Berliner Beauftragter für Datenschutz und Informationsfreiheit
Dr. Alexander Dix

be Berlin

Berliner Beauftragter für Datenschutz und Informationsfreiheit
An der Urania 4 – 10, 10787 Berlin

Federal Trade Commission
Bureau of Consumer Protection
Director
Dr. David C. Vladeck
600 Pennsylvania Ave., N.W.
Washington, DC 20580
USA

GeschZ. (bitte angeben)	Bearbeiter(in)	Tel.: (030) 13 889-0 Durchwahl 13 889 App.:	Datum
683.20.1	Herr Dix		28 February 2011

Protecting Consumer Privacy in an Era of Rapid Change
A Proposed Framework for Businesses and Policymakers
Comments

Dear Dr. Vladeck,

although belatedly I would like to take the opportunity to react to the Preliminary FTC Staff Report on Protecting Consumer Privacy of December 2010, hoping that this may still be in time to be taken into account. I will not answer all the questions set out in the questionnaire attached to the Report and make some more general observations.

First of all I welcome the obvious change of approach to consumer privacy from previous approaches throughout this document. In particular I agree with the statement that the harm-based approach has considerable limitations if it is understood as restricted to physical and economic injury.

To answer one of the questions with regard to scope I would stress that it is feasible and indeed necessary for the framework to apply to data that can be "reasonably linked to a specific consumer, computer or other device". With regard to consumers (or to citi-

zens in general, for data protection in Europe is not restricted to consumers) the application of the framework to data "reasonably linkable to consumers" would seem largely to be in line with European legislation if one considers "reasonably" to reflect indirect identifiability as described in Art. 2 a) of Directive 95/46/EC. Furthermore, the application to data that can be "reasonably linked to a specific computer or other device" goes beyond what is laid down in the Directive if this includes computers and other devices which cannot be linked to individual consumers. However, such a broad scope is indeed necessary to address the possibility of data becoming linkable to individuals in the future even if they are not linkable at present. In an environment of ubiquitous computing any device processing data may at some stage become linkable to individual consumers who use the device or whose data are registered by the device with or without their knowledge. Sensor technology is an example in this respect.

I do not see any practical considerations for excluding companies or businesses from the framework which process only a limited amount of non-sensitive data. Whether data are sensitive very often depends on the context and purpose in or for which they are processed. What a "limited amount" is could be open to interpretation. Such an exception would therefore be difficult to oversee in practice.

With regard to practices that require meaningful general choice the questionnaire asks what additional consumer protection measures are appropriate for the use of deep packet inspection. Here I would like to draw your attention to the Working Paper on the Use of Deep Packet Inspection for Marketing Purposes adopted by the International Working Group on Data Protection in Telecommunications ("Berlin Group", accessible at *http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group*) where the Working Group calls upon Internet access providers to specifically refrain from using DPI technology for targeted/behavioural advertising. In addition, the Working Group calls for more widespread application of secure end-to-end encryption mechanisms. The (optional) provision of such technologies should be mandated by law where this is not already the case, at

least for content providers offering services that involve the processing of sensitive data (e.g. online banking, uses involving credit card information, health data, etc.) as well as providers of communications services (like e-mail, chat, VoIP, etc.).

In the context of social media services privacy friendly default settings should not be limited to teens. We have successfully required a social media service provider in our jurisdiction to set privacy friendly (restrictive) defaults for all users. This does not exclude or replace additional protection measures for teens as "sensitive users". However, in this field awareness raising measures for teens and their parents seem to be equally important as regulatory measures.

With regard to the specific "Do Not Track" proposal in the Report I refer to the discussions in the Art. 29 plenary meeting on 10 February which you took part in. There is a certain tension with the requirement of Art. 5 (3) of the amended E-Privacy Directive. However, instead of discussing this in terms of an alternative "opt-in vs. opt-out" it seems to me that what matters is that an effective universal choice mechanism is put in place which makes a choice by the consumer inevitable. In other words: if the default settings are "Do Not Track" then without active consent the consumer will not be tracked.

I hope these comments – although they do not address all the specific questions – are of some use to the Commission.

Best regards,

Alexander Dix
Berlin Commissioner
for Data Protection
and Freedom of Information