022, but has delayed.

## Other developments

- Schrems/NOYB complaints around data export resulting in first decisions around Google Analytics. Wider effect on US-driven ad tech industry.

# The direction of travel against third party cookies



**Targeting needs a new approach**

There are no audience standards and retargeting across sites won’t work.

**Frequency capping is no longer possible**

Without identifiers it’s no longer possible to track reach and frequency across channels.

**Measurement won’t work**

Measuring campaign performance will be difficult without tracking identifiers.

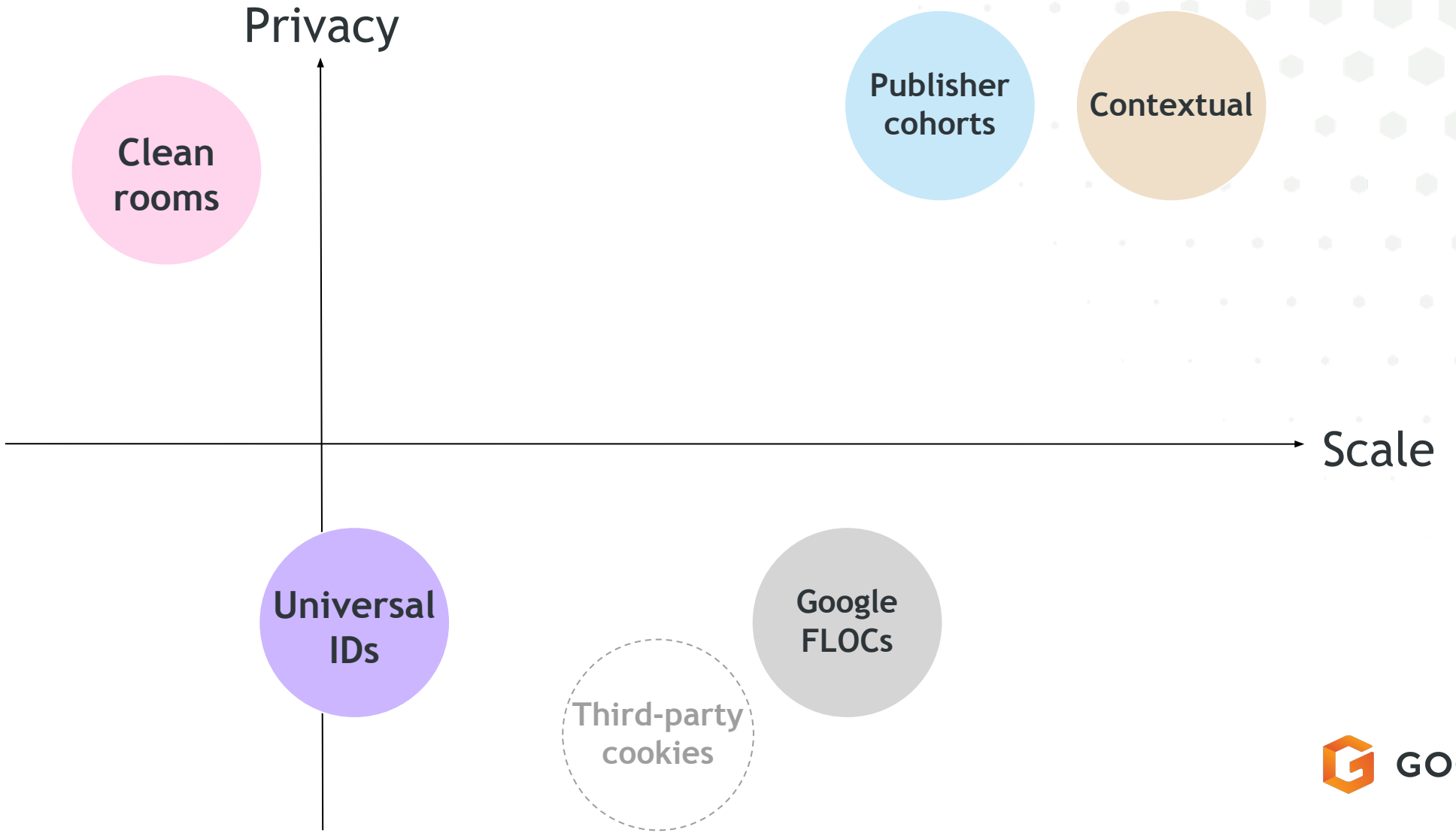
GOODWIN

# Emerging Solutions

| Solution | Requires identifiers | What is it? | Who controls data? |
|---|---|---|---|
| **Universal IDs** | Y | Advertiser first-party data (typically email addresses) is matched with partner data and encrypted by the ID provider. | ID Vendors |
| **Clean rooms** | Y | Advertiser first-party data is matched with publisher data in a secure, controlled environment managed by the advertiser. | Publishers & advertisers |
| **Contextual targeting** | N | Targeting based on the content of the page, not the behaviour of the viewer. | Publishers |
| **Cohorts** | N | First-party data, such as browsing behavior, is used to expose a description of users as a cohort. | Publishers |

GOODWIN

# Evaluate each Solution against Privacy, Performance and Scale




GOODWIN

# Thank You