CNIL
Commission Nationale de l'Informatique et des Libertés

DNT & EU Legislation

Vincent Toubiana

Current status in EU

- **Web Tracking is currently regulated by two Directives:**
  - Data Protection Directive (95/46/EC)
  - ePrivacy Directive (2002/58/EC)

- **Directives were transposed, ambiguity around key concepts :**
  - Personal data & anonymous,
  - Consent (e.g. implicit vs explicit).

- **Different compliance requirements in the 28 countries,**
  - WP29 (EU Data Protection Authorities) Opinions harmonize EU regulation.

General Data Protection Regulation

- **GDPR was adopted in May 2016 and will be fully applicable starting May 2018**
- **Unlike previous Personal Data legislation, it's a *Regulation* not a *Directive*:**
  - No transposition in local laws,
  - The same text will be fully applicable in the 28 countries.
- **What's new in the text:**
  - Personal data definition includes "Online identifiers" ,
  - "Consent" and "Legitimate Interest" remains legal basis for data processing (among others) but…

Consent
Through technical setting

ePrivacy 2009 (recital 66)

Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes […]. The methods of providing information and offering the right to refuse should be as user-friendly as possible […]. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application.

GDPR (recital 32)

Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This 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.

Consent
Through technical setting

ePrivacy 2009 (recital 66)

Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes […]. The methods of providing informati[illegible] should b[illegible] Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application.

When consent is the legal basis, user MUST be able to revoke it.

GDPR (recital 32)

Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data [illegible] a written [illegible], or an oral statement. This 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.

Legitimate Interest & Right to object (Article 21)

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

Legitimate Interest & Right to object (Article 21)

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

Even when you have legitimate interest (no consent required)…

Legitimate Interest & Right to object (Article 21)

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

Even when you have legitimate interest (no consent required)…

… you should pay attention to DNT.

Legitimate Interest & Right to object (Article 21)

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Even when you have legitimate interest (no consent required)…

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

Especially for marketing purpose!

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

… you should pay attention to DNT.

ePrivacy review

- **The review of the ePrivacy directive is in progress:**
  - ePrivacy could be:
    - A Directive (transposition needed)
    - A Regulation like GDPR.
  - ePrivacy could rely on DNT,
    - Coherent with recital 66 of 2002/58/EC,
    - Data Protection Authorities (DPA) are encouraging DNT support.

- **DNT could be used to obtain consent.**

Opinions on ePrivacy Directive Review

European Data Protection Supervisor

Finally, the EDPS emphasizes that users must have user friendly and effective mechanisms to provide and revoke their consent. The EDPS recommends, building on recital 66 of the Users' Rights Directive referred above, that the new provisions for ePrivacy provide for a workable legislative requirement ensuring that the user's consent to the processing could be expressed by using the appropriate settings of a browser or another application. This means that instead of merely relying on website operators to obtain consent on behalf of third parties (such as advertising and social networks), the new legal instrument for ePrivacy can require that browsers and other software or operating systems offer control tools within the browser (or other software or operating system) such as Do Not Track (DNT), or other technical means that allow users to easily express their consent or lack thereof.

Such tools must be offered to the user at the initial set-up with privacy-friendly default settings. Adherence to accepted technical and policy compliance standards by all parties concerned, including the operators of the website, should become obligatory.

Link:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-07-22_Opinion_ePrivacy_EN.pdf

Article 29 (EU DPAs)

When consent is the applicable legal basis, users must be provided with truly easy (user friendly) means to provide and revoke consent. The Working Party recommends rephrasing the requirements in the current Recital 66 of Directive 2009/136/EC. Instead of relying on website operators to obtain consent on behalf of third parties (such as advertising and social networks), manufacturers of browsers and other software or operating systems should be encouraged to develop, implement and ensure effective user empowerment, by offering control tools within the browser (or other software or operating system) such as Do Not Track (DNT), or other technical means that allow users to easily express and withdraw their specific consent, in accordance with Article 7 of the GDPR. Such tools can be offered to the user at the initial set-up with privacy-friendly default settings.

Adherence to accepted technical and policy compliance standards must become a common practice. In addition, website operators should respect and adhere to browser control tools or other user preference settings.

Link: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf

CNIL.

Conclusion

- **GDPR will require at least a way to opt-out through « automated means » in 2018,**
- **EU DPAs explicitly push for DNT support,**
- **No explicit mention of « Self regulation efforts » or « Opt-out » cookies.**

Discussion: Using W3C for EU Compliance

- **How can W3C DNT simplify EU compliance?**
- **How will W3C DNT signals be supported by sites?**
- **Member support for plugfest / TPWG?**

Cookie IDs are Personal Data

Definition of Personal Data:

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

CalOPPA (2013 amendment)

(a) An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site, or in the case of an operator of an online service, make that policy available in accordance with paragraph (5) of subdivision (b) of Section 22577. An operator shall be in violation of this subdivision only if the operator fails to post its policy within 30 days after being notified of noncompliance.

(b) The privacy policy required by subdivision (a) shall do all of the following:

(1) Identify the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.

(2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process.

(3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy for that Web site or online service.

(4) Identify its effective date.

(5) Disclose how the operator responds to Web browser "do not track" signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third-party Web sites or online services, if the operator engages in that collection.

(6) Disclose whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different Web sites when a consumer uses the operator's Web site or service.

(7) An operator may satisfy the requirement of paragraph (5) by providing a clear and conspicuous hyperlink in the operator's privacy policy to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice.