

What are the different types of cross-device tracking, how do they work, and what are they used for?

There are a range of different technologies which could be employed to achieve cross-device tracking which could operate in a covert or overt manner. These could form part of an existing system (e.g. within a web page, mobile app) or operate in a standalone manner. These can include:

- Cookies and similar technologies
- User authentication (e.g. web or app login)
- Tracking of location data
- Monitoring of device identifiers (e.g. UDID, MAC or IP address)

Some technologies may also deliver tracking of the individual in the “real-world” such that behaviours collected online can be linked with real-world behaviours and outcomes. For example, tracking across devices may enable the delivery of advertisements for a certain product. Such advertisements or messages could be delivered to an in-store display or sent via electronic message or post. Tying this with tracking in a physical store may assist in the measurement of conversion of messaging into a behaviour such as a sale at the checkout.

The Article 29 Working Party and the International Working Group on Data Protection in Telecommunications have published guidance of some technologies which may support cross-device tracking:

- [Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting](#)
- [Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential](#)

There is also [a case](#) currently being heard in the UK courts against Google on the case of so-called “browser generated information” and an alleged circumvention of browser cookie controls for the purpose of delivering targeted advertising.

What types of information and benefits do companies gain from using these technologies?

Individuals may use different devices for different purposes. A smart TV and set-top box will be heavily used for entertainment where as a smart phone may be used for more casual internet browsing, messaging and social networking. Individuals may also perform research on one type of device during a particular part of the day (e.g. on a tablet during a commute) and then convert this to a purchase on a different device (e.g. on a laptop at home in the evening). An organisation which is able to perform cross-device tracking would be able to more effectively differentiate between individuals.

The benefits will also depend on the type, quality and granularity of the data. This can be tied to a specific individual and record data over time, be stored in a pseudonymous format and unable to be linked to repeat visits or aggregated with other individuals in an anonymous manner.

Furthermore, information relating to individuals may also be obtained from social media as this information also forms part of the “cross-device tracking”.

What benefits do consumers derive from the use of these technologies?

The benefit to the individual can range depending on the immediacy and directed nature of the effect. This might be considered as:

- Direct benefits – Where the benefit is provided in, or near, real-time and the user can take a specific informed action such as be informed of a traffic delay or receiving a targeted discount.
- In-direct benefits – Where the benefit is less tangible and may be realised at some point in the future such as having a shorter queuing time at a future visit because the organisation has employed additional staff.

Actual benefits to organisations and individuals may not be equal and could be highly skewed one way or the other. This will depend on the direction of the information flows.

What are the privacy and security risks associated with the use of these technologies?

Key privacy risks lie in the fact that such technologies will increase with the volume and type of data that is collected and processed about individuals. It will be the responsibility of the organisations to ensure that individuals are fully informed about the data collection and subsequent processing and given effective tools in order to control such processing.

There is also a risk that large volumes of data which are considered anonymous actually permit the re-identification of individuals either by itself or in combination with other datasets.

From a security perspective the creation of larger and more comprehensive data sets brings an ever increasing level of harm should that data set be lost, stolen or otherwise subject to unauthorised access or processing.

The Article 29 Working Party has published a number of Opinions on these risks:

- [Opinion 8/2014 on the Recent Developments on the Internet of Things](#)
- [Working Document 02/2013 providing guidance on obtaining consent for cookies](#)
- [Opinion 02/2013 on apps on smart devices](#)
- [Opinion 04/2012 on Cookie Consent Exemption](#)

UK's Information Commissioner's Office and the International Working Group on Data Protection in Telecommunications have published guidance of the privacy and security risks associated with "big data":

- [Big data and data protection](#)
- [Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics](#)

How can companies make their tracking more transparent and give consumers greater control over it?

The UK's Information Commissioner's Office has published a Code of Practice to guide organisations through an impact assessment to assess the privacy risks in new projects and address them effectively in addition to guidance to describe important aspects of communicating privacy information effectively:

- [Conducting privacy impact assessments code of practice](#)
- [Privacy notices code of practice](#)

The ICO has also published a Code of Practice which described how organisations who are operating online should use information when they do business online:

- [Personal information online code of practice](#)

Following a review of the changes proposed by Google to their privacy policy the Article 29 Working Party highlighted a number of areas of concern and formed a [taskforce of national data protection authorities](#) to undertake the necessary actions.

The Information Commissioner's Office required Google to [sign](#) a formal undertaking to improve the information it provides to people about how it collects personal data in the UK after concerns were raised around changes to the company's privacy policy. The ICO found that the search engine was too vague when describing how it uses personal data gathered from its web services and products. Whilst this undertaking does not reference cross device tracking it highlights the importance of transparency and providing information in a clear and comprehensive manner to individuals using a service.

Do current industry self-regulatory programs apply to different cross device tracking techniques?

It is not appropriate for the ICO to answer this question.