Cybersecurity, Privacy and Communications Webinar: The Impact of the GDPR and the Proposed ePrivacy Regulation on Digital Advertising in Europe

April 19, 2018

Reed Freeman, Partner
Patrick Bernhardt, Senior Associate

WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Attorney Advertising

Speakers

Reed Freeman, Partner

Patrick Bernhardt, Senior Associate

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A box on the bottom right panel
- Questions will be answered as time permits
- Offering 1.0 CLE credit in California and New York*
- WebEx customer support: +1 888 447 1119, press 2

**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program may be able to claim England & Wales CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire program.*

Setting the Stage

Current privacy framework for digital advertising in Europe:

- Law: Data Protection Directive, until May 24, 2018
- Law: ePrivacy Directive, as amended by the "Cookie Directive" in 2009
- Self-Regulation: EDAA/IAB Europe EU Framework for Online Behavioural Advertising
- Self-Regulation: 2018 NAI Code of Conduct (for NAI members)

The new heavyweights:

- General Data Protection Regulation (GDPR), effective May 25, 2018
- Regulation on Privacy and Electronic Communications ("ePrivacy Regulation") proposed by the EU Commission on January 10, 2017, and currently under consideration by the EU Council (latest version from Parliament here (10.20.2017); latest version from Bulgarian Presidency here (March 7, 2018)

GDPR: Application to Digital Advertising

Definition of "personal data" under the GDPR is broad

- Includes location data and "online identifiers" that likely encompass cookie IDs, mobile ad IDs, IP addresses, statistical IDs, and other persistent online IDs used in online advertising
- "Pseudonymous" data is still personal data

Applies to controllers and processors not established in the EU, if processing activities relate to:

- The offering of goods or services to individuals in the EU, or
- The monitoring of individuals' behavior to the extent their behavior takes place within the EU

Strict data protection compliance regime with severe penalties for violations, up to €20 million or 4% of a company's global revenue, whichever is higher

GDPR: Key Questions for the Online and Mobile Advertising Industry

1. What are the legal bases for processing data under the GDPR and what do they mean for the digital ad tech industry? Can we rely on legitimate interests or do we need consent?
2. What do we need consent for under the existing ePrivacy Directive, and how does obtaining that consent differ once the GDPR is effective on May 25 (e.g., how does implied consent with cookie consent banners change once we need GDPR style consent)?
3. How would the proposed ePrivacy Regulation change the concept of consent under the GDPR? Would companies be able to rely on legitimate interests?
4. How does consent revocation work? Data subject access rights?
5. How does the WP 29 guidance work with the actual regulation? Guidance suggests that a pay wall would be disallowed in lieu of consent for data collection, but how would companies be able to provide content for free?
6. What is the role of the DPO? Must the DPO be an employee of the company or can an outside organization offer those services?
7. How does the GDPR's private right of action affect the litigation landscape in the EU? Can we expect an onslaught of class action lawsuits on May 25?

GDPR: Key Differences from the Data Protection Directive

Extensive documentation requirements

- *E.g.*, Article 30 requirement to maintain records of processing activities

Heightened consent requirements

- *E.g.*, Article 4 defines consent to require "unambiguous" indication by "statement or by a clear affirmative action"

Profiling is expressly addressed

- *E.g.*, Article 21 right to object to profiling for direct marketing purposes

Detailed access, correction, and deletion rights

- *E.g.*, Article 15 (Access), Article 16 (Rectification), Article 17 (Right to be Forgotten), Article 18 (Restrictions on processing), Article 19 (Obligation to notify third parties of restrictions)

GDPR: Key Differences from the Data Protection Directive

Detailed contractual requirements for controller-processor arrangements

- *E.g.*, Article 28

Data breach notification requirements

- *E.g.*, Article 33 and Article 34 require notification to DPA and individuals

Data protection impact assessments (DPIAs) required in certain circumstances

- *E.g.*, Article 35 requires DPIAs where processing "is likely to result in a high risk to the rights and freedoms" of individuals and "in particular using new technologies"

Data protection officer (DPO) requirements

- *E.g.*, Article 37, Article 38, and Article 39 govern the appointment and tasks of DPO

GDPR: Article 29 Working Party Guidelines

Provide detailed and specific guidance on how the GDPR may apply; Best indication yet for how DPAs intend to interpret and enforce the GDPR, but Guidelines are not law.

- Right to data portability
- Data protection officers
- Identifying a lead supervisory authority
- Data protection impact assessments
- Data breach notification
- Automated decision-making and profiling
- Application and setting of administrative fines
- Consent
- Transparency
- Binding Corporate Rules

GDPR: Legal Bases for Processing Data

Article 6 requires a lawful basis for processing, including where:

- "[T]he data subject has given **consent** to the processing . . . for one or more specific purposes"
- "[P]rocessing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject . . ."

Recital 47 describes when legitimate interests may apply:

- ". . . the existence of a legitimate interest would need **careful assessment** including whether a **data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place** . . ."
- " . . . **direct marketing purposes may be regarded as carried out for a legitimate interest**."

WP 29 Guidelines on Profiling suggest that, under Opinion 06/2014, it will be difficult to rely on legitimate interests for profiling/tracking in OBA context

GDPR: Interactions with ePrivacy Directive

But . . . the ePrivacy Directive requires consent for the use of cookies and similar technologies

- Article 95 of the GDPR grandfathers the ePrivacy Directive

Article 94 of the GDPR states that "[r]eferences to the repealed Directive shall be construed as references to this Regulation"

- *E.g.*, definition of consent under GDPR applies to ePrivacy Directive

Uncertainty whether "legitimate interests" will be added to the proposed ePrivacy Regulation as a new legal basis for the use of cookies and similar technologies, but in the meantime, consent is required

GDPR: What is "consent?"

Existing standards for consent under ePrivacy Directive:

- Consent requirements vary greatly across EU Member States
- *E.g.*, notice and opt-out (Italy) or "soft" opt-in (France), via placement of "cookie banners"

Article 4 defines consent under GDPR:

- "[A]ny freely given, specific, informed and **unambiguous** indication of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the processing of personal data."
- "Unambiguous" consent is less than "explicit" consent, but more than opt-out

Recital 32 addresses existing "soft opt-in" or "implied consent" models:

- "[Consent] could include ticking a box when visiting an internet website, choosing technical settings for information society services **or another statement or conduct which clearly indicates in this context the data subject's acceptance** of the proposed processing of his or her personal data."
- "**Silence, pre-ticked boxes or inactivity should not therefore constitute consent**."

GDPR: What is “consent?”

Article 6 and Article 7 contain additional requirements for consent:

- Companies must be able to demonstrate that consent was obtained
- Consent must be specific, informed, and separate for each purpose
- Data subjects must be able to withdraw consent at any time
- Presumption that consent is not “freely given” if consent is tied to provision of services and the processing is not necessary for the performance of the contract/services

Article 29 Working Party Draft Guidelines on Consent (WP 259) indicate how DPAs may interpret and enforce consent requirements

- Guidelines suggest that “pay walls” would not be allowed, but do not provide a solution for ad-supported websites if data subjects do not consent
- Guidelines also do not specifically address consent rules for third parties, who do not have direct relationships with consumers

GDPR: Revocation of Consent and Access, Correction, and Deletion Rights

Article 7 governs revocation of consent:

- Must provide ability for data subject to withdraw consent "at any time"
- Must be "as easy to withdraw as to give" consent
- Withdrawal does not affect the lawfulness of processing before withdrawal

Articles 15-20 provide for data subject access, correction, and deletion rights:

- *However*, Article 11 states that such obligations do not apply if the controller can demonstrate that it cannot identify the data subject without additional information (*e.g.,* if processing "pseudonymous" data), except where the data subject provides additional information to exercise his or her rights
- In OBA context, transparency/choice tools may emerge as industry standard or best practice—Article Working Party Guidelines on Profiling provide some general recommendations

GDPR: Restrictions on Profiling

The GDPR expressly addresses profiling:

- Article 4 defines "profiling" as "any form of automated processing … to evaluate certain personal aspects . . . in particular to analyse or predict aspects concerning that natural person's . . . economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."
- Articles 13, 14, and 15 require notice of the existence and consequences of profiling, "meaningful information about the logic involved," and rights to object to profiling under Article 21

Article 22 generally requires "explicit consent" for decisions based on profiling that produce legal or similarly significant effects

- "Explicit consent" is not defined, but presumably requires an express, written statement

Article 29 Working Party Guidelines on Automated Individual Decision-Making and Profiling (WP 251) indicate that targeted advertising based on profiling will not *typically* have "similarly significant effects," but that it could in certain cases

GDPR: Data Protection Impact Assessments

Article 35 requires data protection impact assessments (DPIAs) where:

- Processing "is likely to result in a high risk to the rights and freedoms" of individuals, "in particular using new technologies"

Data protection impact assessments:

- Must be carried out prior to processing, and revisited if risks change
- May be specifically required (or not required) based on public lists established by DPAs
- Should be overseen by data protection officer
- Must describe processing, assess proportionality and risks, and consider risk mitigation
- May require consultation with DPA if there are high risks in absence of risk mitigation

Article 29 Working Party Draft Guidelines on Data Protection Impact Assessments (WP 248) provide additional guidance

GDPR: DPO Requirements

Article 37 requires designation of DPO where core activities involve processing operations that "by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale"

Regulators expect DPOs to:

- Report directly to "highest management level"
- Have expertise commensurate with the sensitivity, complexity, and amount of data processed, as well as a sufficient level of involvement, resources, and independence
- Be free conflicts of interest on the business side and accessible from EU (e.g., located in EU, even for non-EU establishments in many cases)

External DPO may fulfill role "on the basis of a service contract"

Article 29 Working Party Draft Guidelines on Data Protection Officers (WP 243) provide additional guidance

GDPR: Potential Litigation

GDPR provides individuals and/or consumer associations with rights to:

- Lodge complaints against a supervisory authority (Article 77 and 80(2))
- Seek judicial remedy against a supervisory authority (Article 78 and 80(1))
- Seek judicial remedy against a controller or processor (Article 79 and 80(1))
- Obtain compensation for "material or non-material damage" (Article 82 and 80(1))

Joint and several liability for controllers and processors, except where a controller or processor can prove it is not responsible for damages

Heightened risk of lawsuits initiated by data subjects and consumer associations, as well as disputes with joint controllers and processors

Possible need to (in parallel) defend against supervisory authorities

ePrivacy: From Directive to Regulation

History

- ePrivacy Directive initially adopted in 2002
- Amended by so-called “Cookie Directive” in 2009
- Currently under review to harmonize with GDPR, address technological advancements, and change to a Regulation (which has direct effect in member states)

Status of proposed ePrivacy Regulation

- EU Commission proposed initial draft text on January 10, 2017
- Article 29 Working Party and European Data Protection Supervisor (EDPS) published opinions on proposed text (see here and here)
- European Parliament approved amended text on October 26, 2017
- EU Council consulting with member states on various issues to establish its position in advance of “trilogue” negotiations, which likely will not start before fall 2018

ePrivacy: Key Proposals Applicable to Online and Mobile Advertising

Proposed ePrivacy Regulation applies to **all electronic communications data**—not just personal data

Articles 8 requires **consent (as defined in GDPR) for the use of cookies or similar technologies**, except where necessary for providing the services or for limited first-party web audience measurement

Article 9 authorizes the **use of browser or software settings** to express consent

Article 10 requires software providers to: (a) **offer a means to stop data collection**; (b) **inform users about privacy settings options upon installation**; and (c) require end users to **consent to each setting during installation**

Article 16 requires **consent for direct marketing** (*e.g.*, email and text)

ePrivacy: Key Issues under Discussion

1. **Adding legitimate interest as a legal basis** (**coupled with opt-out**) for using cookies and similar technologies to deliver targeted advertisements, and other exceptions to consent (EU Council)
2. **Prohibiting further processing on the basis of other legal grounds allowed under GDPR**, even if the initial processing is allowed under the ePrivacy Regulation (EDPS, EP, WP29)
3. **Prohibiting "tracking walls"** (EDPS, EP, WP29)
4. **Requiring companies to comply with browser or software privacy settings** or other accepted technical and policy compliance standards (EDPS, EP)
5. **Requiring browser and software settings to be privacy-protective by default** (EDPS, EP, WP29) and/or making other adjustments to browser and software privacy settings (EP, EU Council)
6. **Imposing additional restrictions on first-party analytics** without consent (data must be aggregated and kept separate from data collected on other sites, and opt-out must be provided) (EP)
7. **Establishing standalone definitions** that do not rely on the telecommunications code (EDPS, EP)

ePrivacy: Impacts on Consent

It remains to be seen whether legitimate interests (coupled with opt-out) will be added as a legal basis for online advertising

Under current proposals, consent likely will shift from a "cookie banner" approach to one that relies on browser and software privacy settings

- The amended text proposed by the European Parliament would require that browser or software privacy settings "**shall be binding on, and enforceable against, any other party**"
- It also requires the European Data Protection Board to issue guidelines and determine the technical specifications and signaling methods that would fulfill the conditions for consent

There is a possibility that browser and software settings will need to be "privacy-protective" by default, which poses challenges for third parties

"Tracking walls" may be prohibited

Industry Initiatives on GDPR and ePrivacy Regulation

Interactive Advertising Bureau Europe (IAB Europe) established a GDPR Implementation Working Group to provide guidance to the advertising industry:

- GDPR Compliance Primer
- Working Paper on the Definition of Personal Data
- Working Paper on GDPR Consent
- Working Paper on Data Subject Requests

On Feb. 9, 2018, the IAB Tech Lab announced an OpenRTB Advisory that specifies how to pass user consent signals via an OpenRTB protocol, and it launched a GDPR Technical Working Group

On March 8, 2018, IAB Europe released draft technical specifications for its GDPR Transparency and Consent Framework—vendors and consent management providers can apply for approved status now

Finally, IAB UK has released a draft factsheet on the proposed ePrivacy Regulation

Takeaways

1. **Q: What are the legal bases for processing data under the GDPR and what do they mean for the digital ad tech industry? Can we rely on legitimate interests or do we need consent?**
   - *A: It **may** be possible to rely on legitimate interests for processing data for direct marketing, but the ePrivacy Directive requires consent for the use of cookies and similar technologies.*
2. **Q: What do we need consent for under the existing ePrivacy Directive, and how does obtaining that consent differ once the GDPR is effective on May 25 (e.g., how does implied consent with cookie consent banners change once we need GDPR style consent)?**
   - *A: The ePrivacy Directive requires consent for the use of cookies and similar technologies and will use GDPR's definition of consent after May 25, 2018—requires "unambiguous" indication by "statement or by a clear affirmative action."*

Takeaways

3. **Q: How would the proposed ePrivacy Regulation change the concept of consent under the GDPR? Would companies be able to rely on legitimate interests?**
   - *A: At the moment, it's unclear whether the proposed ePrivacy Regulation will be amended to allow processing based on legitimate interests for digital advertising. The proposed ePrivacy Regulation may have the effect of replacing cookie banners with browser and software privacy settings.*
4. **Q: How does consent revocation work? Data subject access rights?**
   - *A: It must be "as easy to withdraw as to give" consent. Data subject access rights depend on whether personal data is "pseudonymized," but transparency tools may emerge as a best practice.*
5. **Q: How does the WP 29 guidance work with the actual regulation? Guidance suggests that a pay wall would be disallowed in lieu of consent for data collection, but how would companies be able to provide content for free?**
   - *A: Article 29 Working Party guidelines are not law, but they indicate how DPAs will interpret and enforce the GDPR. The guidelines do not provide a solution for ad-supported websites if data subjects do not consent.*

Takeaways

6. **Q: What is the role of the DPO? Must the DPO be an employee of the company or can an outside organization offer those services?**
   - *A: The DPO role must be built around GDPR's numerous requirements, but a company can designate an external DPO that is capable of meeting those requirements.*
7. **Q: How does the GDPR's private right of action affect the litigation landscape in the EU? Can we expect an onslaught of class action lawsuits on May 25?**
   - *A: New rights to seek judicial remedies and obtain compensation will lead to a heightened risk of lawsuits initiated by data subjects and consumer associations, potential disputes with joint controllers and processors, and a need to (in parallel) defend against supervisory authorities.*

Questions?

Reed Freeman, Partner
reed.freeman@wilmerhale.com
+1 202 663 6267

Patrick Bernhardt, Senior Associate
patrick.bernhardt@wilmerhale.com
+1 202 663 6549

**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program may be able to claim England & Wales CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire program.*