Newsflash Technology and Information November 2016

November 1, 2016

Introduction

Profiling and tracking has been one of the focus areas of the Dutch Data Protection Authority (DDPA). Recently the DDPA investigated the practices of WiFi tracker Bluetrace and imposed an order subject to penalty on Bluetrace for various violations of the Dutch data protection rules. The investigation and imposed order by the DDPA provide helpful insight for retail stores and shopping malls on the use of WiFi tracking in accordance with the Dutch data protection rules.

WiFi tracking

Mobile devices such as smartphones and tablets constantly emit wireless signals to find local networks to connect with. These 'probe requests' contain a unique identifier that is specific to that user's device, the media access control address (MAC address). WiFi sensors can record these probe requests and extract the MAC address for further processing and track (to a large extent) where the user of that mobile device is. With the use of multiple WiFi sensors it becomes possible to track the user's movements through and shopping behaviour in the store or shopping mall.

With the use of WiFi tracking Bluetrace collects location data of visitors and passers-by of, inter alia, stores and/or shopping malls, as well as location data of local residents (bycatch). This data allows retail stores and shopping malls to analyse user's movements and consumer shopping habits to improve efficient store layouts and use of staff and store experiences.

Data protection

The DDPA considers MAC addresses personal data and accordingly, MAC addresses may only be processed in accordance with the Dutch Data Protection Act. The DDPA addressed three violations of the Dutch Data Protection Act by Bluetrace:

1. no legal basis for the processing of personal data of local residents (as bycatch);
2. retention of personal data of passers-by and local residents for longer than is necessary; and
3. failure to adequately inform the data subjects.

In its investigation the DDPA distinguishes between the processing of personal data of visitors, passers-by and local residents.

Legal basis for the processing of personal data

The Dutch Data Protection Act sets out an exhaustive list of six justifications for the processing of personal data of which in this case only one applies: the processing is necessary for the legitimate business interests of the controller (the entity that determines the purposes and means of the processing of personal data. In this case: Bluetrace) and the interests and fundamental rights of the data subjects do not override such business interests.

The DDPA states that there is no necessity to process personal data of local residents and to retain the collected personal data of passers-by for 24 hours. People should be able to move around freely in public spaces and in their homes. According to the DDPA Bluetrace could choose to limit the scope of the data collection to the shops, so that the presence of passers-by on public streets or residents of adjacent premises is not recorded, or at least as little as possible.

Further, the DDPA establishes that the business interests of Bluetrace do not outweigh the interests and fundamental rights of local residents and passers-by. According to the DDPA Bluetrace violates the Dutch Data Protection Act by processing their personal data.

Retention of personal data for longer than is necessary

Under the Dutch Data Protection Act personal data may not be retained for longer than is necessary for the purposes for which the data were collected. According to the DDPA a retention period of 24 hours for personal data of visitors to the store or shopping mall is in accordance with the Dutch Data Protection Act.

The DDPA establishes that the personal data of passers-by should be deleted or anonymised directly after the collection of these data. As, according to the DDPA, no legal basis exists for the processing of personal data of local residents, such data should not be retained at all. Consequently, the retention of personal data of passers-by and local residents for 24 hours is not in accordance with the Dutch Data Protection Act.

Failure to adequately inform the data subjects

Under the Dutch Data Protection Act data subjects should be informed on the identity of the controller and the purposes of the processing for which the data are intended, prior to the processing of the personal data. According to the DDPA this information could be provided to visitors by clearly visible signs at the entrance of the stores and/or shopping malls. Passers-by could be informed, inter alia, via signs in the public areas outside the stores and/or shopping malls, clearly visible in the areas where MAC addresses are collected.

Further information regarding retention periods and safeguards could be provided, inter alia, via brochures available in the store or shopping mall, and through an online privacy statement.

Conclusion

Companies considering implementing WiFi tracking (or which have implemented WiFi tracking) should make sure that they meet the applicable rules to avoid the risk of high fines and damage to their brand and reputation by, inter alia:

1. avoiding the collection of MAC addresses of local residents and limiting the processing of personal data of passers-by as much as possible;
2. deleting or anonymising the MAC addresses as soon as possible. MAC addresses of visitors should be deleted or anonymised ultimately within 24 hours and those of passers-by should be deleted or anonymised directly after collection (if collected at all; see under (i)) ; and
3. prior to the actual collection of the MAC addresses, providing visitors inside and outside stores with visible and adequate information on its identity, the purpose(s) of the processing activities, the data retention period, and where visitors can obtain further information (e.g. on a website, in the store or at the information desk of the

shopping mall).

Your Key Contacts

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08
marc.elshof@dentons.com