scripted

Volume 14, Issue 2, December 2017

The Draft ePrivacy Regulation: No More *Lex Specialis* for Cookie Processing?

*Andrew Cormack**

DOI: 10.2966/scrip.140217.345

Abstract

The European Commission's draft ePrivacy Regulation appears to transfer legal responsibility for the storage and retrieval of cookies from websites to web browsers. However, where the subsequent processing of cookies involves personal data, website operators will still be responsible for ensuring this complies with the General Data Protection Regulation. Applying general, rather than specific, legislation to this processing should result in a better experience for both the operators of websites and their users.

Keywords

cookies, data protection, ePrivacy, GDPR

* Chief Regulatory Adviser, Jisc, UK, Andrew.Cormack@jisc.ac.uk

1 Introduction

In 2017 the European Commission proposed, in its draft ePrivacy Regulation,[1] revisions to the "cookie law" introduced in the 2002 ePrivacy Directive[2] and refined in the 2009 Citizens' Rights Directive.[3] Much commentary has focussed on the reduced range of cookies to be covered by the new law. However, this article suggests that a more significant change is the re-allocation of responsibilities between providers of websites and browsers. Current law makes website operators responsible both for the storage and retrieval of cookies and for the subsequent processing of data derived from them. This has encouraged interpretations that apply the Directive to both operations, even though its text provides no basis for that. By mandating a legal role for web browsers in storage and retrieval – and allowing website operators to rely on them performing it – the draft Regulation should clarify that subsequent processing has always been a legally separate activity subject not to the specific cookie law but, if it involves personal data, to general data protection law. Data derived from cookies should not be treated as a special case, but instead as another type of (potentially) personal data, whose processing is subject to the full range of data protection law. This should produce more appropriate controls for both website operators and

1 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 (2017/0003 (COD)) (hereinafter 'draft ePrivacy Regulation').

2 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37.

3 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L 337/11 (hereinafter 'Citizens Rights Directive').

users, and an improved experience for both.

This paper maps the development of the *lex specialis* for cookies and how its scope has been extended beyond the actual text. It then suggests how the draft ePrivacy Regulation could correct this and result in the use of more appropriate general law for cookie processing.

2 Cookie laws: 2002 and 2009

In 2002, the ePrivacy Directive introduced a special legal regime for cookies –

> Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller.[4]

The 2009 Citizen's Rights Directive replaced this "right to refuse" with a requirement that "the subscriber or user concerned has given his or her consent".[5] A recital to the Directive appeared to allow such consent to be inferred from the settings of the user's web browser:

> 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.[6]

---

4 *Supra* n. 2, art. 5(3).
5 *Supra* n. 3, art. 2(5).
6 *Ibid*., Recital 66.

However the Article 29 Working Party of Data Protection Supervisors pointed out that in 2010 "three [of the four] major browsers have as a default setting to allow all cookies",[7] and that a user's failure to change this setting could not be taken as "a clear and unambiguous indication of his/her wishes".[8] For a browser's settings to provide valid consent, it must by default reject third-party cookies and require an affirmative action by the user before it accepts them.[9] In 2013 the Working Party re-iterated that consent could only be inferred from browser settings "[w]here the website operator can be confident that the user has been fully informed and actively configured their browser or other application".[10] With the Commission confirming in 2017 that "the default settings for cookies are set in most current browsers to 'accept all cookies'",[11] the option of relying on browser settings still seems to be unavailable to website operators.

Instead, most websites have implemented technical measures to obtain consent, typically using banners or pop-ups that users must click before viewing the content they want. As a result, according to the European Commission "end-users are overloaded with requests to provide consent".[12] Furthermore, although the ePrivacy Directive only covers storing and accessing cookies, the Article 29 Working Party encouraged website operators to treat this interaction as also providing consent to the subsequent processing of any personal data that might be derived from those cookies: "users' single acceptance to receive a cookie may also entail their acceptance for the subsequent readings of the cookie, and hence

---

7 Article 29 Working Party, "Opinion 2/2010 on Online Behavioural Advertising" 00909/10/EN WP 171, p. 14.

8 *Ibid*.

9 *Ibid.*, p. 15.

10 Article 29 Working Party, "Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies" 1676/13/EN WP 208, p. 4.

11 Draft ePrivacy Regulation, *supra* n. 1, Recital 23.

12 *Ibid.*, Recital 22.

for the monitoring of their internet browsing".[13] Despite an observation that the Data Protection Directive (95/46/EC) "applies to matters not specifically covered by the ePrivacy Directive whenever personal data are processed",[14] this Working Party guidance has been widely interpreted as meaning that consent is required for processing cookies data, not just – as the ePrivacy Directive actually states – for storing and accessing them.

This interpretation creates two anomalies. The ePrivacy Directive exempts some cookies – those used solely for transmissions over a network and those necessary to provide a service explicitly requested by a user[15] – from the requirement to obtain consent to storage and access. A website that omits these cookies from its consent interface may have no legal basis for processing personal data that may be derived from them. Conversely websites that obtain consent for storage and access may be encouraged to also use consent as the basis for subsequent processing even where alternative provisions under the Data Protection Directive would be more suitable.

3 The draft ePrivacy Regulation 2017

In 2017, the European Commission published its proposal for a new ePrivacy Regulation.[16] This reaffirms many aspects of the 2009 Directive and the Article 29 Working Party's comments on it: that the *lex specialis* only applies to storing and accessing cookies, not subsequent processing; that such storing or accessing requires prior, informed consent;[17] that, now in an Article rather than a Recital, such "consent may be expressed by using the appropriate technical settings of a

13 Article 29 Working Party, "Opinion 2/2010 on Online Behavioural Advertising", *supra* n. 7, p. 3.

14 *Ibid.*, p. 8.

15 Citizens Rights Directive, *supra* n. 3, art. 2(5), replacing art. 5(3) of Directive 2002/58/EC.

16 *Supra* n. 1.

17 *Ibid*., Recital 20.

software application enabling access to the internet";[18] and that, to be valid, such settings must be the result of a "clear, affirmative action" action by the user.[19]

However, in an apparent recognition of the failure of previous legislation that merely declared the possibility of relying on technical settings to express consent, there is a new explicit statement that "web browsers … are in a privileged position to play an active role to help the end-user to control the flow of information to and from the terminal equipment".[20] And, to ensure that browsers do, in future, play that role, the Commission propose a new legal duty on those supplying web browsers to the European market:

> 1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.
> 2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.
> 3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.[21]

If this becomes law, web browsers will be required to present their users with an active choice whether or not to allow the storing and accessing of cookies, in a way that ensures the user has given legally valid consent. Articles 10(2) and 10(3) suggest that this requirement could be satisfied by a choice offered when

---

18 *Ibid.*, art. 9(2).
19 *Ibid.*, Recital 22.
20 *Ibid.*, Recital 22.
21 *Ibid.*, art. 10.

the software is installed or first updated. Although doubts have been expressed whether such an interface can in fact provide sufficient information to obtain valid consent,[22] the draft legislation is clear that in future this will be an issue for browser suppliers, not website operators. The inclusion of a cut-off date, by which all browsers must behave in this way, appears to resolve the concerns previously expressed by the Article 29 Working Party: after that date, website operators will know that browser technical settings are the result of an active, informed choice by their users and that, as a result, they have valid consent for any storing or accessing of cookies that those settings permit.

4 What law for cookie processing?

An active choice presented when a browser is installed or first updated may provide valid consent for storing and accessing cookies but, since "[t]he definition of and conditions for consent provided for under Articles 4(11) and 7 of [the General Data Protection Regulation (GDPR)] shall apply",[23] it is unlikely that such an interface could also provide valid consent for subsequent processing. Making the active choice interface part of the browser installation process means website operators are very unlikely to have the access or control that will be required to satisfy the GDPR's requirements that they "be able to demonstrate that the data subject has given consent to the processing operation",[24] or to ensure it is "as easy to withdraw as to give consent".[25] And, even if such an interface could provide information about the "purposes of the

[22] E.g. Eoin Carolan, "The continuing problems with online consent under the EU's emerging data protection principles" (2016) 32 *Computer Law & Security Review* 462-473.

[23] Draft ePrivacy Regulation, *supra* n. 1, art. 9.

[24] 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 25/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 (hereinafter 'GDPR'), art. 13(1), Recital 42.

[25] *Ibid*., art. 7(3).

processing for which the [cookies] are intended"[26] at the time the browser is installed, it gives website operators no possibility of updating that information as they change their processing and purposes over time.

Thus, although the draft Regulation will mean that website operators can rely on browser technical settings to express users' consent to the storing and accessing of cookies, the Article 29 Working Party's suggestion that the same consent could extend to subsequent processing of information derived from those cookies no longer appears tenable. Website operators will therefore need to take their own measures to ensure that their processing of cookie data complies with the law. And, where cookies constitute personal data, it should now be clear that the relevant law has never been the special cookie provisions of ePrivacy law but, from 25 May 2018, the GDPR. Using cookies will therefore resemble other examples, presented in the Working Party's 2011 Opinion on Consent, of compound processing where different aspects may be covered by different legal provisions.[27] Website operators must therefore identify and apply the relevant aspects of the GDPR when processing any personal data derived from cookies. This resolves the anomalies that arise when the ePrivacy Directive alone is used for cookie processing: appropriate legal bases – including contract and legitimate interests, as well as consent – become available both for cookies exempt under that Directive and for those where consent is inappropriate or unavailable. The Working Party's Opinion 04/2012 on the Cookie Consent Exemption[28] provides examples of both exempt and non-exempt cookies that illustrate how applying normal data protection law to the processing of cookie data results in legal bases

[26] *Ibid*., Recital 42.

[27] Article 29 Working Party, "Opinion 15/2011 on the Definition of Consent" 00197/11/EN WP187, p. 8.

[28] Article 29 Working Party, "Opinion 04/2012 on Cookie Consent Exemption" 00879/12/EN WP 194, pp. 6-11.

that are both consistent with the cookie storage rules and provide appropriate safeguards and obligations for data subjects and data controllers respectively.

Load-balancing cookies are considered necessary for communication over the network, so are exempt from storage notification:[29] since they only identify a server, not a client machine, they will not contain personal data, so their processing does not engage data protection law and does not require processing notification either. Cookies that are used only to customise the user interface – for example to indicate a preferred language or format for content – do not require any unique identifier so are unlikely to constitute personal information.[30] They may, depending on persistence, require a notice before storage: the Working Party suggests placing this clearly beside the "remember setting" button.[31] Cookies used to store user input – for example the contents of a shopping cart – are likely to constitute personal data. Though these are exempt from storage notification,[32] a legal basis for processing is required. The obvious basis is that processing is necessary for, or at the user's request to prepare for, a contract with the user.[33] Websites must therefore notify users about the processing: since this must be done "at the time when personal data are obtained",[34] a static web page linked from the shopping cart option is likely to be suitable. Using this basis also gives users the right to data portability, however any storage of purchasing history is more likely to be associated with the user's account rather than with a transient session cookie. Similar considerations are

---

29 *Ibid.*, s. 3.5.

30 Frederik Zuiderveen Borgesius, "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation" (2016) 32 *Computer Law & Security Review* 256-271, p. 257.

31 Article 29 Working Party, "Opinion 04/2012 on Cookie Consent Exemption", *supra* n. 28, s. 3.6.

32 *Ibid.*, s. 3.1.

33 GDPR, art. 6(1)(b).

34 *Ibid.*, art 13(1).

likely to apply to session authentication,[35] user-centric security,[36] and multi-media player session cookies.[37]

In 2012 the Working Party reluctantly concluded that – even though they were "not likely to create a privacy risk" – the ePrivacy Directive required cookies used for first-party website analytics to obtain storage consent.[38] Article 8(1)(d) of the draft Regulation now follows the Working Party's recommendation and adds "audience measuring" by websites to its exempted list. The obvious GDPR basis for this processing, which is likely to involve personal data, is that it is necessary for a legitimate interest of the data controller.[39] This basis requires that the impact on the individual's rights and freedoms be minimised and that any remaining risk be balanced against the benefit of processing to the data controller. Since the aim of these cookies is to gather information about the website, while having no effect on its users, tools such as pseudonymisation can be used and will often reduce the risk sufficiently to satisfy this balance.[40] Users must be informed of the processing, the interest that it serves, and their right to object to it (in which case the rights balance must be reassessed in the light of that particular user's circumstances). Again, this information can be provided through a static web page, rather than requiring an active dialogue.

Persistent (multi-session) authentication cookies are an example where consent is likely to be the basis for both storage and processing. So long as the cookie is only used for authentication, it should be possible to obtain informed,

35 Article 29 Working Party, "Opinion 04/2012 on Cookie Consent Exemption", *supra* n. 28, s. 3.2.
36 *Ibid*., s. 3.3.
37 *Ibid.*, s. 3.4.
38 *Ibid.*, s. 4.3.
39 GDPR, art. 6(1)(f).
40 *Ibid.*, Recital 28.

prior, opt-in consent to both through a single "remember me" button with an accompanying notice.[41]

More complex uses that are required to obtain consent for storage include social plug-in tracking[42] and third party advertising.[43] Zuiderveen Borgesius considers "the fact that a company sees personal data processing as useful or profitable does not make the processing 'necessary'[44] to provide the contracted service to the user. Processing for these purposes might be considered necessary for a legitimate interest of the social network provider or third party, but only if that interest is not overridden by the user's rights and freedoms.[45] Otherwise, it will require the user's free, informed consent.[46] While Recital 47 of the GDPR indicates that the legitimate interests basis might be available for direct marketing, it does not explain how to satisfy the Article 6(1)(f) balancing test. This basis would require the interested party to provide information to users and handle objections from them, but would avoid the need for an active consent dialogue. More detailed guidance from regulators would, therefore, be welcome on the conditions under which legitimate interests could apply. In other circumstances the remaining legal basis, consent, is likely to be an even more onerous choice than under the current Data Protection Directive, since the GDPR requires, among other things, that it be specific, actively granted,[47] recorded,[48] easily withdrawn and data erased.[49] The Working Party's conclusion that such cookies are "not strictly necessary to provide a functionality explicitly requested

41 Article 29 Working Party, "Opinion 04/2012 on Cookie Consent Exemption", *supra* n. 28, s. 3.2.

42 *Ibid.*, s. 4.1.

43 *Ibid.*, s. 4.2.

44 Frederik Zuiderveen Borgesius and Joost Poort, "Online Price Discrimination and EU Data Privacy Law" (2017) 40(3) *Journal of Consumer Policy* 347-366, p. 360.

45 GDPR, art. 6(1)(f).

46 *Ibid.*, art. 6(1)(a).

47 *Ibid.*, art. 4(11).

48 *Ibid.*, art. 7(1).

49 *Ibid.*, art. 7(3).

by the user",[50] suggests that consent cannot be inferred from the user's willingness to use the service but must, under the GDPR, be obtained separately.[51] In addition, using consent involves complying with data portability requests,[52] which will include data collected over the entire lifetime of the cookie.[53] The ePrivacy Regulation's provisions on browser settings will not, therefore, eliminate the need for consent dialogues for these cookies: indeed the GDPR requirements for consent to processing are likely to make them more complex.

Treating the processing of cookie data as a normal activity involving personal data should also highlight that all aspects of the GDPR apply. Thus, for example, cookie data that is used to make automated decisions with legal, or other significant, effect on an individual will be subject to the profiling provisions in Article 22. Or, as the Working Party note, website operators who wish to have a third party perform website audience measurement on their behalf can use a "GDPR-compliant [data] processor agreement" to do so.[54]

5 Conclusion: general, rather than special, law

By separating responsibility for the technical aspects of storing and accessing cookies from the legal aspects of processing data derived from them, the draft ePrivacy Regulation supports the Article 29 Working Party's 2012 view that "[t]he risk to data protection comes from the purpose(s) of processing rather than

50 Article 29 Working Party, "Opinion 04/2012 on Cookie Consent Exemption", *supra* n. 28, s. 4.1

51 General Data Protection Regulation, *supra* n 24, art. 7(4).

52 *Ibid.*, art. 20.

53 Article 29 Working Party, "Guidelines on the Right to Data Portability" 16/EN WP 242 rev.01, p. 9.

54 Article 29 Working Party, "Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)" 17/EN WP 247, p. 19.

the information contained within the cookie".[55] The GDPR was specifically designed to provide a comprehensive regime to regulate such processing. Furthermore, applying the Regulation ensures that the same rules apply to processing irrespective of who performs it or what technology may be used: cookies, super-cookies, browser fingerprinting, or any future invention.

As recently as 2013, the Working Party appeared to exclude any legal basis other than consent: "[f]or the processing of the personal data that goes together with the reading and setting of tracking cookies the data controller needs to obtain the unambiguous consent of the user".[56] This seems likely to have resulted in both an excessive number of unnecessary and inappropriate consent dialogues and, where cookies were declared exempt, processing of personal data without any consideration of legal basis or requirements. It may well explain the Department for Culture, Media and Sport's (DCMS) finding that:

> [T]he biggest unanticipated impact has been the consumer reaction which ranges from apathy to frustration, but nowhere near the positive reassurance that introduction of the requirement was expected to deliver.[57]

If regulators and website operators now take the opportunity to apply general data protection law to the processing of cookie data, there should be much less frustration and apathy from both consumers and website operators, and much more of the positive reassurance that DCMS were hoping for.

---

55 Article 29 Working Party, "Opinion 04/2012 on Cookie Consent Exemption", *supra* n. 28, p. 5.

56 Article 29 Working Party, "Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies", *supra* n. 10, p. 6.

57 Department for Culture, Media and Sport, "Post Implementation Review of the EU Electronic Communications Framework 2009" (April 2017), p. 16, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/610586/PIR_EU_Electronic_Communications_Regulatory_Framework_2009.pdf (accessed 19 May 2017).