Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The continuing problems with online consent under the EU's emerging data protection principles

Eoin Carolan *

School of Law, University College, Dublin, Ireland

Keywords:
Data protection
Privacy
Consent
Internet users
European law
Behavioural science
Nudging

ABSTRACT

Since the original Data Protection Directive in 1995, EU law has attached particular importance to user consent. This emphasis on consent is retained – albeit in different forms – in the various positions adopted by the EU institutions on the draft General Data Protection Regulation in advance of their trilogue negotiations. This article identifies three distinct models of user consent in the EU jurisprudence in this area: presumed consent; informed consent; and active consent. The article suggests that the later models developed as a response to empirical concerns about treating consent as a reliable proxy for user privacy preferences online. On this analysis, the active consent model advocated by the Article 29 Working Party and favoured by the Parliament's draft Data Protection Regulation is assumed to address the empirical issues associated with the presumed and informed consent models. In fact, the psychology and behavioural science research shows that website users are subject to a variety of specific situational influences that intuitively impel the giving of consent. The article concludes that the EU's approach to data and privacy protection online, even under current proposals, is fundamentally misguided and makes four recommendations about the future direction of EU law in this area.

1. Introduction

The recent initiation of an inter-institutional trilogue between the European Commission, Parliament and Council suggests that the protracted process of updating Europe's data protection rules may be approaching its endgame. The trilogue is the latest and likely final stage in the extended and often discordant debate about the future of European data protection regulation that followed the publication of a draft General Data Protection Regulation (GDPR) by the European Commission in January 2012. With the trilogue currently scheduled to conclude in December of this year, the Commission has suggested that the detail of the final reform should be agreed by the end of 2015.

That may underplay, however, the depth of the divisions that remain between the institutions as they embark upon these negotiations. Even leaving aside reports of Member State disagreements about the Council's approach, the published position papers of the Council, Commission and Parliament reveal continuing differences on several points of significance. These include the important question of how to establish user consent. Broadly speaking, the Council advocates a continuation of the current approach while the Commission and Parliament are pushing for more exacting evidential standards. Given the centrality of consent to the data protection

* School of Law, Sutherland School of Law, Belfield, Dublin 4, Ireland.
E-mail address: eoin.carolan@ucd.ie.

http://dx.doi.org/10.1016/j.clsr.2016.02.004

regime, the resolution of this disagreement will be critical to the content and impact of any future reforms.

This is especially pertinent to data protection online. Online activity is an area in which the traditional legal approach to consent has proved particularly problematic. That individuals may not fully understand the nature or scope of the activities to which they have consented has been widely recognised.[1] What makes the European approach to this issue worthy of detailed scrutiny, however, is that EU data protection reforms over two decades have consciously sought to deal with this issue. As explained below, the concept of consent under EU data protection rules has not been static during this period. Various refinements or revisions have been advocated or adopted at different times by different bodies. On each occasion, one of the primary justifications for the proposed change was to address the practical problems that hinder the effectiveness of consent as a mechanism for protecting data protection rights online. As the text itself makes clear, the draft GDPR is simply the latest (if by far the most comprehensive) in a series of EU efforts to adapt data protection rules to the empirical realities of online engagement.[2]

The first part of this article seeks accordingly to position the pre-trilogue difference of views between the EU's main institutions within this broader evolution of EU attitudes to online activity. The article identifies three distinct models of user consent in the EU data protection jurisprudence: presumed consent; informed consent; and active consent. The article suggests that the later models (which represent, respectively, the Council and Commission and Parliament views) were developed as a response to empirical concerns about treating consent as a reliable proxy for user privacy preferences online.

The second part of the article goes beyond an analysis of the relative merits of these models to suggest a more fundamental difficulty with the EU's approach: namely that its emphasis on consent is inherently problematic. Initially, the most common criticism of a consent-based approach was that it represented the blind application of traditional doctrine which took no account of the changed context of online activities. The active consent model for which Parliament in particular is campaigning is assumed by its advocates to address these contextual and empirical issues. However, it is contended below that behavioural science research shows that website users remain subject to a variety of specific situational influences that intuitively impel the giving of consent even under an active consent approach. This suggests a more fundamental weakness which may require a re-thinking of the approach entirely.

The main claim of this article therefore is that the use of consent – even in the enhanced form envisaged by some EU actors – as a technique of legitimation is likely to give rise to a formalistic and permissive system of privacy regulation. This suggests that a predominantly consent-oriented strategy for promoting privacy online is inevitably flawed. What is required is a more empirically-sensitive approach which goes beyond the law's traditional trust in consent as a safeguard of individual privacy.

2. The three models of consent under EU data protection rules

2.1. *The philosophical basis for the role of consent*

Consent has traditionally played a prominent part in European approaches to privacy and data protection issues. This is often associated in the academic literature with the German right to informational self-determination,[3] although its popularity as a legal proxy for privacy- or autonomy-oriented protection is not necessarily so limited.[4] Regardless of its origins, the importance of consent under the EU's privacy regime was copper fastened by Article 8 of the Charter of Fundamental Rights. Article 8 identifies consent as a broadly applicable basis for the lawful processing of personal data:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

This emphasis on the value of consent is consistent with an understanding of privacy and data protection laws as the functional expression of dignitarian values. EU law's association of data protection and privacy[5] echoes the Charter's opening commitment to the inviolability of individual dignity.[6] This suggests a view of privacy as a necessary condition of individual autonomy because of the way in which it facilitates the making of autonomous choices.[7] On this analysis, the act of obtaining consent preserves the autonomy of the individual by respecting a residual entitlement to take his or her own decisions about the permissible usage of personal data. As the Article 29 Working Party has observed:

[1] Ira S. Rubinstein, Ronald Lee & Paul Schwartz., "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches" (2008) 75 University of Chicago Law Review 261; Avner Levin & Patricia Sanchez Abril, "Two Notions of Privacy Online" (2009) 11 Vanderbilt Journal of Law & Technology 1001.

[2] Recitals 5 and 6.

[3] Population Census Decision, Judgment of 15 December 1983, 1 BvR 209/83, BVerfGE 65, 1.

[4] See the discussion of the evolution of consent under the Swedish, German US and UK systems in Eleni Kosta, Consent in European Data Protection Law (Brill, 2013), 34–82.

[5] The Court of Justice historically treated data protection rules as a specific embodiment of the more general right to privacy. Case C-139/01 Österreichischer Rundfunk and Others [2003] ECR I-4989; C-28/08 European Commission v Bavarian Lager [2010] ECR I-6055. This conflation is criticised, with some force in Orla Lynskey, "Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order" (2014) ICLQ 569. There seems to be a change in recent decisions towards the vindication of the right as a stand-alone entitlement: Joined Cases C-293/12 and 594/12 Digital Rights Ireland and Seitlinger (8 April 2014); Joined Cases C-141/12 and C-372/12 YS, M and S v Minister voor Immigratie (17 July 2014).

[6] See Chapter 1 and, in particular, Article 1.

[7] Beate Rossler, The Value of Privacy (Polity, 2005).