Resolution

on web tracking and privacy

35th INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS
PRIVACY: A COMPASS IN TURBULENT WORLD
Warsaw, 23-26 September 2013

Web tracking allows organisations to monitor almost every single aspect of user behaviour on the Web. The type of information that can be collected through tracking (e.g., IP addresses, device identifiers, etc.) can lead to the identification of a particular data subject. This capability creates the potential for organisations to develop a rich profile of an identifiable data subject's online activities over extended periods.

Data on user activity, collected from a computer or other device (e.g., a smart phone) while using various services of the information society on the Internet, are increasingly combined, correlated and analysed by different actors for various purposes ranging from charitable to commercial purposes of the different actors offering such services or parts thereof. Generated interest profiles (or "user profiles") can be enriched with data from the "offline world" on almost every aspect of private life, including financial information as well as information on, for instance, leisure interests, health concerns, political views and/or religious opinions.

We recognise that tracking offers some consumer benefits, such as network management, security, and fraud prevention, and may facilitate the development of new products and services. Nevertheless tracking poses serious privacy risks for citizens in an information society, threatening to erode the core privacy principles of transparency, purpose limitation and individual control.

Consequently, all stakeholders, including governments, international organisations and providers of information services should prioritise the protection of privacy in the design, provision and use of services of the information society.

The International Conference of Data Protection and Privacy Commissioners therefore calls on all stakeholders to do the following where relevant and appropriate:

- observe the principle of purpose limitation;
- provide notice and control over the use of tracking elements, including device and browser fingerprinting;
- refrain from the use of invisible tracking elements for purposes other than security/ fraud detection or network management
- refrain from deriving a set of information elements (fingerprint) in order to uniquely identify and track users for purposes other than security/fraud prevention or network management;
- ensure adequate transparency about all types of web tracking practices to enable informed consumer choices;

The Information Commissioner of the Republic of Slovenia and the French data protection authority abstained from voting on this resolution

- offer easy to use tools to allow users appropriate control over the collection and use of their personal data;
- avoid tracking children and tracking on websites aimed at children absent verifiable parental consent;
- respect the principle of privacy-by-design and conduct a privacy impact assessment at the start of new projects;
- use techniques that reduce the privacy impact, such as anonymisation / pseudonymisation;
- promote technical standards for better user control (e.g., an effective Do-Not-Track standard).