TILBURG LAW REVIEW
Journal of International and European Law

Curtailing the Cookie Monster through Data Protection by Default

RESEARCH ARTICLE

PAARTH NAITHANI

ubiquity press

ABSTRACT

Cookies are an important part of today's internet but all is not well with cookie consent. Various designs and defaults settings are being used to influence consent to store third party cookies and tracking cookies on user devices. Dark patterns, complex options to reject cookies and privacy-infringing default settings are being used to manipulate users into tracking, profiling and behavioural advertising. User privacy is suffering and there is a clear need to curtail the use of cookies. This article proposes that cookies can be curtailed by default using an important principle under data protection law which is data protection by default. The article looks at the present and proposed law on cookies, recent decisions in respect of cookies, and the requirements of data protection by default. The article proposes data protection by default settings for browsers and websites in respect of cookies. It also makes recommendations for the upcoming cookie law in the EU, the proposed ePrivacy Regulation.

CORRESPONDING AUTHOR:

Paarth Naithani

Assistant Lecturer, O.P. Jindal Global University, Sonipat, India

pnaithani@jgu.edu.in

KEYWORDS:

Cookies; Data protection by default; ePrivacy Regulation; ePrivacy directive; General Data Protection Regulation (GDPR); Internet browsers – Websites

TO CITE THIS ARTICLE:

Paarth Naithani, 'Curtailing the Cookie Monster through Data Protection by Default' (2022) 27(1) *Tilburg Law Review* pp. 22–36. DOI: https://doi.org/10.5334/tilr.311

DOI: 10.5334/tilr.311

1 INTRODUCTION

There are many concerns with the use of cookies for tracking, profiling and behavioural advertising. First, there is a power and information asymmetry as most processing is invisible and there is opacity in online tracking.[1] Second, there is excessive processing of people's preferences which can enable manipulation.[2] Third, there is a likelihood that data collected can be misused for secondary and incompatible purposes.[3] Fourth, such practices can cause chilling effects on individuals who might alter their behaviour if they believe they are being tracked.[4] Ultimately, it leads to reduced trust and confidence in digital services and lesser voluntary data sharing or use of digital services.[5]

Given the above concerns, it becomes important to assess what happens when users do not make any privacy choice with respect to cookies. One needs to understand the idea of default settings. These are the preselected settings that would not change unless users themselves change the settings. These default settings govern how the system would work if nothing is changed.[6]

Default settings are important as they decide what happens when users don't change or are not willing to change the settings.[7] Default setting are important also because it is not very intuitive to control flows of personal data using technical settings.[8] As per studies, majority of people do not change default privacy settings.[9] There is a lack of awareness of data privacy settings.[10] For instance, users generally lack understanding of the ways to opt-out.[11] Thus, default settings are crucial as they decide the privacy settings of the majority of the people. Default settings are even more crucial for vulnerable groups such as children and elderly.[12] These groups may not be aware of privacy or how to change privacy settings.

Default settings are also important from the point of view of behavioural economics as reflected below -

> "*[F]irst, that any default chosen will be 'sticky,' meaning that more consumers stay with the default than would explicitly choose to do so if forced to make a choice. Second, that those consumers with a preference for the opt-out position -and only those consumers-will opt out. Third, that where firms oppose the default position, they will be forced to explain it in the course of trying to convince consumers to opt out, resulting in well- informed decisions by consumers.*"[13]

---

1 Information Commissioner's Office (ICO) UK, 'Information Commissioner's Opinion: Data protection and privacy expectations for online advertising proposals' (25 November 2021) <https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf> accessed 16 March 2022. (ICO, UK Opinion: Data protection and privacy expectations for online advertising proposals).

2 Ibid.

3 Ibid.

4 Ibid.

5 Ibid.

6 European Union Agency for Cybersecurity (ENISA), 'Recommendations on shaping technology according to GDPR provisions – An overview on data pseudonymisation' (28 January 2019) <https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions> accessed 16 March 2022. (ENISA Recommendations on shaping technology according to GDPR provisions).

7 Ibid.

8 Jef Ausloos, Els Kindt, Eva Lievens, Peggy Valcke and Jos Dumortier, 'Guidelines for Privacy-Friendly Default Settings' (18 February 2013) ICRI Research Paper No. 12/2013 <https://ssrn.com/abstract=2220454> accessed 16 March 2022. (Guidelines for Privacy-Friendly Default Settings).

9 Ibid.

10 Article 29 Data Protection Working Party, 'Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising' (8 December 2011) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf> accessed 16 March 2022. (A29 WP Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising).

11 Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising' (22 June 2010) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf> accessed 16 March 2022. (A29 WP Opinion 2/2010 on online behavioural advertising).

12 Lina Jasmontaite , Irene Kamara, Gabriela Zanfir-Fortuna & Stefano Leucci, 'Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR' (2018) 4 Eur Data Prot L Rev 168.

13 Damian Clifford, 'EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster – Tracking the Crumbs of Online User Behavior' (2014) 5 J Intell Prop Info Tech & Elec Com L 194.

DOI: 10.5334/tilr.311

Despite the importance of default settings, they are often set in a way that does not respect privacy.[14] Moreover, systems are designed in ways that do not enforce privacy but rather infringe privacy.[15] For instance, it is not uncommon to see that consent is not asked, and users need to opt-out of processing.[16] It often takes high efforts to change privacy settings and there is lack of awareness of how to change the settings.[17] Often, dark patterns are used to nudge people towards tracking.[18] These dark patterns are a way of manipulating the user into a setting that is privacy infringing.

Default privacy invasive settings are in stark contrast with user expectations. Studies and surveys suggest that the public's reasonable expectations are that defaults must be privacy preserving. As per the Eurobarometer survey on ePrivacy cited in the proposed Regulation on Privacy and Electronic Communications (hereinafter proposed ePrivacy Regulation), "*89% agree with the suggested option that the default settings of their browser should stop the sharing of their information.*"[19] As per public consultations organised by the EU Commission, "*81.2% of citizens and 63% of public authorities support imposing obligations on manufacturers of terminal equipment to market products with privacy-by-default settings activated.*"[20]

Given the user expectations and importance of default settings, this article studies how default browser and website settings for cookies should respect the principle of data protection by default. With an introduction in Section 1, the paper discusses the requirement of data protection by default in Section 2. Section 3 provides a background discussion to help explain what cookies are, how the EU regulates cookies, and how the EU proposes to regulate cookies. A perusal of this section shows that while the ePrivacy law in the EU regulates cookies through consent, it does not explicitly recognise the requirement of data protection by default. In Sections 4 and 5, the paper proposes that data protection by default must apply to websites and browsers in respect of cookies.

2 UNDERSTANDING DATA PROTECTION BY DEFAULT

According to Ann Cavoukian, who laid down seven principles of privacy by design, one's privacy must remain intact even if the person does not do anything.[21] Privacy must be built into the system by default and no action must be required by the individual to protect privacy.[22] Ann Cavoukian proposed the principle of privacy as default setting.[23] This principle requires that by default non-identifiable interactions and transactions must be designed into programs, systems and ICT.[24]

A concept with similar thrust of ideas[25] has been introduced by the General Data Protection Regulation (GDPR) requirement of data protection by default, although there is a difference. The difference is that privacy by design and data protection by design focus on different subject matter for protection which are privacy and right to protection of personal data respectively.[26]

14 ENISA Recommendations on shaping technology according to GDPR provisions (n 6).

15 Ibid.

16 Ibid.

17 Ibid.

18 Ibid.

19 Proposal for a Regulation 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), COM/2017/010 final – 2017/03 (COD). (Proposed ePrivacy Regulation).

20 Ibid.

21 Guidelines for Privacy-Friendly Default Settings (n 8).

22 Ibid.

23 Daniela Ježová, 'Principle of Privacy by Design and Privacy by Default' (2020) <https://doi.org/10.18485/iup_rlr.2020.ch10> accessed 16 March 2020.

24 Ibid.

25 Lee A. Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4(2) Oslo Law Review 105–120 <https://ssrn.com/abstract=3035164> accessed 16 March 2022.

26 Lina Jasmontaite , Irene Kamara, Gabriela Zanfir-Fortuna & Stefano Leucci, 'Data Protection by Design and by Default' (n 12).

This article focuses on data protection by default and not privacy by design. Data protection by default is a requirement under the EU GDPR, and the article proposes how data protection by default should apply in respect of cookies.

Article 25 of the GDPR[27] lays down the requirement of data protection by default. The implementation of technical and organisational measures must ensure that by default "*only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.*" The requirement is thus of "*minimally intrusive processing: minimum amount of personal data, minimum extent of processing, minimum storage period and minimum accessibility to personal data.*"[28]

Data protection by default can be seen as a culmination of various principles including data minimisation, purpose limitation, necessity, retention limitation, confidentiality etc. First, "*the less data, the better*" or data must be collected in a "*need to know*" basis.[29] Second, there must be minimal processing or "*the less processing the better*".[30] This would include avoiding use of data for profiling and tracking.[31] Third, the storage period is "*the minimum the better*".[32] Importantly, these conditions must prevail without the need for the data subject to intervene.[33]

Data protection by default is further explained by Recital 78 of GDPR which requires transparency in the processing, enabling monitoring of data processing by data subjects and pseudonymization of personal data as soon as possible. The EDPB has also explained data protection by default in its Guidelines on Article 25.[34] By default, processing settings and options must be implemented in a way that only that processing is carried out by default which is "*strictly necessary*" to achieve the set lawful purpose.[35] The boundaries of compatible purposes must not be extended and the reasonable expectations of the data subject must be considered.[36] The retention period must be limited to that necessary for the purpose of processing.[37] The storage of personal data must be limited by the conditions of necessity, compatible purpose and legal grounds under Article 6(4).[38] The processing must not permit the identification of data subjects for longer than is necessary for purposes of processing.[39]

The EDPB explained that various data protection principles need to be implemented to achieve the principle of data protection by design and default (data protection by default and data protection by design are two separate but interrelated principles of which data protection by default is the focus of this article). While implementing the lawfulness principle, the elements to be considered include autonomy of the data subject, consent of the data subject and the ease of withdrawal of consent.[40] Consent must be specific, informed, freely given and unambiguous, and withdrawal of consent must be as easy as giving consent.[41] While implementing the

27 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, 1–88.

28 Spanish Data Protection Authority (AEPD), 'Guidelines for Data Protection by Default' (2020) <https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto-en.pdf> accessed 16 March 2022. (AEPD Guidelines for Data Protection by Default).

29 ENISA Recommendations on shaping technology according to GDPR provisions (n 6).

30 Ibid.

31 Ibid.

32 Ibid.

33 AEPD Guidelines for Data Protection by Default (n 28).

34 European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (20 October 2020) <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en> accessed 16 March 2022. (EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default).

35 Ibid.

36 Ibid.

37 Ibid.

38 Ibid.

39 Ibid.

40 Ibid.

41 Ibid.

fairness principle, the reasonable expectations of the data subjects must be considered.[42] The vulnerabilities of data subjects must not be exploited.[43] Dark patterns must not be used as they are "*contrary to the spirit of Article 25*".[44]

Overall, data protection by default is not just a GDPR requirement but also a way of putting user needs as a starting point.[45] It is a way of meeting user expectations and also of developing user trust.[46]

3 UNDERSTANDING COOKIES

3.1 COOKIES

Cookies are small text files stored on devices that connect to the internet. Cookies can serve various functions like remembering user actions on a website, keeping track of information entered on a website and authenticating users accessing an online service.[47] Cookies can also be used for privacy invasive functions such as tracking, profiling and behavioural advertising.

Cookies are categorised as first party cookies if the host website stores the cookie. When a user visits a website, it is not just the host domain that stores cookies on the user device. Cookies are also stored by domains other than the host domain. Usually, Like buttons and social plugins on the host website facilitate third parties to store cookies. These cookies are referred to as third party cookies. Some sites allow third party cookies from multiple ad-networks to be placed on the user device, sometimes upto 200 separate cookies.[48]

Cookies can also have an expiry date and are classified as session cookies or persistent cookies depending on their expiry immediately after closing the browser or later than that.

3.2 ePRIVACY DIRECTIVE

The present EU-wide law on cookies is the Directive on Privacy and Electronic Communications (ePrivacy Directive).[49] The requirement of Article 5(3) of ePrivacy directive is that prior consent must be taken before cookies are placed on the user device.[50] Consent must be obtained only after prior information about cookies is provided.[51]

The exceptions under Article 5(3) are "*technical storage or access for the sole purpose of carrying out the transmission of a communication*" and strict necessity to provide explicitly requested information society service. When these exceptions do not apply, there is a need for prior consent and prior information. Cookies that merely assist or speed up transmission over communication are not necessary for the "*technical storage or access for the sole purpose of carrying out the transmission of a communication*".[52] Such cookies require prior consent and prior information before they are stored on user devices. Cookies that can be exempted under

42 Ibid.

43 Ibid.

44 Ibid.

45 ENISA Recommendations on shaping technology according to GDPR provisions (n 6).

46 Ibid.

47 Data Protection Commission, Ireland, 'Guidance Note: Cookies and other tracking technologies' (April 2020) <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf> accessed 16 March 2022. (DPC, Ireland Guidance Note: Cookies and other tracking technologies).

48 Matthew S. Kirsch, 'Do Not Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising›, (2011) 18 (1) Rich. J.L. & Tech <https://scholarship.richmond.edu/jolt/vol18/iss1/3> accessed 16 March 2022.

49 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, 37–47, as amended by Directive 2009/136/EC, OJ L 337, 18.12.2009, 11–36.

50 A29 WP Opinion 2/2010 on online behavioural advertising (n 11).

51 Ibid.

52 DPC, Ireland Guidance Note: Cookies and other tracking technologies (n 47).

the exception of strict necessity to provide explicitly requested information society service need to pass the dual test of explicitly requested and strict necessity.[53] It is important to note that tracking does not fall under either of the exceptions of Article 5(3).[54]

Recital 17 of Directive 2002/58 provides guidance on the requirement of consent under Article 5(3). It states that consent under the directive has the same meaning as consent under Directive 95/46 (replaced by GDPR). Thus, consent under Article 5(3) has the same meaning as consent under the GDPR.[55] As per Recital 32 of GDPR, consent must be through a clear affirmative act and through an unambiguous indication. As per Recital 32, consent should also be informed and specific. Consent must be an active 'indication' of user's wishes.[56] Consent must be freely given by leaving no room for deception or significant negative consequences for not consenting.[57] The user must have a real choice.[58]

The CJEU has interpreted Article 5(3) of the ePrivacy Directive and consent under GDPR in the *Planet49*.[59] The CJEU decided that a preselected tick in a checkbox is not valid consent for cookies as it does not constitute active behaviour.[60] The requirement of 'indication' is that the user behaviour must be active rather than passive.[61] The active behaviour requirement is also supported by the requirement of unambiguous consent.[62]

Various recent decisions of Data Protection Authorities such as the French Data Protection Authority (CNIL) have also interpreted the requirement of consent in the context of cookies. In CNIL decision against Google,[63] the facts involved seven cookies being placed on the arrival of user on a website before the user took any action.[64] Four of these cookies were tracking cookies.[65] No prior information was provided on the cookie banner about these cookies.[66] Prior consent was not sought for these cookies.[67] Thus, breach of obligations under data protection law was found.[68]

In a CNIL decision against Facebook,[69] CNIL found a breach of data protection law because it was not as easy to refuse cookies as it was to accept them. Free consent requires data subjects to have a real choice.[70] This requires opt-out mechanism to not be more complex than opting-

53 Ibid.

54 Article 29 Data Protection Working Party, 'Opinion 04/2012 on Cookie Consent Exemption' (7 June 2012) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf> accessed 16 March 2022. (A29 WP Opinion 04/2012 on Cookie Consent Exemption).

55 EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 16 March 2022.

56 Article 29 Data Protection Working Party, 'Working Document 02/2013 providing guidance on obtaining consent for cookies' (2 October 2013) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf> accessed 16 March 2022. (A29 WP Working Document 02/2013 providing guidance on obtaining consent for cookies).

57 Ibid.

58 Ibid.

59 Case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Ver- braucherzentrale Bundesverband eV v Planet49 GmbH, ECLI:EU:C:2019:801. (CJEU in Planet49 case).

60 Ibid.

61 Ibid.

62 Ibid.

63 French Data Protection Authority (CNIL), 'Deliberation of the Restricted Committee n° SAN-2020-012 of 7 December 2020 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED' <https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_restricted_committee_san-2020-012_of_7_december_2020_concerning_google_llc_and_google_ireland_limited.pdf> accessed 16 March 2022. (CNIL Deliberation against Google).

64 Ibid.

65 Ibid.

66 Ibid.

67 Ibid.

68 Ibid.

69 French Data Protection Authority (CNIL), 'Deliberation of the restricted committee No. SAN-2021-024 of 31 December 2021 concerning FACEBOOK IRELAND LIMITED' <https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_the_restricted_committee_no._san-2021-024_of_31_december_2021_concerning_facebook_ireland_limited.pdf> accessed 16 March 2022. (CNIL Deliberation against Facebook).

70 Ibid.

in.[71] This is pertinent because around 93.1% of Internet users only stop at the first level of cookie banners.[72] There is thus a need for a prominent reject all button.[73] Making it easy to accept all cookies by providing that option at the first level of a banner and making it complex to reject all cookies by providing the option at the second level of the banner is against data protection law.[74]

A recent European Data Protection Supervisor (EDPS) decision[75] has held that data subjects must consent to tracking cookies specially from third parties, analytics and social plug-ins. The decision goes on to consider even first party analytics to require consent as they "*are not strictly necessary to provide a functionality explicitly requested by the user*" (which is one of the two exceptions under Article 5(3) of ePrivacy directive).[76]

With respect to browsers and cookie settings, an important provision in the ePrivacy directive is Recital 66 which states that "*the user's consent to processing may be expressed by using the appropriate settings of a browser or other application*". This provision seems to indicate that the browser settings may be used to consent to cookies. But Recital 66's suggestion that browser settings can be used as a way to obtain consent is not an exception to Article 5(3).[77] Moreover, there are several reasons why a general browser setting cannot constitute a valid consent under ePrivacy directive and the GDPR (discussed later).

3.3 ePRIVACY REGULATION

There is a 2017 proposal to replace the ePrivacy Directive with a proposed ePrivacy Regulation.[78] There is also a revised version of this proposal which has emerged after further discussions (hereinafter Council's position on ePrivacy Regulation).[79]

Article 8 of the proposed ePrivacy Regulation provides that collection of information from devices and use of storage in devices can happen on various grounds. These include user consent, "*necessary for the sole purpose of carrying out the transmission*", for providing information society service requested by user, and web audience measuring carried out by provider of service requested by user.

The words "strictly" and "explicitly" have been omitted from the draft ePrivacy Regulation while laying down the ground similar to exception under Article 5(3) of ePrivacy directive which provides, "*strictly necessary in order to provide an information society service explicitly requested by the subscriber or user*".[80] These omissions are concerning because when users visits a website, the information society service "explicitly" requested by users is that which the website provides and not that of the ad service providers and most other third parties on the website. If the word "explicitly" is omitted, it can be argued that the ground includes services of even third parties on a website. This may lead to allowing third party cookies on the users' devices under the ground of information society service requested by users. The Council's position on ePrivacy Regulation has reconsidered the position under the proposed ePrivacy Regulation. The provision under Council's position on ePrivacy Regulation provides "*it*

71 Ibid.

72 Ibid.

73 Ibid.

74 Ibid.

75 European Data Protection Supervisor, 'Decision of the European Data Protection Supervisor in complaint case 2020-1013 submitted by Members of the Parliament against the European Parliament' <https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf> accessed 16 March 2022. (EDPS Decision against the European Parliament).

76 Ibid.

77 A29 WP Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising (n 10).

78 Proposed ePrivacy Regulation. (n 19).

79 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) – Mandate for negotiations with EP <https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf> accessed 16 March 2022.

80 Article 29 Working Party, 'Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)' (4 April 2017) <https://ec.europa.eu/newsroom/article29/items/610140> accessed 16 March 2022. (A29 WP Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)).

is 'strictly' necessary for providing a service 'specifically' requested by the end- user". The ground not only adds the word 'specifically' but also the word 'strictly' necessary. Third party cookies are not strictly necessary as they are related to service different from that "explicitly requested" by the users.[81] Thus, they should require consent. Moreover, analytics are not strictly necessary and should require consent.[82]

The proposed ePrivacy Regulation has created a ground of web audience measuring carried out by providers of services requested by users. This ground is concerning because first party can often be a social media site which can store a cookie on the user device under this ground. Later, the party may use this cookie to track the user across the web because once a cookie is stored, it can subsequently be read by the party when it acts as a third party on other websites. For example, a cookie placed by fr-fr.facebook.com under the web audience measuring exception can later be read by Facebook when a user visits a website which has a Facebook Like button. This is a potential loophole in the ground of web audience measuring.

Article 9 of the proposed ePrivacy Regulation provides for consent under Article 8(1) to be provided by technical settings of software which enable access to the internet. This provision seems to suggest that browser settings can be used for consent. But, as mentioned above general browser settings are unsuitable for providing consent as per GDPR by not being informed and specific enough.[83] There are other reasons why a general browser setting would not constitute a valid consent under the GDPR (discussed later). It is important to note that article 9 has been deleted from the Council's mandate on ePrivacy Regulation.

Article 10 of the proposed ePrivacy Regulation requires software that provide for retrieval and presentation of information from the internet to allow the option to prevent third parties from processing information stored in devices or storing information on devices. In other words, browsers should provide an option to reject all third party cookies. There is an issue with the terminology of "third party" in this provision because many first parties such as social media platforms may use tracking cookies.[84] An alternative is to instead use the terms site-wide and internet-wide.[85]

Article 10 of the proposed ePrivacy Regulation further provides that end-users must be required to consent to a setting while installing software. In other words, while installing browsers, users may need to make a choice regarding browser cookie settings. Browsers could provide options including "accept all cookies", "reject all cookies", "reject third party cookies" or "accept only first party cookies".[86] It is important to note that article 10 has been deleted from the Council's mandate on ePrivacy Regulation.

The provisions of the ePrivacy law and related decisions point to the requirements that non-necessary cookies should not be stored before a user consents. The consent requirement under the ePrivacy directive and the proposed ePrivacy Regulation varies as provisions are worded differently. Notably, both the ePrivacy directive and the proposed ePrivacy Regulation do not explicitly recognise the requirement of data protection by default. Data protection by default can provide strong protection to individuals in addition to the requirement of consent recognised under the ePrivacy law.

While the ePrivacy directive and proposed ePrivacy Regulation apply to cookies, there is a need to understand how data protection by default can apply to cookies. In this respect, an important question to ask is, can data protection by default under the GDPR apply to cookies?

---

81 Ibid.

82 Information Commissioner's Office (ICO) UK, 'Guidance on the use of cookies and similar technologies, ICO' <https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf> accessed 16 March 2022. (ICO, UK Guidance on the use of cookies and similar technologies).

83 A29 WP Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (n 80).

84 Ibid.

85 Ibid.

86 Daniela Ježová, 'Principle of Privacy by Design and Privacy by Default' (n 23).

4 DATA PROTECTION BY DEFAULT FOR COOKIES

4.1 CAN DATA PROTECTION BY DEFAULT APPLY TO COOKIES?

Recital 5 of the proposed ePrivacy Regulation states that it complements and particularised general rules under GDPR. The Recital further states that the ePrivacy Regulation does not lower the level of protection under the GDPR. Recital 23 of the proposed ePrivacy Regulation refers to the data protection by design and default principle under the GDPR while suggesting that browsers must offer users high, low and intermediate settings to never accept cookies, always accept cookies and reject third party cookies. It has been argued that there is a need for clarification that the data protection by default provision under Article 25 of the GDPR applies to the processing of information under the ePrivacy Regulation.[87]

In this respect, it is established that ePrivacy law (ePrivacy directive and proposed ePrivacy Regulation) is the lex specials whereas GDPR is the lex generalis.[88] If information consists of personal data, the GDPR comes into play and it has been suggested that most cookies constitute personal data.[89] Hence, the GDPR must apply to the processing of personal data through cookies and consequently, data protection by default must apply to cookies. This is especially true of tracking cookies whose purpose is to single out persons for purposes such as behavioural advertising. Since tracking cookies single out persons, they constitute personal data and data protection by default under GDPR must apply.

Even if the information does not constitute personal data, there is a case for data protection by default to apply under the proposed ePrivacy Regulation for two reasons. First, the proposed ePrivacy Regulation itself states under Recital 5 that it complements the GDPR and does not lower the protections under GDPR. This implies that data protection by default must apply under the ePrivacy Regulation. Second, studies point to the fact that it is desirable to have privacy protecting default settings because users generally do not change the default settings,[90] including for cookies. Thus, data protection by default must apply so as to cover cookies.

Another question to ask is who should the principle apply to? It seems that the principle of data protection by default is addressed primarily to the data controller.[91] It is clear from a CJEU judgement that websites need to comply with data protection law.[92] Thus, data protection by default would apply to websites. Besides, Recital 78 of the GDPR seems to indicate the requirement of data protection by default is towards "*producers of the products, services and applications*." This seems to suggest that data protection by default can also be adopted by browsers.

4.2 DATA PROTECTION BY DEFAULT – WEBSITE COOKIE SETTINGS

This section makes an analysis of how data protection by default should apply to website settings for cookies. An analysis is made under the various elements of data protection by default such as necessity, consent, accessibility, data retention, transparency, and technical and organisational measures.

87 Max von Grafenstein, Julie Heumüller, Elias Belgacem, Dr. Timo Jakobi, and Patrick Smieskol, 'Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking technologies in personalised internet content and the data protection by design approach – Effective Regulation through Design.' (2021) <https://doi.org/10.5281/zenodo.5008420> accessed 16 March 2022.

88 EDPB, 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (12 March 2019) <https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf> accessed 16 March 2022.

89 Max von Grafenstein, Julie Heumüller, Elias Belgacem, Dr. Timo Jakobi, and Patrick Smieskol, 'Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR)' (n 87).

90 Guidelines for Privacy-Friendly Default Settings (n 8).

91 ENISA Recommendations on shaping technology according to GDPR provisions (n 6).

92 Case C-40/17 Judgment of the Court (Second Chamber) of 29 July 2019 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV Request for a preliminary ruling from the Oberlandesgericht Düsseldorf ECLI:EU:C:2019:629.

4.2.1 Necessity

By default, only those cookies must be stored on a user device by a website which are necessary. This has been recognised by the French CNIL in its decision against Google discussed above.[93]

While considering whether a cookie is necessary, the mere importance of the cookie would not suffice unless the cookie is also strictly necessary.[94] The transmission of the requested service must not be possible without the cookie.[95] Thus, by default, only those cookies must be stored which are indispensable for transmission. By default, only those cookies must be stored which are key enablers of the service. As discussed before, cookies that merely assist or speed up transmission over communication, third party cookies and tracking cookies are not necessary. Such cookies must not be enabled by default.

By default, first party analytics cookies must also not be enabled by default. This has been recognised in the EDPS decision against the European Parliament discussed above.[96] But, the proposed ePrivacy Regulation provides for a ground of processing for web audience measuring. This ground suffers from a loophole as discussed above. Thus, the possibility of blocking third party cookies (by default) must take precedence over web audience measuring under draft ePrivacy Regulation Article 8(1)(d).[97] There must be a possibility that tracking cookies are blocked (by default) even though a website has the option of analytics for web audience measuring.[98]

4.2.2 Consent

Data protection by default requires consent to be informed, specific, and freely given. Thus, if a non-essential cookie is enabled on websites by default without user consent, there would be an absence of valid consent as the user choice is taken away.[99] The GDPR requires active behaviour for valid consent. Active behaviour could be a traceable user client request such as clicking on a banner.[100] It is thus difficult to argue that consent has been given unambiguously if non-essential cookies are stored by default without the user initiating active behaviour on entering the website's entry page.[101]

Cookie banners that just pop-up and disappear by default are non-compliant as it cannot be assumed that user has been informed.[102] Neither can it be demonstrated that the user has engaged with the information.[103] It is also not permissible for a cookie banner to state that it would be assumed that the user consents to cookies by merely clicking, using, or scrolling through the cookie banner.[104] Moreover, the GDPR requires that silence cannot constitute valid consent. User inaction to cookie banners must be seen as silence by the user. Thus, non-essential cookies must not be placed by default as a response to user inaction to cookie banners. This is especially true of tracking cookies for which unambiguous consent must be required for the processing of personal data to set and read these cookies.[105]

The support for a default non-acceptance of cookies on user inaction can be found in the *Planet49* case from which one can derive the foundational argument for data protection by default while using cookies. The CJEU stated in this case that a pre-selected checkbox accepting cookies does not constitute a valid consent.[106] There is no way to know that a user has even

93 CNIL Deliberation against Google (n 63).

94 ICO, UK Guidance on the use of cookies and similar technologies (n 82).

95 A29 WP Opinion 04/2012 on Cookie Consent Exemption (n 54).

96 EDPS Decision against the European Parliament (n 75).

97 A29 WP Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (n 80).

98 Ibid.

99 ICO, UK Guidance on the use of cookies and similar technologies (n 82).

100 A29 WP Working Document 02/2013 providing guidance on obtaining consent for cookies (n 56).

101 Ibid.

102 DPC, Ireland Guidance Note: Cookies and other tracking technologies (n 47).

103 Ibid.

104 Ibid.

105 A29 WP Working Document 02/2013 providing guidance on obtaining consent for cookies (n 56).

106 CJEU in Planet49 Case (n 59).

noticed the checkbox or read the information accompanying the checkbox before continuing activity on the website.[107] It is difficult to ascertain whether a user has been informed or has given informed consent by not deselecting the ticked checkbox.[108]

Thus, it can be argued that when a user does not engage with the cookie banner by neither accepting nor rejecting cookies, and continues to browse through the website, there is no way to know or ascertain that the user has even looked at the cookie banner (thereby being informed) or has consented in an informed manner. It is difficult to ascertain whether a user has given informed consent by not selecting the accept option. Given the lack of awareness, it is also a fallacy to assume that data subjects have unambiguously consented[109] in such cases.

When users do not engage with the cookie banner, even implied consent is difficult to assume.[110] The failure to click either accept or reject may imply overlooking of the banner or lack of awareness.[111] Thus, by default, if the user does not engage with cookie banner, non-essential cookies must not be stored as there would be a lack of user consent.

4.2.3 Accessibility

Data protection by default also requires confidentiality through limiting accessibility. As per Article 25 of GDPR, data must not be accessible to an indefinite number of people. It has been argued that the indefiniteness of people should be assessed based on a number larger than the reasonable expectations.[112] Usually, the cookie that is stored by a domain is only readable by that domain. For instance, cookie stored by google.fr can only be read by google.fr. But, Google also has a presence on many other websites. The cookie of Google can thus track the user on all websites where it has a presence through advertisements, social plugins etc.

To limit the accessibility of data by Google across websites, there is a need to curtail third party cookies by restricting them by default. These cookies engage in cross-site tracking and build browsing histories and behavioural profiles of persons. These profiles and behavioural profiles are used for purposes including advertising. Thus, through third party cookies, user data across websites is made accessible beyond the reasonable expectations. Thus, there is a need to curtail accessibility by curtailing third party cookies by default.

Apart from third party cookies, it is also important to curtail first party cookies that are cross site cookies. An example can help illustrate. When a user visits fr-fr.facebook.com the cookies stored by Facebook are first party cookies as they belong to the host domain. But these cookies can be used to track persons across the web where Facebook has a presence through social plugins, Like buttons etc. Thus, a first party cookie can also be a cross-site tracking cookie. To restrict accessibility, third party cookies as well as first party cookies engaging in cross-site tracking need to be restricted by default.

4.2.4 Data retention

Data protection by default requires adherence to data retention and storage limitation principles. It has been recommended by Data Protection Commission, Ireland that the user consent for cookies must not be valid for more than six months after which revised consent would need to be sought.[113] Thus, by default, the cookie consent must be valid for a limited time after which revised consent must be sought.

The Article 29 WP has suggested that even cookies exempted from consent should have an expiration date considering the time for which they are necessary.[114] The reasonable

107 Ibid.

108 Ibid.

109 Damian Clifford, 'EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster – Tracking the Crumbs of Online User Behavior' (n 13).

110 Giuseppe B. Abbamonte, 'The Protection of Computer under EU Law' (2014) 21 Colum J Eur L 71.

111 Ibid.

112 Lina Jasmontaite , Irene Kamara, Gabriela Zanfir-Fortuna & Stefano Leucci, 'Data Protection by Design and by Default' (n 12).

113 DPC, Ireland Guidance Note: Cookies and other tracking technologies (n 47).

114 A29 WP Opinion 04/2012 on Cookie Consent Exemption (n 54).

expectations of the average user must be considered.[115] For instance, cookies used to store shopping basket preferences would constitute necessary cookies. These cookies must, by default, have an expiration date considering, for instance, the reasonable expectation of recovering basket items.[116] Thus, by default cookies must have an expiry date rather than users being required to use browser settings to themselves delete cookies.

4.2.5 Transparency

By default, users must be given prior clear and comprehensive information about cookies. Data protection by default could require the use of symbols and related messages to alert the users that cookies are being used to track them.[117] For instance, icons could be used as a constant reminder of tracking.[118] Icons could be designed like danger signals to alert users of the tracking throughout the processing. The use of symbols and icons for informing about cookies and tracking would greatly help vulnerable or unaware public.

When the user is informed of the use of non-essential cookies by default, there would be rise in user awareness of cookies and tracking. This would help users gain control over the processing of cookies by taking privacy preserving measures such as the deletion of cookies from browsers or the use of private browsing mode which would cause cookies to be deleted once the browser is closed.

4.2.6 Technical and organisational measures

Data protection by default requires implementation of technical and organisational measures which are appropriate.[119] The data controller is free to decide the measures.[120] Article 5(3) ePrivacy directive compliance can benefit from codes of conduct on data protection by default.[121] Moreover, the ICO, UK has suggested a 'cookie audit' of online services.[122] Such a cookie audit could help ensure data protection by default for cookies.[123] The cookie audit proposed by the ICO entails various steps as discussed below.

The cookies being used need to be identified and the purpose of the cookies needs to be established.[124] The type of cookie needs to be confirmed – persistent or session, and the lifespan of cookies needs to be established.[125] Justifiable duration of cookies needs be established and strictly necessary cookies need to be distinguished.[126] Consent mechanisms need to be reviewed.[127] These findings should be documented and reviewed periodically.[128] Such an organisational measure can help decide the appropriate default setting for different cookies to enforce data protection by default.

4.3 DATA PROTECTION BY DEFAULT – BROWSER COOKIE SETTINGS

Merely providing an option to select a setting on installation of software (like a browser) does not amount to data protection by default.[129] Terminal equipment and software (like browsers)

115 Ibid.

116 Ibid.

117 Ibid.

118 A29 WP Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising (n 10).

119 Lina Jasmontaite , Irene Kamara, Gabriela Zanfir-Fortuna & Stefano Leucci, 'Data Protection by Design and by Default' (n 12).

120 Ibid.

121 Giuseppe B. Abbamonte, 'The Protection of Computer under EU Law' (n 110).

122 ICO, UK Guidance on the use of cookies and similar technologies (n 82).

123 Ibid.

124 Ibid.

125 Ibid.

126 Ibid.

127 Ibid.

128 Ibid.

129 A29 WP Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (n 80).

must provide privacy protective settings by default.[130] This is important because it cannot be assumed that all users would be able to configure cookie settings in the browser to correctly reflect privacy preferences.[131] As per Article 29 WP, "*The responsibility for [cookie] processing cannot be reduced to the responsibility of the user for taking or not taking certain precautions in his browser settings.*"[132]

Default settings of most browsers is set to "accept all cookies".[133] If browser default settings is "accept all cookies", and this general browser settings is used by websites to store cookies, consent requirements would not be fulfilled as per ePrivacy directive and GDPR (as mentioned above, general browser settings cannot constitute valid consent). The reasons are that consent would not be prior or specific.[134] Consent would also not be informed since users might lack the knowledge to change such settings.[135] An "accept all cookies" option is also against the concept of granular consent.[136] If browser settings are used for consent by providing general information about third party cookies and the basic browser setting to avoid them, it would also not comply with the "clear and comprehensive information" requirement under Article 5(3) of ePrivacy directive.[137]

On the other hand, if default browser settings "reject all third party cookies", and user is later required to take affirmative action to accept cookies on websites, it could constitute valid and effective consent.[138] This suggestion must be distinguished from Do Not Track mechanisms. For example, there is a suggestion that the ePrivacy Regulation should make it mandatory for browsers to implement measures such as Do Not Track.[139] It is suggested that this would give users genuine choice and control from interference with devices.[140] It is important to note that Do Not Track does not block cookies but only alerts the network of user's preferences. Thus, the success of Do Not Track depends, to a large extent, on its acceptance by the advertisers.[141] There are measures similar to Do Not Track such as Global Privacy Control (GPC) that allow the user to notify online services of their preferences through browser settings or an extension.[142] But, it is important to note that the GPC is not a withdrawal of consent under ePrivacy directive nor is it an objection to processing.[143] Thus Do Not Track and related measures depend on their acceptance by advertisers. On the other hand, default browser settings to reject all third party cookies is a measure that is stricter as it can be enforced under the legal principle of data protection by default. The onus would then lie on the website to show that it has obtained valid consent.

Default browser settings to reject all third party cookies must also be distinguished from a combination of Privacy by Design and Privacy Enhancing Technologies. For instance, Microsoft's Edge browser fulfils "browser privacy promise" by blocking trackers from sites that the user has not visited.[144] Mozilla's Firefox blocks cross-site tracking cookies.[145] A large part of the success of

130 Ibid.

131 ICO, UK Guidance on the use of cookies and similar technologies (n 82).

132 Article 29 Data Protection Working Party, 'Opinion 1/2008 on data protection issues related to search engines' (4 April 2008) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf> accessed 16 March 2022.

133 Daniela Ježová, 'Principle of Privacy by Design and Privacy by Default' (n 23).

134 A29 WP Opinion 2/2010 on online behavioural advertising (n 11).

135 Giuseppe B. Abbamonte, 'The Protection of Computer under EU Law' (n 110).

136 A29 WP Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (n 80).

137 DPC, Ireland Guidance Note: Cookies and other tracking technologies (n 47).

138 A29 WP Opinion 2/2010 on online behavioural advertising (n 11).

139 A29 WP Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (n 80).

140 Ibid.

141 Damian Clifford, 'EU Data Protection Law and Targeted Advertising' (n 13).

142 ICO, UK Opinion: Data protection and privacy expectations for online advertising proposals (n 1).

143 Ibid.

144 French Data Protection Authority CNIL, 'Alternatives to third-party cookies: what consequences regarding consent?' (23 November 2021) <https://www.cnil.fr/en/alternatives-third-party-cookies-what-consequences-regarding-consent> accessed 17 March 2022.

145 Ibid.

DOI: 10.5334/tilr.311

such initiatives rests again with the advertisers who may find ways to bypass such measures or not readily cooperate with such self-regulatory measures. On the other hand, default browser settings to "reject all third party cookies" is a legal measure under data protection principle of data protection by default.

The suggestion of this article that browser default settings must reject all third party cookies has also found voice in the leaked draft of the ePrivacy Regulation which did not find place in the official draft ePrivacy Regulation.[146] The provision read,

> "*The settings of all the component of the terminal equipment placed on the market shall be configured to, by default, prevent third parties from storing information, processing information already stored in the terminal equipment and preventing the use by third parties of the equipment's processing capabilities.*"[147]

Such an explicit recognition of data protection by default is an ideal solution. The ePrivacy law applies in a technology neutral manner not just to cookies but also to other tracking technologies.[148] A provision like the one above would thus protect from any kind of tracking by default. Such a provision is also important to answer the possible counter-arguments that data protection by default does not apply under the ePrivacy law.

The proposal for a default "reject all third party cookie" setting must go one step beyond the suggestion of the CNIL that, "*where refusal can be expressed by merely closing the consent window or by the lack of interaction with that window for a certain period of time, this option must be clearly indicated to users on that window.*"[149] The CNIL seems to suggest that refusal of cookies can be inferred from user inaction where the cookie banner explicitly mentions that this is possible. It can be argued that the CNIL position means that where the cookie banner does not explicitly mention that refusal of cookies can be inferred from user inaction, there is a need for refusal through positive action. This is a concerning position to take in light of the fact that a sizeable population of persons is not aware of cookies and an onus cannot be placed on such people to positively opt-out. Besides, this position is concerning also because websites often offer complex mechanisms to opt-out which makes it difficult to positively opt-out. Thus, if a user does not engage at all with the cookie banner or the browser settings, third party cookies and other cookies that are non-essential should not be stored by default.

5 CONCLUSION

Data protection by default can help curtail cookies from being used for non-essential purposes by default. Such a default setting would help protect vulnerable, unwary, unwilling, unaware and all kinds of users against tracking, profiling and behavioural advertising by default. Such a default setting would sustain unless the users themselves opt-in to non-essential cookies through an unambiguous action constituting valid consent under the GDPR.

> The default cookie setting on websites should be –
>
> By default, only essential cookies should be stored.
>
> By default, non-essential cookies such as third party cookies should not be stored.
>
> By default, non-essential cookies such as third party cookies must be stored only when the user makes an affirmative choice by clicking the accept cookies button.
>
> By default, non-essential cookies such as third party cookies should not be stored if a user does not click the accept cookies button.

146 Jeroen Terstegge, 'The EU's privacy by default 2.0' (6 January 2017) <https://iapp.org/news/a/the-eus-privacy-by-default-2-0/> accessed 16 March 2022.

147 Ibid.

148 European Data Protection Board, 'Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications' (25 May 2018) <https://edpb.europa.eu/our-work-tools/our-documents/other/statement-edpb-revision-eprivacy-regulation-and-its-impact_en> accessed 16 March 2022.

149 CNIL Deliberation against Facebook (n 69).

> By default, non-essential cookies should not be stored if the user does not interact with the cookie banner.

The default cookie setting on a browser should be -

> By default, all third party cookies and cross-site cookies must be disabled by the browser. This default setting would constitute valid rejection of non-essential cookies on websites unless the user chooses non-essential cookies on the website through valid consent under GDPR.
>
> By default, the option of accept all cookies must not be enabled. If this option is enabled by default, it cannot be used to override cookie consent on a website as general browser settings cannot be used for valid consent as discussed above.

While data protection by default is an existing requirement under the GDPR, the ePrivacy law in the EU does not explicitly recognise the requirement. This paper suggests that the requirement of data protection by default must apply and be recognised under ePrivacy law.

The way forward is to recognise that data protection by default applies under the proposed ePrivacy Regulation. There can be a special provision that requires software providers as well as services to, by default, not allow third parties to store information or gain access to stored information from user devices. The mention of data protection by default under the ePrivacy Regulation is essential because the ePrivacy does not merely apply to use of cookies but to other tracking techniques such as fingerprinting which also need to be curtailed by default.

Recognising data protection by default under the ePrivacy law would provide robust protection to individuals. It would help protect all individuals by default, irrespective of whether they interact with cookie consent banners. It would help protect all individuals by default regarding their browser settings. Consequently, it would help significantly curtail user tracking on the internet. Data protection by default would greatly help users who do not meaningfully engage with consent settings in the browser and on websites.

The omission of the provision from the Council's mandate on ePrivacy Regulation that allows browser settings as a means to consent to cookies is a good move. But there must be a provision that clarifies that a browser setting that rejects all non-essential cookies including third party cookies would constitute a valid rejection of cookies on websites unless the user actively opts-in on the website.

Overall, there is an urgent need to curtail the cookie monster to protect user privacy on the internet through data protection by default. The requirement of data protection by default would limit user tracking by default. It would require little effort on the user's part to protect internet privacy by meaningfully engaging with cookie banners and browser settings. While it is helpful to focus on empowering users to make meaningful consent decisions, it is essential to fill the gap that users do not meaningfully engage with consent banners and settings. Data protection by default can help fill this gap.

COMPETING INTERESTS

The author has no competing interests to declare.

AUTHOR AFFILIATION

Paarth Naithani
Assistant Lecturer, O.P. Jindal Global University, Sonipat, India

TO CITE THIS ARTICLE:
Paarth Naithani, 'Curtailing the Cookie Monster through Data Protection by Default' (2022) 27(1) *Tilburg Law Review* pp. 22–36. DOI: https://doi.org/10.5334/tilr.311

Published: 17 February 2023