07 PROFILING

What is needed?

Profiling is a process whereby assumptions are made about individuals based on automated processing of data which has been collected about them. This type of profiling is most commonly used for business purposes (for targeted advertising or credit ratings, in particular) and for law enforcement purposes. Due to the ever-increasing scale of electronic data collection and the increasing complexity of profiling calculations, the types of data being generated are becoming more and more privacy-intrusive. Profiling tends to reinforce societal stereotypes and has a built-in acceptance of errors – the profile will guess who is a potential terrorist or a bad insurance risk. The fact that it might be wrong 5% of 10% of the time is not important from the perspective of the business, but of potentially huge importance to the individual citizen. Recent research from the University of Cambridge shows that surprisingly extensive, sensitive and relatively accurate information can be obtained about an individual based on small amounts of data.

As a result, it is important that profiling be prohibited both online and offline unless certain strict conditions are met, including the consent of the individual. Strong safeguards should be put in place, including the right to be provided with meaningful information about the logic behind the profiling.

negative amendments

Negative amendments seek to change profiling from an opt-in provision (where positive consent is needed) to an opt-out rule (where individuals can be subjected to profiling but have the right to object or request not to be profiled). In effect, such amendments would allow citizens to be tracked without their knowledge or consent.

ALDE: 1545, 1547, 1555, 1556, 1557, 1559, 1560, 1568, 1572

EPP: 1549

ECR: 1553

S&D: 1551

Independent: 1554

positive amendments

Positive amendments seek to strengthen and clarify the rights of the individual.

EPP: 1546, 1548,

ALDE: 1550, 1561,

S&D: 1552, 1562, 1563

LAW ENFORCEMENT ACCESS

We have seen from the stockpiling and use of airline passenger name records (PNR), financial data (TFTP) and communications data (data retention) that big databases will inevitably be re-used – often illegally – for "law enforcement" purposes. The types of data that can be generated by profiling includes the most sensitive personal information (sexual orientation, political orientation, family relationships, health-related information, etc).

The fact that these data will be stockpiled over months and years means that profiling companies will have a more profound insight into individuals' lives, trends and location than the individuals will have about themselves, particularly with regard to older information.

This is a new and growing threat to personal privacy and security that must be treated with utmost seriousness.

It is absolutely crucial for both privacy and that the collection and to avoid a profound chilling effect for online communication that profiling can only be done with consent and with a right to erasure.

EUROPEAN DIGITAL RIGHTS