01 DEFINITIONS

What is needed?

The increasing possibilities to extract data from large datasets and to merge different types of data makes it easier to identify and analyze individuals based on seemingly isolated pieces of data. The definition of "personal data" must take these possibilities into account. An incomplete definition will undermine the whole legislative proposal. If legislation on personal data does not cover all personal data, it will be destined to fail.

Especially in an online environment, data about users is often not directly identifiable. Online tracking companies do not need or want to know the name of an individual as they care about what a person is are and not who the person is – users are being singled out as worthy of being sold a particular product or accepted for a particular service at a particular price... or not.

This happens regardless of how the data is stored: creating a 'pseudonym' will not prevent tracking and analyzing of personal data or taking decisions based on these data.

In order to ensure thorough privacy protection, all personal data including data which is not directly identifiable (like a set of mobile phone numbers) must be given equal protection. So-called 'pseudonymous data' should not fall under a separate regime. The mere fact that data (such as your mobile phone number) does not directly identify you should not mean that it is not worthy of the same protection as your name or your address.

negative amendments

These fall into two categories. Firstly, there are amendments (AMs) which limit the scope of what constitutes 'personal data'. Currently, all data linked to an individual are considered personal data. These AMs restrict the scope of personal data by establishing that data is only personal data for the organisation that processes the data (the "controller") or by a third party "working together with the controller". Apart from these parties, data relating to a natural person will not be considered "personal data" and will not be protected. AMs 715 and 716 (ALDE), 717 (EPP) & 720 (independent) fall into this category.

A 2nd set of AMs seeks to give less protection to data which are "pseudonymous", which means that a directly identifiable piece of data is replaced by a pseudonym. This lowering of protection includes all types of data that are 'pseudonimised', incl. data generated by profiling individuals' personality in online social media, for example AMs:

ALDE: 726, 728, 729, 732, 851, 887, 897, 904, 1542, 1568 - EPP: 730, 898, 921, 922, 1543, 1585, 1630.

positive amendments

Positive amendments seek to clarify that the "singling out" of individuals produces personal data, while maintaining the main direction of the Commission's original proposal. Such amendments include:

ALDE: 714 - S&D: 719 - EPP: 721

LAW ENFORCEMENT ACCESS

The PRISM scandal shows us that pseudonymous data are at considerable risk of access and identification from anyone that has the ability to access multiple databases. As pseudonymised data are often used for the creation of detailed personality profiles by online advertising companies, the potential impact of re-identification of data is enormous. The fact that some of the data are only indirectly identifiable or pseudonymised does not in any way reduce the intrusion into each individual's privacy and freedom of communication.

EUROPEAN DIGITAL RIGHTS