




Bird & Bird

&





New Facebook
advertising terms, new
Apple iOS 14 privacy
rules and updated
cookie guidance: help!



Gabriel Voisin
Partner, UK



Izabela Kowalczyk-Pakula
Partner, Poland



Sophie Dawson
Partner, Australia



James Fenelon
Senior Associate, UK



New Facebook Custom Audience & Lookalike terms

Apple iOS 14 and upcoming transparency and consent requirements regarding the access to IDFA

Updated cookie guidelines from EU



New Facebook Custom Audience & Lookalike terms

Updates to  business terms

Joint control - are you listening?



European Data Protection Board

New terms - what data is Facebook Joint Controller of?

Facebook Business Terms - Updated August 2020



Does your company use:

The Facebook Pixel

Social plugins



Or



Matching for Facebook Custom Audience can be based on (1) email or (2) cookies via the Pixel. It is only the Pixel matching that is caught by the joint controller terms.



If **Yes**, you will now be a joint controller with Facebook for certain processing activities

What are you joint controller of with Facebook?

What data?

The Joint Control pertains to 'Event Data' . This is defined as 'information that you share about people and the actions that they take on your websites and apps or in your shops, such as visits to your sites, installations of your apps and purchases of your products'



What purposes?

- 1 For targeting ads
- 2 To deliver commercial and transactional messages
- 3 & to improve ad targeting and delivery optimization.

No.	Obligation under GDPR	Facebook Ireland	You
1	Article 6: Requirement of legal basis for Joint Processing	<p style="text-align: center;">×</p> <p style="text-align: center;">(regarding Facebook Ireland's processing)</p>	<p style="text-align: center;">×</p> <p style="text-align: center;">(regarding your own processing)</p>
2	Articles 13,14: Providing information on Joint Processing of Personal Data		<p style="text-align: center;">×</p>
3	Article 26(2): Making available the essence of this Controller Addendum		<p style="text-align: center;">×</p>
4	Articles 15-20: Rights of the Data Subject with regard to the Personal Data stored by Facebook after the Joint Processing	<p style="text-align: center;">×</p>	
5	Article 21: Right to object insofar as the Joint Processing is based on Article 6(1)(f)	<p style="text-align: center;">×</p> <p style="text-align: center;">(regarding Facebook Ireland's processing)</p>	<p style="text-align: center;">×</p> <p style="text-align: center;">(regarding your own processing)</p>
6	Article 32: Security of the Joint Processing	<p style="text-align: center;">×</p> <p style="text-align: center;">(regarding the security of the Applicable Products)</p>	<p style="text-align: center;">×</p> <p style="text-align: center;">(regarding the correct technical implementation and configuration of the Applicable Products)</p>
7	Articles 33, 34: Personal Data Breaches concerning the Joint Processing	<p style="text-align: center;">×</p> <p style="text-align: center;">(insofar as a Personal Data Breach concerns Facebook Ireland's obligations under this Controller Addendum)</p>	<p style="text-align: center;">×</p> <p style="text-align: center;">(insofar as a Personal Data Breach concerns)</p>

What do you have to do?

1. **Be aware of the change**
2. **Explain to individuals 'the essence of the arrangement'. The Customer is responsible for providing notice to the individual, under the Terms, this notice should include the fact:**
 - that Facebook Ireland is Joint Controller of the Joint Processing;
 - purposes for which the collection and transmission of personal data that constitutes the joint processing takes place;
 - in relation to data subject rights, in respect of the joint processing, Facebook is the data subject's primary contact for exercising their rights;
 - Further information on how Facebook Ireland processes personal data, including the legal basis Facebook Ireland relies on, and information on exercising data subjects rights, can be found in [Facebooks Privacy Policy](#).

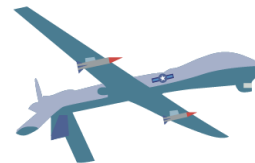
Other points to note:

- Under JCA obligations to forward correspondence from data subjects or regulators within 7 calendar days. Customer *'not authorised to act or answer on Facebook Ireland's behalf'*
- *If you are providing customer data on behalf of a third party, you are required represent and warrant to Facebook that you have authority as agent to such third party to use and process such data on its behalf and bind such third party to these Business Tools Terms.*

Australian Adtech: Change on the horizon

ACCC Digital Platforms Inquiry

- It made a number of important recommendations such as:
 - Changes to privacy laws to bring them up to and beyond General Data Protection Regulation,
 - An introduction of a tort of privacy which would have major ramifications for investigative journalism,
 - Increases in penalties for breaches of privacy laws,
 - A Digital Platforms Code to govern the relationship between digital platforms and traditional media,
 - A Take Down Code dealing with online copyright infringement,
 - A 'Fake News' code dealing with online dis-information,
 - A variety of competition-based changes.



Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020

- Google, Facebook and other designated digital platform services to:
 - Compensate registered media businesses in relation to making available certain content
 - content test, revenue test, professional standards test and Australian audience test for registration of news business
 - Mandatory arbitration process to resolve any dispute



Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020

- Designated digital platforms which make available covered news content must provide certain information to registered news businesses, including:
 - Explanation of data
 - Certain changes to algorithms affecting referral traffic



Privacy Law Reform

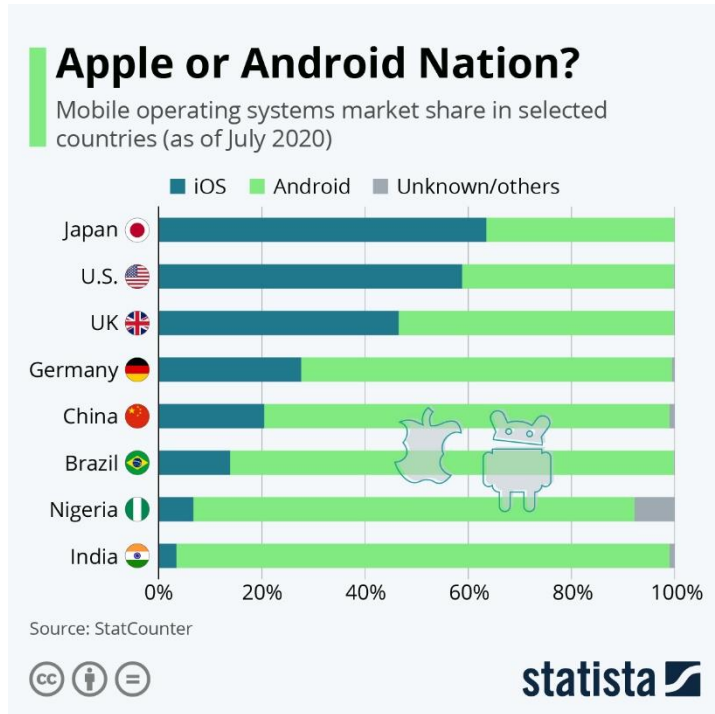
- Move towards GDPR
- May go further in significant respects
- First round of submissions in now: detailed round of exposure drafts and submissions in 2021





Apple iOS 14 and upcoming transparency and consent requirements regarding the access to IDFA

Why is this an important topic?



- iOS has a large market share in key leading markets
- The changes will be imposed on app publishers
- Non-compliance can trigger a risk to see an app delisted from the App Store for instance

The saga started over the summer



- June 2020 Apple Conference announcing more transparency and prior user consent before IDFA can be accessed
- IDFA = Identifier for Advertisers is a random device identifier assigned by Apple to a user's device
- Strictly speaking, nothing new in Europe given existing ePrivacy requirements (i.e. consent required for cookies & similar technologies unless exemptions apply)

Then things started to get heated...

- Various letters from interested parties sent to Apple
- Facebook complained about Apple's privacy moves
- On September 3rd, Apple (i) announced its intent to delay the requirement to seek user consent before IDFA can be accessed to 2021 but (ii) went ahead with its transparency push



And... it escalated and backfired...

- In October, 4 online advertising lobby groups (IAB France, MMAF, SRI and UDECAM) filed an antitrust complaint against Apple in FR
- In November, noyb filed complaints against Apple in ES and DE

"We believe that Apple violated the law before, now and after these changes. With our complaints we want to enforce a simple principle: trackers are illegal, unless a user freely consents. The IDFA should not only be restricted, but permanently deleted. Smartphones are the most intimate device for most people and they must be tracker-free by default."

Stefano Rossetti, privacy lawyer at noyb.eu

But Apple is not backing down...

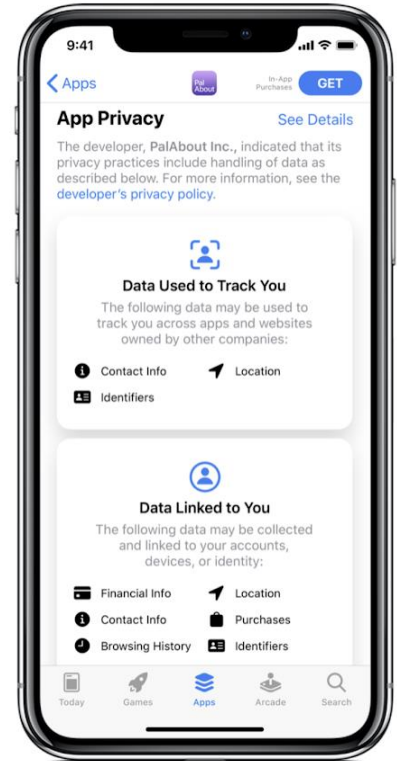


SCAN ME



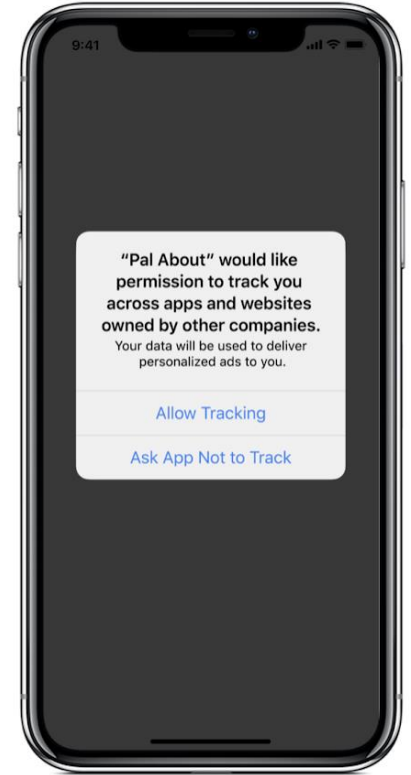
So what to expect? First, transparency obligations

- Also known as "*privacy nutrition labels*" they require app developers to disclose all the information they and their third-party partners collect
- Input to be maintained up-to-date and self-reported by app developers
- App developers were required to start submitting labels for their apps starting on December 8th, and the labels themselves are expected to start appearing "*later this year*" in the App Store



Second, a need to seek users' consent before IDFA can be accessed

- Also known as ATT (Anti Tracking Transparency)
- This will be a native consent overlay pushed by iOS
- Safari users will remember its browser equivalent known as ITP (Intelligent Tracking Prevention)
- GDPR compliant? See EPDB consent opinion:
 - The controller's identity
 - The purpose of each of the processing operations for which consent is sought
 - What (type of) data will be collected and used
 - The existence of the right to withdraw consent
- Setting to be enforced "*early next year*" says Apple





Updated cookie guidelines from the EU

Why should we care about EU cookie rules?

Regulators are increasingly active on the cookie enforcement front.

- Example: AEPD



- Vueling, €30,000 fine (October 2019)
- IKEA, €10,000 fine (December 2019)
- Twitter, €30,000 fine (June 2020)

- BIG NEWS! – CNIL



- Google will be fined €100 million and Amazon €35 million for violations of rules around using cookie tracking tech.
- Google fine - the biggest fine so far
- When? – today
- Source: [Politico](#)
- CNIL has not confirmed the amount, but has confirmed the date

Updated EU cookie guidelines

1. **France: CNIL** (October 2020)

- Updated provisions in relation to the CNIL cookie guidelines originally published in July 2019
- A series of recommendations on practical ways to collect consent
- FAQs

2. **Spain: AEPD** (July 2020)

- Guidance on the use of cookies and other internet-tracking technologies and updated to ensure consistency with EDPB guidelines on consent

3. **Ireland: DPC** (April 2020)

- Cookie guidelines updated

4. **UK: ICO** (July 2019)

- New guidance on the use of cookies and other internet-tracking technologies

5. **Germany**

- German conference of supervisory authorities published guidance on internet tracking (March 2019)
- German state-level guidance

Similarities

Other technologies covered?	Yes , like pixels, software development kit in mobile.
Implied consent	<ul style="list-style-type: none">• No, GDPR threshold for prior consent (informed, specific, unambiguous)• DPAs in France, UK, Spain, Germany: a user continuing to browse a website (e.g., clicking a button or link or scrolling) does not amount to that user's consent• <i>Ireland: "The circumstances where browser settings are likely to be considered valid to constitute consent to the setting of cookies are likely to be very limited and they would need to be assessed on a case-by-case basis."</i>• Change for Spain: consent by means of a clear and affirmative action in no longer accepted.
Contractual consent	<ul style="list-style-type: none">• DPAs in France, UK, Spain: T&C ≠ consent. DPAs in Germany and Ireland– no comments but likely agree.
Global consent	<ul style="list-style-type: none">• Consent must cover each purpose for which personal data will be processed (i.e., each purpose for which cookies are used).• DPAs in France, UK, Spain, Ireland: organisations can offer a global consent for all cookies for which consent is required in their first consent layers. DPAs in Germany – do not comment on this.

Similarities

Granular consent	<ul style="list-style-type: none">• French DPA: a second layer should allow the user to give specific consent to each purpose separately.• Spanish DPA: the first layer should include a link to a tool that enables users to give granular consent to each category of cookies (at least, grouped by purpose).• Irish DPA: the first layer should include specific purpose• This is not spelled out in the UK DPA's guidance, but based on the authority's own practice, purpose-specific consent options are likely to be regarded as best practice.• German DPAs require granular consent, but do not specify whether this should be part of the first layer or could be moved to a second layer.
Consent for whom?	<ul style="list-style-type: none">• The user must be able to identify all parties processing their data.• French, German, UK and Spanish DPAs: name all parties who will rely on users' consent.• French DPA: the list of third parties placing cookies should be: (1) easily accessible at all times and (2) updated regularly.

Differences

	France	UK	Germany	Spain	Ireland
Grace period	Yes. 6 months. March 2021	No	No	Yes but partially, November 2020	Yes, 6 October 2020
Are cookie walls allowed?	<ul style="list-style-type: none"> No longer provide a blanket prohibition of cookies walls. Cookie walls are unlikely to meet the threshold for valid consent under the GDPR. “Case by case” approach . 	<ul style="list-style-type: none"> Consent that is forced via a cookie wall is “unlikely to be valid.” GDPR must be balanced against other rights. 	No	<ul style="list-style-type: none"> Revised version: No, unless alternative and equivalent service for which consent is not necessary is offered, and as long as the user is informed about it. 	No guidance
Do analytic cookies require consent?	<ul style="list-style-type: none"> Yes, but not always, CNIL’s position has changed. Certain types of analytic cookies can be regarded as “strictly necessary” if cumulative conditions were met (e.g., lifespan of analytic cookies must not exceed 13 months, etc). Possible cookie analytic cookie exceptions under ePrivacy Regulation? 	<ul style="list-style-type: none"> Yes. There is no exception. “Unlikely that priority for any formal action would be given to uses of cookies where there is a low level of intrusiveness and low risk of harm to individuals,” and first-party analytics cookies are given as an example of cookies that are potentially low risk. 	<ul style="list-style-type: none"> No, unless they lead to a transfer of personal data to a third party. Even in that case, likely no consent would be necessary if users can easily opt out from the data transfer to the third party. 	Yes	Yes , first-party analytics cookies are not likely to create a privacy risk when they are strictly limited to first-party aggregated statistical purposes, and are unlikely to be considered a priority for enforcement action. Third party analytics may be considered to represent a greater privacy risk to the user.

Differences – "Your Choices"

France	Spain	Ireland
<p>The first layer of the cookie banner:</p> <ol style="list-style-type: none">1) “reject all” and “accept all” buttons alongside a “preferences”2) “accept all” and a “preferences” buttons and offer the possibility for users to reject cookies by clicking on a sentence such as “continue without accepting [X]” in the top right corner.3) “accept all” and a “preferences” buttons and offer the possibility for users to reject all cookies by continuing browsing/not interacting with the cookie consent banner. However, in such cases (1) the text of the first layer of the cookie consent banner must make this clear and (2) the cookie consent banner must “disappears after a short period of time, so as not to hinder the use of the site or the application and so as not to condition the user’s browsing comfort on the expression of his consent to the cookies.”	<p>The first layer of the cookie banner:</p> <ol style="list-style-type: none">1) A “Consent”/ “Accept” button. Although “By continued browsing ...” solutions are no longer valid, the Spanish authority still recognises that consent through a clear and positive action could still be valid as long as the user is provided with enough information.2) A tool (or a link to a tool) that enables users to give granular consent to each category of cookies (at least, grouped by purpose) and to reject all cookies.3) Unless offered in the tool mentioned above, a “Reject all” button.	<p>" If organisation uses a button on the banner with an ‘accept’ option, you must give equal prominence to an option which allows the user manage cookies to ‘reject’ cookies, or to one which allows them to and brings them to another layer of information in order to allow them do that, by cookie type and purpose.</p>

Differences - Cookie lifespan and retention periods

France	UK	Germany	Spain	Ireland
<p>The lifespan of analytic cookies benefitting from the CNIL consent exception must not exceed 13 months. Information collected through these can be kept for a maximum of 25 months.</p> <p>Best practice:</p> <ul style="list-style-type: none">• cookies consent should be valid for 6 months. There is no perfect “one size fits all” answer to this question.• any refusal to the placement of cookies must be retained for the same duration as consent.	<p>The lifespan of cookies must be proportionate in relation to the intended outcome and limited to what is necessary to achieve the purpose.</p> <p>The maximum possible technical duration of a cookie (e.g., “31/12/9999”) would not be regarded as proportionate in any circumstances.</p>	<p>No specific lifespan for cookies, shorter lifespan is more likely to meet the requirements of legitimate interest test.</p>	<p>The lifespan of cookies must be proportionate in relation to the purposes for which they are intended; consent should be renewed after 24 months.</p>	<p>The expiry date of any cookie should always be proportionate to its purpose.</p>

Want to know more?

Check out our article on ICO, CNIL, German and Spanish DPA revised cookie guidelines



Meet the authors:



Gabriel
Voisin
Partner, UK



Ruth Boardman
Partner, UK



Dr Simon Assion
Counsel,
Germany



Clara Clark
Nevola
Associate, UK



Lupe Sampedro
Partner, UK &
Spain



Ester Vidal
Senior Associate, Spain

E-Privacy regulation

Will we ever get to see a final version of the ePrivacy Regulation?

Attempts to harmonize diverse areas including cookie/similar tracking rules – However, this is a slow process, that has recently had significant setback, and the timeline remains uncertain



Brussels, 20 November 2020
(OR. en)

12891/20

Interinstitutional File:
2017/0003(COD)

LIMITE

TELECOM 215
COMPET 556
MI 465
DATAPROTECT 125
CONSUM 187
JAI 967
DIGIT 120
FREMP 116
CYBER 229
CODEC 1142

NOTE

From:	Presidency
To:	Delegations
No. Cion doc.:	5358/17 TELECOM 12 COMPET 32 MI 45 DATAPROTECT 4 CONSOM 19 JAI 40 DIGIT 10 FREMP 3 CYBER 10 IA 12 CODEC 52
Subject:	Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Progress report



Bird & Bird

&





Thank you!