



---

**PROGRAM MATERIALS**  
**Program #29148**  
**September 16, 2019**

## **The ePrivacy Directive and Regulation: Where do we stand?**

**Copyright ©2019 by Julie O’Neill, Esq. and Alex van der  
Wolk, Esq., Morrison & Foerster LLP**  
**All Rights Reserved.**  
**Licensed to Celesq®, Inc.**

---

**Celesq® AttorneysEd Center**  
**[www.celesq.com](http://www.celesq.com)**

**5301 North Federal Highway, Suite 180, Boca Raton, FL 33487**  
**Phone 561-241-1919      Fax 561-241-1969**

**MORRISON  
FOERSTER**

# **COOKIES, E-PRIVACY AND ONE-STOP-SHOP: GDPR AT THE ONE-YEAR MARK**

**Julie O'Neill**

**Alex van der Wolk**

September 16, 2019

# What We Will Cover

---

## ePrivacy

1

- Differences between the Directive and the Regulation
- Status of the Regulation
- Interplay between GDPR and ePrivacy
- DPAs' approach to ePrivacy

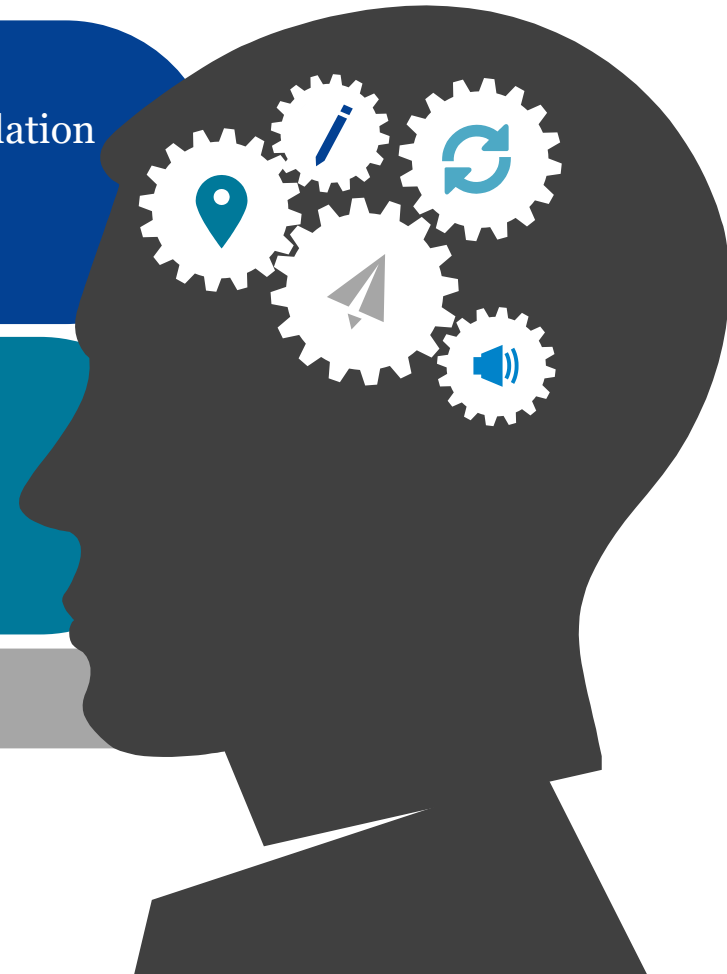
## Cookie Consent Requirements

2

- What constitutes valid consent?
- Different approaches to obtaining consent
- The use of cookie walls
- Intersection with GDPR

3

## GDPR at the one-year mark



# **ePrivacy: The Directive & The Regulation**

# ePrivacy – What Does It Regulate?

---

- **GDPR provides for a general privacy framework**
  - Applies to personal data, regardless of type of use, sector or industry
- **Since 2002: ePrivacy**
  - Regulates specific uses of (personal) data and technologies:
    - Cookies and similar technologies
      - Regardless of whether the data collected through cookies amounts to personal data
      - Prior consent required (will talk more about this later), but exceptions apply
    - Electronic direct marketing
      - E.g., email, text message and fax marketing and, in the future, possibly Whatsapp or other direct messaging
      - Prior consent required, but exceptions apply
    - Phone marketing
      - No prior consent required but must honor opt-outs (including prior opt-outs administered via Do-Not-Call list)
  - Also contains requirements specific to the telecommunications sector

  
**2002**

# ePrivacy Directive vs. Regulation

---

## Since 2002 (and updated in 2009): ePrivacy Directive

## Post-GDPR: ePrivacy Regulation



Requires implementation  
in national law



Not all countries have  
implemented to date  
(e.g., Germany)



Like GDPR, would have  
direct applicability  
(and enforceability) in all  
EU Member States

# ePrivacy Regulation – Status

Not yet finalized

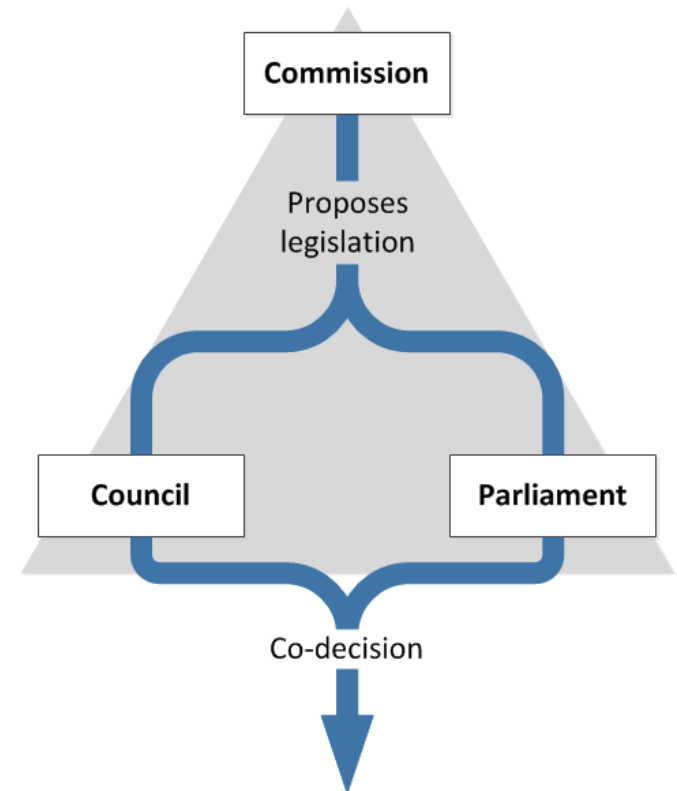
European Commission's proposal issued January 2017 and originally intended to take effect simultaneously with GDPR (May 2018)

Like GDPR: requires consensus among EC, Parliament and Council

Council is not yet internally aligned on its position (last published version Feb. 2019)

Not expected to be finalized until end of 2019

Will then have period of time before entry into force



# ePrivacy Regulation – What to Expect?

---

**Tightened requirements around consent**



**Introduction of privacy-by-default requirements**



**Extension of direct marketing rules to a broader range of channels**



**Unclear if harmonization for B2B marketing will be introduced**





# What to Expect? (cont'd)

---

**Introduction of rules for Wi-Fi or beacon scanning and other location-based tracking**



**Broader definition of “cookies”**



**Likely: exemption for cookie consent broadened to include (certain types of) analytics cookies**



**Penalty regime aligned with GDPR**  
(though still debate on which ‘bands’ should apply to what)



# Interplay Between GDPR and e-Privacy

	GDPR	e-Privacy
<b>Nature</b>	General regime	<ul style="list-style-type: none"> <li>• Special regime for specific activity only</li> <li>• E-privacy rules take precedence over GDPR for these activities</li> </ul>
<b>Scope</b>	All processing of personal data	<ul style="list-style-type: none"> <li>• Direct marketing emails and other electronic marketing messages               <ul style="list-style-type: none"> <li>• On-site banners?</li> </ul> </li> <li>• Cookies and similar tracking technologies</li> <li>• Based on where the end user (not the company) is located</li> </ul>
<b>Notice</b>	General requirements	<ul style="list-style-type: none"> <li>• Specific information</li> <li>• GDPR for the rest (if personal data are collected)</li> </ul>
<b>Consent</b>	Yes, but other grounds available (e.g., legitimate interest)	Yes, but there are exceptions (e.g., strictly necessary cookies)
<b>Rights</b>	Broad – access, rectification, deletion, etc.	Limited – opt-in/out

# Interplay Between GDPR and e-Privacy (cont'd)

---

## ePrivacy is considered a “*lex specialis*” compared to GDPR:

- It governs a specific subject matter
- It applies on top of GDPR
- It refers to GDPR for interpretation of certain points (such as when consent is deemed valid)
- It takes precedence with respect to areas specifically provided for by ePrivacy, such as consent for direct marketing
- But it does not put GDPR out of play
  - For example: the use of cookies is subject to ePrivacy requirements, but where the use of cookies amounts to a processing of personal data, then GDPR also applies

## EDPB Opinion, adopted on March 12, 2019

- Regarding the interplay of ePrivacy and GDPR

# DPAs' Approach to ePrivacy post-GDPR

---

**Even though the ePrivacy Regulation has not yet been finalized, local implementations of the ePrivacy Directive continue to apply**

Existing consent requirement for direct marketing and cookies

**Because of GDPR, the ePrivacy Directive's requirements on consent have already been tightened**

For interpretation of consent, ePrivacy refers to the general privacy regime – i.e., GDPR

**ePrivacy doesn't put GDPR out of play**

Where the use of cookies or similar tracking technologies involves the processing of personal data, GDPR fully applies: legal basis, duty to inform, competency of DPA to enforce GDPR, etc.

# **Cookie Consent Requirements**

# Cookie Consent Post-GDPR

- **GDPR requirements for valid consent:**

**Evidenced by an  
“affirmative act”**

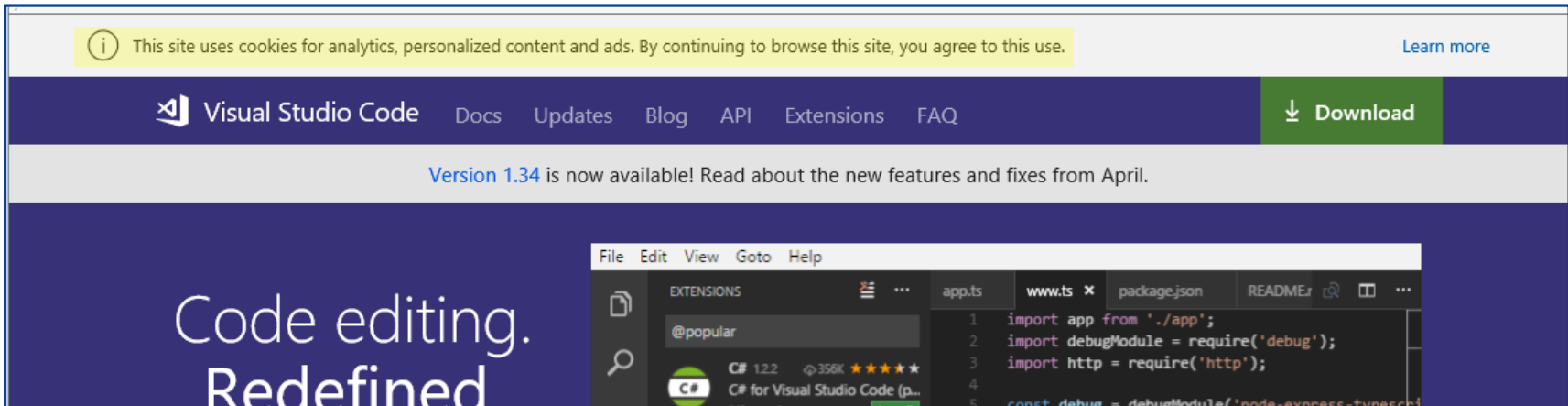
Inactivity does not  
constitute consent

**Provision of a service  
pursuant to a contract  
cannot be conditioned  
on consent for  
processing that is not  
essential to the service**

**Freely given, specific  
and informed**



# Cookie Consent: Affirmative Act



***Is the continued use of a website an affirmative act from which consent may be inferred?***

➤ **EDPB Consent Guidelines: No**

*“merely continuing the ordinary use of a website is not conduct from which one can infer an indication of wishes by the user to signify his or her agreement to a proposed processing operation. [...] scrolling down or swiping through a website will not satisfy the requirement of a clear and affirmative action, because such alert may be difficult to distinguish and/or may be missed when an individual is quickly scrolling through large amounts of text and such an action is not sufficiently unambiguous.”*

# Affirmative act? continued use of website

---

*Is the continued use of a website an affirmative act from which consent may be inferred?*

➤ **France (CNIL Guidance on Cookies): No**

“The acts of continuing to browse a website, use a mobile application, or scroll down the page of a website or mobile application are not clear positive actions equivalent to valid consent.”

➤ **UK (ICO Guidance on Cookies): No**

Implied consent is not acceptable. A cookie banner including wording such as *‘By continuing to use our website, you consent to our use of cookies’* will not represent valid consent, even if it also includes an ‘OK’ or ‘Accept’ button.



## **Presenter to read NY Code**

**This code is required for all attorneys wishing to receive CLE credit in the state of NY and taking the program 'on-demand' at Celesq AttorneysEd Center either online or via CD**

**Please notate it carefully**

**The presenter will only be able to read the code twice and will not be able to repeat it or email it to you.**

**Thank you!**

# Cookie Consent: Affirmative Act (cont'd)

---

***Does the use of a pre-checked cookie box count as valid consent?***

➤ **Advocate General of the European Court of Justice: No**

Planet 49 (*Case C-673/17*):

To be valid, consent must be manifested by a clear affirmative act. In addition, to be valid, consent must be separate: consents to different items (such as to a service and to the use of cookies) cannot be bundled into the one request for consent.



# Cookie Consent: Exemption

---

## *Are analytics cookies exempt from consent?*

- Currently: not yet harmonized
- Expected to be harmonized across Europe via ePrivacy Regulation

### ➤ **France: yes, under circumstances**

Analytics and audience measurement are exempt from consent under specific circumstances.

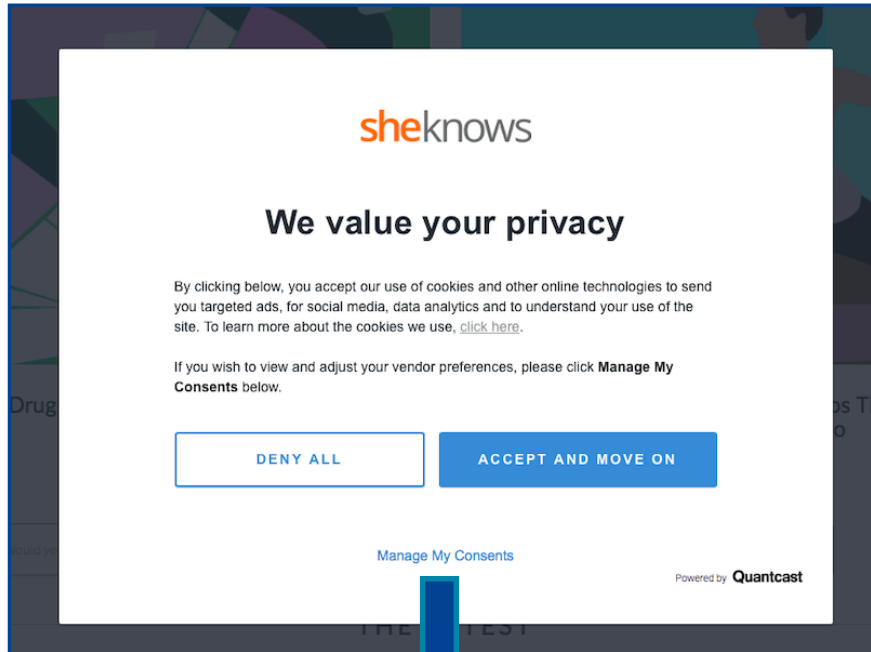
They must be first-party cookies, erased within 13 months, and serve only limited purposes (e.g., to evaluate content and/or functioning of the website). Also, users must be given prior notice and the opportunity to object.

### ➤ **UK: No**

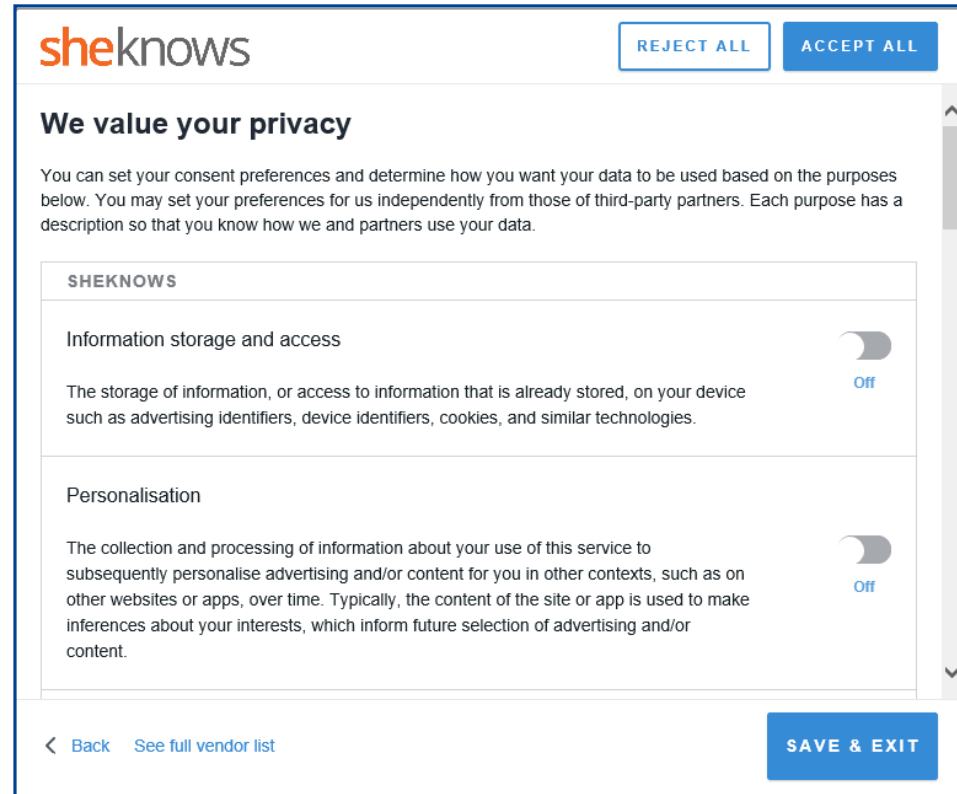
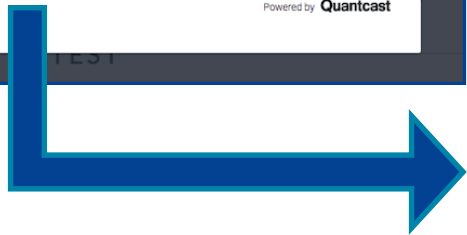
Analytics cookies are not ‘strictly necessary’, because they are not part of functionalities that the user requests when using a service online.

Analytics cookies require prior consent (although they pose a low risk)

# Approach to Cookie Consent: Gold Standard



The image shows a standard cookie consent banner for sheknows. It features the sheknows logo at the top, followed by the heading "We value your privacy". Below this, there is a paragraph explaining that clicking below indicates acceptance of cookies and other technologies for targeted ads, social media, and data analytics. A link "click here" is provided for more information. Another paragraph invites users to "Manage My Consents" to view and adjust vendor preferences. At the bottom, there are two buttons: "DENY ALL" and "ACCEPT AND MOVE ON". A "Manage My Consents" link is also present, and the banner is noted as being "Powered by Quantcast".



The image shows a detailed cookie consent interface for sheknows. It features the sheknows logo at the top left, with "REJECT ALL" and "ACCEPT ALL" buttons at the top right. The heading "We value your privacy" is followed by a paragraph explaining that users can set their consent preferences and determine how their data is used based on the purposes below. The interface lists two categories of data processing:

- SHEKNOWS**
  - Information storage and access**: The storage of information, or access to information that is already stored, on your device such as advertising identifiers, device identifiers, cookies, and similar technologies.  Off
  - Personalisation**: The collection and processing of information about your use of this service to subsequently personalise advertising and/or content for you in other contexts, such as on other websites or apps, over time. Typically, the content of the site or app is used to make inferences about your interests, which inform future selection of advertising and/or content.  Off

At the bottom, there are links for "Back" and "See full vendor list", and a "SAVE & EXIT" button.

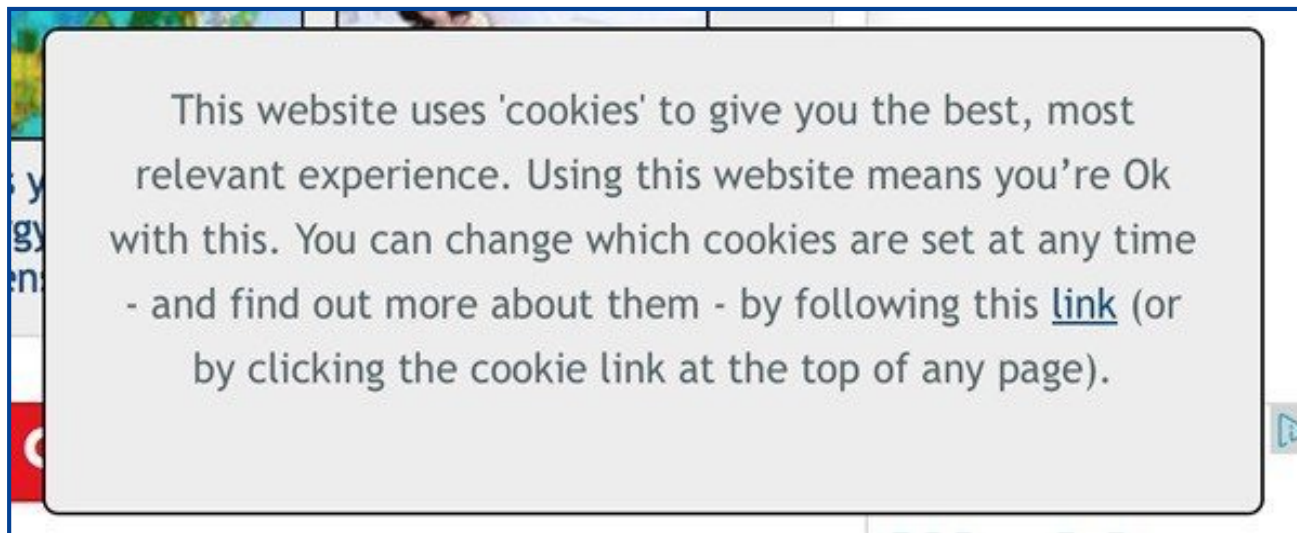
# Approach to Cookie Consent: Market

---



# Approach to Cookie Consent: Risk-Based

---



# Scanning / Consent Tools

---

Various scanning tools available in the market help identify which cookies are used on your website



Scanning tools may also help with categorizing consent and obtaining consent



Beware of the 'bucketing' of cookies

- Ensure the right bucketing structure
- Ensure that cookies end up in the right bucket



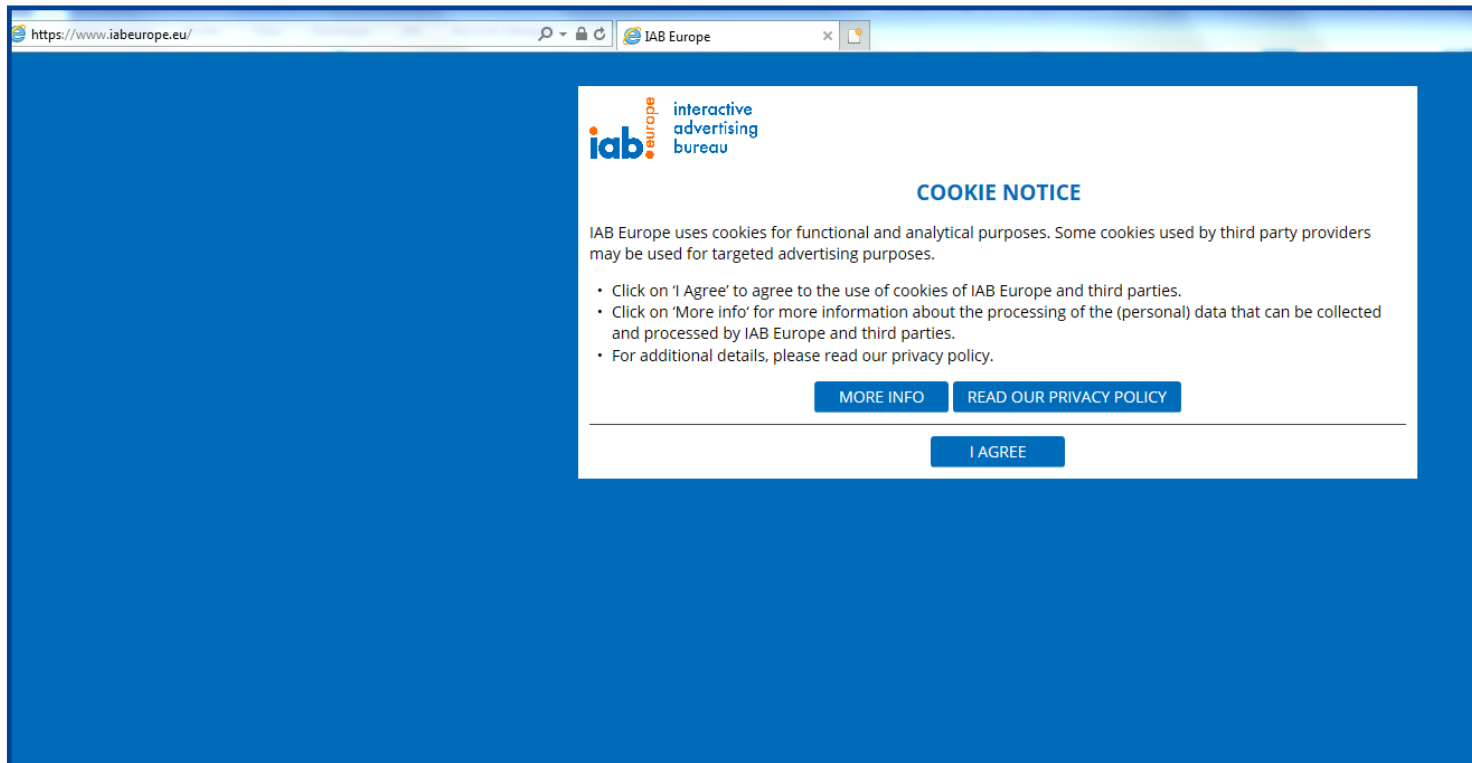
Beware of default settings

- Are cookies placed upon landing or pursuant to choices exercised?

# The Use of Cookie Walls

---

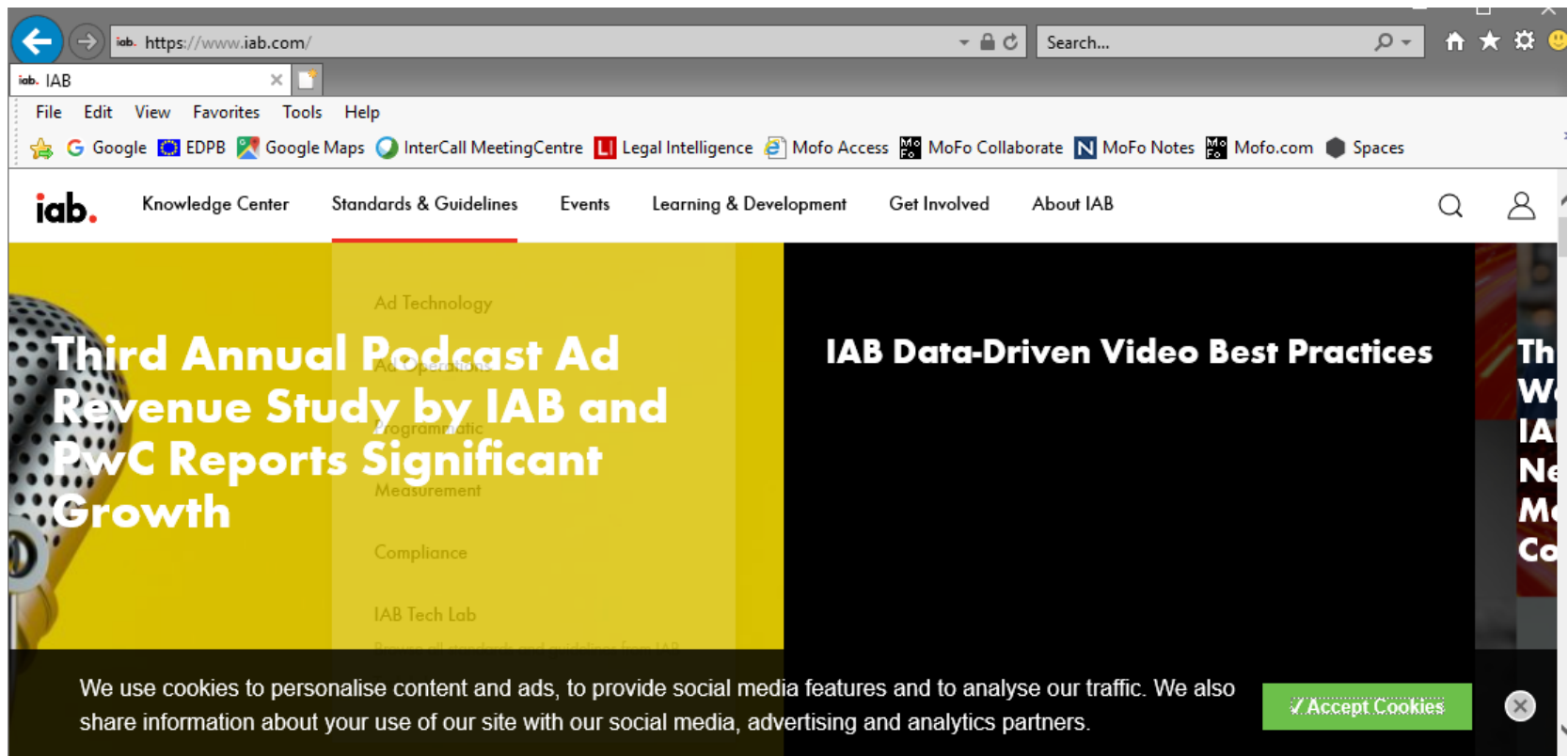
- A cookie wall blocks access to a website unless the user first accepts the use of cookies.
- Cookie walls take two forms:
  1. The website is not accessible unless cookies are accepted:





# The Use of Cookie Walls (cont'd)

2. The website does not provide the option to use the website without cookies. In other words, there is no option to deny the use of cookies.



The screenshot shows a web browser window displaying the IAB website. The browser's address bar shows the URL <https://www.iab.com/>. The website's navigation menu includes links for Knowledge Center, Standards & Guidelines, Events, Learning & Development, Get Involved, and About IAB. The main content area features two large promotional banners: one for the 'Third Annual Podcast Ad Revenue Study by IAB and PwC Reports Significant Growth' and another for 'IAB Data-Driven Video Best Practices'. At the bottom of the page, a dark cookie consent banner is visible, containing the text: 'We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners.' To the right of this text is a green button labeled 'Accept Cookies' and a small 'X' icon to close the banner.

# Cookie Walls (cont'd)

---

- **Cookie walls have historically not been outright prohibited**
  - But there is a push to prohibit them under the ePrivacy Regulation
  - Also: issue may be moot, considering regulators' recent approach:

➤ **UK:** consent is likely to be invalid if the cookie wall restricts access with the intention of “**influencing users to give consent**”.

- Without a genuine free choice, consent is invalid
- Still, the right to data protection is not absolute



➤ **France:** cookie walls are “**not compatible with the GDPR**”, because individuals cannot exercise their choice without detriment (i.e., refusal of cookies means no access).

# Cookie Walls (cont'd)

---

- **Austria:** cookie walls are not prohibited as long as they provide a degree of choice that results in freely given consent, and the user
- Is in full control of the situation, and
  - Can withhold consent by entering into a paid subscription or leaving the website



- **Netherlands:** consent is not freely given if a cookie wall is a “**take it or leave it**” proposition.
- There should be an alternative so that the user can access a website even if cookies are declined.

# What if personal data are collected?

---

## **DPAs have started to push cookie compliance forward in anticipation of the finalization of the ePrivacy Regulation**

- DPAs have brought enforcement actions where the use of cookies has resulted in a processing of personal data

## **Most likely area of overlap between cookies and personal data: (cross-site) tracking cookies**

- GDPR provides that unique (**online**) identifiers can amount to personal data, in particular when they are used to gather data about a user's preferences or to create a profile about him or her
- A tracking cookie records a user's behaviour. Depending on the data collected, it may be able to be used to compile preferences or a profile

# What if personal data are collected? (ct'd)

---

## Need for a legal basis (art. 6 GDPR)

- In principle, can be any of the legal bases, including performance of a contract and legitimate interest, but, in practice, may often be consent (depending on how the data are used)

## Transparency (art. 13 GDPR)

- May need to be more specific in informing users how tracking cookies are used and with whom the data collected is shared

## Individual's rights (art. 15 GDPR and further)

- There are no access and correction rights under ePrivacy, but there are under GDPR

**Brings cookie enforcement within the realm of GDPR and thus also the GDPR fines**

# Enforcement: *Planet49*

---

- **ECJ case on Planet 49** (March 2019)
- The Advocate General considered whether it makes a difference whether the data stored or accessed through cookies qualifies as personal data
- The answer: **no**. The obligation to obtain consent to the use of cookies applies regardless of whether personal or non-personal data is processed
- **Why?**
  - Article 5(3) of the ePrivacy Directive refers to the “**storing of information or the gaining of access to information already stored**”
  - Intended to protect the user from interference with his or her private sphere, regardless of whether the interference involves personal or other data

# Enforcement: *Google*

---

- **CNIL's action against Google** (January 2019)
- Complaints alleged “**forced consent**” by Android users to the entire Google privacy policy
- GDPR violations:
  - **Transparency** –
    - Overall lack of accessibility to essential information
    - Insufficiently clear and comprehensible disclosures
  - **Consent to processing for ad personalization** –
    - Not sufficiently informed
    - Not specific or unambiguous
- €50 million fine

# Practice Tips

---

## Determine approach to cookies

- Wait and see for ePrivacy?
- Update approach to consent in light of GDPR?
- Middle of the road: inventory cookies used + adopt a mechanism that allows for a degree of choice



## Determine roadmap

- *How many websites do you have?*
- *Which department oversees the use of cookies (IT, Communications, Marketing)?*
- *What kind of consent mechanism do you currently use?*
- *What process is used to introduce new cookies or to discontinue certain cookies?*
- *What approval processes are in place for updating cookies and the consent mechanism?*
- *How do you address legacy and decommissioned websites?*



# **GDPR: One Year Later**

# GDPR at the One Year Mark



## GDPR was a major event in 2018

Lots of guidelines issued and updated before May 2018



## Fewer guidelines issued after May 2018

Most notable one on applicability (which is still in draft)



## First signs of enforcement

Approx. 35 enforcement actions across approx. 12 countries

### Most notable:

- Google/CNIL enforcement (highest fine – €50 million)
- Four other enforcement actions with fines >€100,000
- Most enforcement actions have been about inadequate data security and resulting breaches, access rights and the use of sensitive personal data

**Still**, many DPAs have not yet enforced at all and their focus in the first year (as they had indicated) appears to have been on compliance

# Enforcement

---

- **One-stop-shop**
  - Addressed by the CNIL in Google matter
  - Determined that the one-stop-shop mechanism did not apply in this instance
    - Although Google has EU headquarters in Ireland, the Irish entity did not have decision-making power with respect to the particular processing and thus could not be considered Google's main establishment in the EU

**MORRISON**  

---

**FOERSTER**