Clickstream data: Revisiting the notion of "Personal Data" under the Data Protection Directive

Rebecca Wong
Senior Lecturer in Law, Nottingham Law School
Email: Rebecca.Wong@ntu.ac.uk

Abstract

There has been much literature written about clickstream data, but very little is discussed over the extent to which this is considered as "personal data" within the Data Protection Directive 95/46/EC. In this paper, I will consider the extent to which clickstream data is covered under the Data Protection Directive 95/46/EC (hereinafter "DPD") and the Directive 2002/58/EC on Privacy and Electronic Communications (hereinafter "DPEC") and the implications of taking a broad definition of "personal data".

The definition under Art. 2(a) of the DPD covers 'any information relating to *an identified* or *identified natural person* ('data subject'); an identifiable person is one who can be identified, *directly* or *indirectly* in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.'[1]

Although there is no legal definition of clickstream data provided under the DPD or DPEC, it can be taken to refer to "the generic name given to the information a website can know about a user simply because the user has browsed the site."[2] This could include a record of a user's activity on the Internet, any webpages visited, how long the user was on a page or site, their IP addresses and the order the pages were visited.

The key question for the purposes of the DPD is whether clickstream data *relates* to an identified or identifiable individual. If clickstream data cannot *relate* to an identified or identifiable person, then arguably, the such data falls outside the scope of the DPD. The DPD expressly provides for the protection of an individual rather than a group of individuals (see Art. 1(1) DPD),[3] so clickstream data belonging to a group is unlikely to fall within the scope of the DPD. Similarly, data belonging to an unidentifiable individual is unlikely to fall within the DPD. However, it is arguable that the distinctions drawn by DPD can be difficult to apply. For example, if Joe Blogs uses a family shared computer and browses the internet and Jane Blogs, his sister also uses the internet, is it always certain that websites were necessarily visited by Joe Blogs and not by Jane Blogs? One means of identifying a particular user is through the use of static IP addresses.[4] Some Data Protection Authorities such as Sweden[5] and Germany[6] have taken the view that IP addresses are "personal data" for the purpose of the DPD. However, technology has become so sophisticated that it is possible to identify and collect a user's profile including their computer usernames and websites visited. For example, Doubleclick, an advertising company collected over 100 million user profiles by the year 2002.[7]

Whilst there may be some difficulties of determining that clickstream data belongs to a specific individual, the Art. 29 Working Party[8] has not been slow to respond and has taken the view that in most instances, clickstream data would qualify as personal data.[9]

The broad interpretation of "personal data" under the DPD, however, does also leave some open questions over the application of the DPD (as provided under Art. 4[10] of the DPD) to organisations that collect clickstream data (particularly those based outside the EEA) and the extent to which clickstream data is construed as "sensitive data" under Art. 8(1) of the DPD.

The paper will explore Art. 4(1)(c) DPD and the application of Art. 8(1) DPD as applied to clickstream data. In particular, the broad interpretation of "personal data" as defined under the DPD raises some difficulties with the overall application of the DPD to organisations or individuals who directly or indirectly collect clickstream data. The DPD is a starting point in protecting clickstream data, but the enforcement of Art. 4(1)(c) to non-EEA data controllers that collect clickstream data and are not based within an EU country is unlikely to provide an adequate remedy for users online. What is needed is further discussion with the Data

Protection Authorities, Art. 29 Working Party and companies over the broad scope of the Data Protection Directive 95/46/EC.

---

1 Recital 26 of the DPD adopts a broad criterion for identifiability. It provides that 'to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.' *Recommendation R(89) 2 on Protection of Personal Data used for Employment Purposes (adopted 18.1.1989*) also provides that '…an individual shall not be regarded as 'identifiable' if the identification requires an unreasonable amount of time, cost and manpower.' See also the Council of Europe (2005). *Informational self-determination in the internet era*, (http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Events/T-PD%20_2005_%20RAP%2021%20E.pdf), Last accessed June 2006 – the authors of the report discuss the difficulties with the concept of identity.

2 Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet* (2002) 17 BERKELEY TECH. L. J. 1085, 1104. This information includes a user's detailed browsing activity and TCP/IP address, which can be used to discover personal information about the user.

3 Four Member States, however, have extended their data protection laws to legal persons (Austria, Denmark, Italy and Luxembourg). See Korff, D. "Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons (http://europa.eu.int/comm/internal_market/privacy/studies/legal_en.htm), Last accessed January 2007.

4 IP addresses can be assigned temporarily, so that they change every time a user logs in (dynamic) or can be assigned permanently to a user's computer (static). It is the latter, which is likely to be construed to be personal data. See also the Art. 29 Working Party. *The use of unique identifiers in telecommunications terminal equipments: the example of Ipv6* (http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_en.pdf), 30 May 2002.

5 s 2 of the Swedish Personal Data Act 1998 defines "personal data" as 'all kinds of information that directly or indirectly may be referable to a natural person who is alive.'

6 §3 of the German Federal Data Protection Act 2000 defines "personal data" as 'any information concerning the personal or material circumstances of an identified or identifiable individual.' The Federal Data Protection Commissioner shares the same view as the Art. 29 Working Party that IP addresses are personal data – confirmed through e-email correspondence with Ms Jennen from the Federal Data Protection Commissioner's Office on 2nd May 2005.

7 *See In re DoubleClick*, 154 F. Supp. 2d at 505. For further discussion, see Garrie, D.B. "The Legal Status of Software" (2005) 23(4) JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 711.

8 The Art. 29 Working Party is an independent advisory body set up under the Data Protection Directive 95/46/EC to provide opinions on the application of the DPD and DPEC. See Art. 30 of the DPD, which details the functions of the Art. 29 Working Party.

9 The Art. 29 Working Party. *Invisible and automatic processing of personal data on the internet performed by software and hardware*, Recommendation 1/99 (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp17en.pdf) Adopted 23 February 1999.

10 Art. 4 of the DPD covers the application of the data protection laws in a Member State. For the purposes of this paper, I will consider Art. 4(1)(c) DPD which applies to non-EU data controllers that collect personal data using equipment in an EU Member State. Art. 4(1)(c) reads as follows: 'The controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.'