



Excerpt from:

# WiFi tracking technology in shops and on public roads by Bluetrace

## Investigation by the Dutch Data Protection Authority, October 2015

### 6. Conclusions

On the basis of article 60 of the Dutch Data Protection Act, the Dutch Data Protection Authority initiated an official investigation into the processing of personal data by the company Bluetrace B.V., having its registered offices in Amsterdam (hereafter: Bluetrace), by means of WiFi tracking technology in shops and around shops on public roads.

Bluetrace offers clients in the retail sector WiFi sensor technology which makes it possible to register mobile devices. The Bluetrace technology makes use of the fact that smartphones automatically transmit their unique WiFi MAC address. By picking up these signals, the devices can be counted and their movements can be mapped out. As the location of a smartphone corresponds to the location of its owner during most of the day, and even at night, and because the device is almost always switched on, WiFi tracking *de facto* makes it possible to register and follow its owner. This does not only involve people who visit shops, but also people outside of shops, such as passers-by in the street.

By way of WiFi tracking, Bluetrace collects data about the number of people who visit and/or pass by a shop and about the time people spend at certain places. The data processing carried out by Bluetrace affects a large number of Dutch citizens. Bluetrace sensors are installed in shops located in dozens of large or medium sized cities in the Netherlands. Bluetrace usually installs one sensor in a shop, but the measurement range of the sensor includes the public road outside the shop. As a result, Bluetrace collects data about shop visitors and passers-by alike. Bluetrace does not inform those concerned about the fact



that they are being registered in this way and being tracked unnoticed via their mobile device. Bluetrace processes these data for the purpose of providing (location based) data analysis services to its clients and to generate relevant data on retail performance for them.

### Personal data

By way of WiFi tracking Bluetrace collects unique MAC addresses of mobile devices combined with information concerning location, date and time of registration. In this manner Bluetrace collects and processes personal data as referred to in article 1, under a, of the Dutch Data Protection Act. WiFi tracking involves the processing of personal data which are of a sensitive nature, i.e. location data of individuals. By doing so, a picture can be drawn up of the data subject's shopping pattern. Hashing of the MAC addresses as applied by Bluetrace after a period of three weeks does not lead to the conclusion that they are no longer processing personal data.

### Responsibility

Bluetrace collaborates closely with its clients in implementing WiFi tracking. Within this cooperation, Bluetrace determines the essential aspects of the data processing through WiFi tracking. Among others, Bluetrace determines which types of data will be processed, for how long and by what means. In addition, Bluetrace has actual control of all data stored in the tracking process and also controls any retention periods to be observed, as well as the provision of data to third parties. Therefore, Bluetrace cannot be considered a data processor, but is a data controller within the meaning of the Dutch Data Protection Act.

Nevertheless, there is interdependence between the activities of Bluetrace and those of its clients. In this case there is joint responsibility, because the various data processing operations by Bluetrace and its business partners are integrated. This means that both Bluetrace and its clients are jointly controlling the total of processing operations in connection with WiFi tracking. As a joint controller, Bluetrace can be held accountable for both actions that are actually in its power and for the aspects of data processing that are more or less related to what clients determine within the scope of their co-operation. The latter involves the provision of information to the public, choosing the locations to be monitored, the duration of data retention and the purposes for the application of the information related to business economics (obtained via WiFi tracking) to the client's organisation.

### Legal ground

Bluetrace does not engage in any agreements with data subjects and does not ask for their consent either. Bluetrace cannot rely on the principles as laid down in article 8, under c, d, and e, of the Dutch Data Protection Act (a statutory provision, a vital interest or the exercise of a public duty). Bluetrace has stated that it processes data concerning shoppers and passers-by on the legal ground of article 8, heading and under f, of the Dutch Data Protection Act (necessary for serving a legitimate interest).

### Lawfulness of WiFi tracking inside shops

In general, processing data of visitors in and around shops means that the interest of shop keepers in obtaining data about visitor numbers and their behaviour may, in itself, serve a legitimate interest, provided that Bluetrace informs the data subjects adequately and that the processing of personal data is necessary to realise the purposes envisaged.



However, the current working method of Bluetrace, as investigated by the Dutch Data Protection Authority, does not meet the requirements of proportionality and subsidiarity. This is because the company can achieve the set purposes in a less intrusive manner by reducing the extent of the data processing. This can be done by collecting less data, during a shorter period. Moreover, given the interests of data subjects and the sensitive nature of the location data, there are less intrusive manners in which Bluetrace can practice WiFi tracking for the set purposes. For example, WiFi tracking inside shops will be less intrusive if the personal data processed will be made anonymous as soon as possible, or at least within 24 hours.

By processing personal data for the purpose of generating information related to retail performance by way of WiFi tracking inside shops without a valid legal ground, Bluetrace is acting in violation of article 8 of the Dutch Data Protection Act.

#### Lawfulness of WiFi tracking outside of shops

Generating information related to retail performance by way of WiFi tracking outside of shops in a manner which by its nature remains concealed for data subjects cannot be regarded as an interest that is legitimate as meant in article 8, heading and under f, of the Dutch Data Protection Act. In case the processing of these data is made known to the data subjects, then it is possible to invoke the above legal ground if the processing is deemed necessary and outweighs the individual interests of the data subjects involved, in particular the protection of their privacy.

It does not appear from the investigation that Bluetrace made a deliberate choice for a method whereby the WiFi tracking outside of shops remains completely hidden to the data subject. However, the Dutch Data Protection Authority does observe that there is a profound lack of transparency. The current method applied by Bluetrace does not meet the requirements of necessity, proportionality and subsidiarity. WiFi tracking takes place 24 hours a day, 7 days a week and Bluetrace stores the data indefinitely. In the light of their right to protection of privacy, Bluetrace has insufficiently substantiated the necessity to track people (such as passers-by and neighbours) outside of shops. Bluetrace can choose to limit the scope of the data collection to the shop itself, 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. Even if Bluetrace could substantiate the necessity of this data processing and if the company would meet the criteria of proportionality and subsidiarity, then Bluetrace should anonymise the personal data irreversibly and immediately, or at least as soon as possible after the first recording.

Finally, the interests of Bluetrace do not outweigh the right to protection of the privacy of data subjects because of the lack of an effective and realistic way for data subjects to opt-out of WiFi tracking.

By processing personal data for the purpose of generating information pertaining to retail performance by way of WiFi tracking outside shops without a valid legal ground, Bluetrace is acting in violation of article 8 of the Dutch Data Protection Act.

#### Information

The Dutch Data Protection Authority establishes that Bluetrace does not provide information to the public regarding the processing of personal data gathered by way of WiFi tracking in and outside shops. Although Bluetrace carries out the WiFi tracking partly on the instructions of its clients and the WiFi tracking actually occurs at the client's location, Bluetrace, as the joint controller of the data processing, has to



provide (or give instructions to provide) information in this respect. Since Bluetrace does not provide information about the data it processes by means of WiFi tracking, Bluetrace is acting in violation of article 34 of the Dutch Data Protection Act. Because compliance with the information duties as defined in the Dutch Data Protection Act is a requirement for fair data processing, Bluetrace is also acting in violation of article 6 of the Dutch Data Protection Act.

### Retention period

Bluetrace has not established policies for data retention and in practice the company retains all data records for an indefinite period of time, in a form that allows for identification of the data subjects. The investigation has not demonstrated that, in order to reach the set purposes for which the data are processed, it is necessary to keep those data for an indefinite period of time. Therefore, Bluetrace is acting in violation of article 10 of the Dutch Data Protection Act.

After Bluetrace received the report of the Dutch Data Protection Authority on preliminary findings, the company gave an explanation of its views, containing an action plan which includes proposals for future action and further investigation into Bluetrace's procedures with regard to WiFi tracking. Bluetrace's views have not led to a modification of the conclusions of the investigation because, in the opinion of the Dutch Data Protection Authority, the proposed approach does not offer concrete prospects of ending the detected violations.