Data protection

Wi-Fi location analytics

ico.
Information Commissioner's Office

Wi-Fi location analytics

Data Protection Act

Contents

Introduction

1. The Data Protection Act 1998 (the DPA) is based around eight principles of good information handling. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

2. An overview of the main provisions of the DPA can be found in The Guide to Data Protection.

3. This is part of a series of guidance, which goes into more detail than the guide, to help data controllers to fully understand their obligations and promote good practice.

4. This guidance explains how operators of Wi-Fi and other communication networks may use location and other analytics information in a manner that complies with the DPA.

5. This guidance specifically targets the use of analytics data collected from the operation of Wi-Fi networks. It does not consider the implications of providing internet connectivity through Wi-Fi which, if provided by a public electronic communications service provider, is also subject to the Privacy and Electronic Communications Regulations.

Overview

- The processing of device identifiers collected through the provision of Wi-Fi networks can involve the processing of personal data.
- Organisations must give clear and comprehensive information for individuals to make them aware of the processing.
- Organisations must avoid excessive data collection and take steps to reduce the risk of identification of the individuals in the collected data.

What the DPA says

6. The first principle of the DPA states that:

> Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
>
> (a) at least one of the conditions in Schedule 2 is met, and
>
> (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

7. This means that people should be aware of which organisations are collecting and processing their personal data and what it is being used for.

What is Wi-Fi analytics?

8. Mobile devices such as smartphones and tablets are commonly equipped with a Wi-Fi connection for wireless connectivity either in the home or on the move.

9. Many organisations also offer Wi-Fi access to their customers as an incentive or other benefit. Organisations may also install a Wi-Fi network within their premises for business or other operational reasons for use solely by employees.

10. When a Wi-Fi enabled device is switched on, it will continually broadcast 'probe requests' in order to discover Wi-Fi networks that are within range. If it finds one that is known to the device (eg the user's home network) it may attempt to connect.

11. The probe request and response will contain an identifier that will be specific to that user's device. This identifier is known as the media access control (MAC) address and is intended to be unique to the device (although it can be modified or spoofed using software). The first part of the MAC address is also unique to the manufacturer of the Wi-Fi interface controller.

12. An organisation can therefore collect probe requests and extract the MAC address for further processing. Monitoring of the signal strength received by the access point can also estimate the distance of the device from the access point. If the user's device is within range of more than one access point then the location of the device can be pinpointed more accurately.

13. This could mean that an organisation can monitor the location of the device and track the behaviour of a particular device over time. If an individual can be identified from that MAC address, or other information in the possession of the network operator, then the data will be personal data.

14. Simply because you do not know the name of an individual does not mean that you cannot identify that individual. Using a MAC address or other unique identifier to track a device with the purpose to single them out or treat them differently (eg by offering specific products, services or content) will involve the processing of personal data.

15. Given that this type of Wi-Fi analytics does not require the device to connect to the Wi-Fi network (it is simply required for the Wi-Fi feature to be switched on) there is also a risk that data relating to an individual is processed in a covert manner.

Conduct a privacy impact assessment

16. A privacy impact assessment (PIA) is a tool that an organisation can used to identify and reduce the privacy risks and can be especially useful when considering technology such as this.

17. A PIA will help data controllers:

    - consider the types of personal data they are processing;
    - reduce the risk of harm to individuals through the misuse of their personal information;
    - design more efficient and effective processes for handling personal data; and
    - question whether it is necessary to process personal data to provide a service or deliver a project.

18. Organisations can read more information in the Conducting privacy impact assessment code of practice.

Define your purposes

19. The second principle of the DPA states that:

> Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

20. This means that organisations need to be clear from the outset about why they are collecting personal data and what they intend to do with it. Once organisations have a clearly defined purpose they can embed privacy-friendly design solutions in order to help them comply.

Be clear and transparent - notify individuals

21. Clear and prominent information is one way to alert individuals that certain processing is taking place.

22. The information should clearly define:

    - the identity of the data controller;
    - the defined purposes of the processing; and
    - information relating to any third-parties or other organisation that the data may be shared with.

23. The collection of probe requests can occur without the knowledge of the individual and therefore any further processing of personal data can occur in a covert manner.

24. Data controllers should consider the use of:

    - signage at the entrance to the collection area;
    - reminder information throughout the location where data is being collected;
    - information on their websites and in any sign-up or portal page of the Wi-Fi network they may be providing; and
    - detailed information to explain how individuals can control the collection of personal data using the settings on their device.

Remove identifiable elements

25. Organisations should consider converting the MAC address into an alternative format that suits the specified purposes and remove the identifiable elements. Retaining the MAC address in

its original form can present an unnecessary privacy risk. You should delete the original data once it is no longer required.

26. Read the ICO Anonymisation code of practice for more information.

Example
An organisation intends to use Wi-Fi analytics to count the number of visitors per hour across different retail outlets. It is not necessary to know whether an individual has visited an individual store, or multiple stores, before.

To achieve this in the most privacy-friendly manner the organisation will use a hash function so that the original MAC address cannot be determined. In order to remove the possibility of identifying repeat visitors the organisation also introduces random data into the hash function (also known as a salt).

Using the same salt value for a short period of time allows the organisation to identify an individual device but only for that limited period. Once the salt value has expired a new one is generated. It would therefore be unlikely to be able to identify stored hash values from different time periods as being derived from the same MAC address.

Define the bounds of collection

27. Data controllers should ensure that individuals are given ample opportunity to view information about processing before it occurs. They should also remember that certain areas or locations may be more sensitive than others.

28. Organisations can also consider the location of the data collection device as well as sampling methods to reduce the volume or privacy intrusion of the data collected or to define specific collection periods (eg at specified times of day).

Example
An airport is considering using Wi-Fi analytics to provide a more accurate picture of passenger journeys.

Having conducted a PIA the organisation concludes that Wi-Fi access points should not be located close to doors or windows in

order to avoid the collection of data from devices which are 'passing by' and may not have been informed about the potential for collection.

The airport also considers steps to limit collection near bathrooms and rooms set aside for staff, first-aid and worship which may have particular sensitivity.

Define a data retention period

29. The fifth data protection principle states that you must not retain personal data for longer than is necessary for the purpose you obtained it for. Data which is held at an individual level can still present a risk to data subjects even if not linked with the original MAC address.

Example
A sports stadium is considering using Wi-Fi analytics to review supporters' movements through the venue. For example, to assess whether or not there are sufficient facilities available (including toilets, concessions and first aid facilities).

Data is collected and retained on an individual level basis during the sports event and aggregate reports are generated as soon as possible after the event. Comparisons between matches are conducted using the aggregate reports.

Once the aggregate reports have been created there is no further need for the stadium to retain the individual level data and it is deleted.

Create a simple and effective means to control collection

30. Organisations should have a system in place which will give individuals a simple and effective means to control the processing.

31. Frequent visitors to a location could be subject to a higher level of data collection. This is particularly relevant to employees, contractors or volunteers. Further guidance about monitoring employees at work is available in the ICO employment practices code of practice.

32. Examples of effective control mechanisms include:

- a terminal at the location entrance into which users place their device. The terminal receives the device MAC address and offers an opt-in or opt-out choice;
- including a URL or QR code in privacy notices which direct users to a webpage where they can input the device MAC address and either opt-in or opt-out to the processing;
- including a URL on the organisation's website, Wi-Fi sign-up and portal page which directs users to a webpage where they can input their device MAC address and either opt-in or opt-out to the processing; and/or
- briefings given to regular visitors such as staff and privacy notices posted in appropriate staff areas.

An organisation may also be able to make use of an industry-wide opt-in or opt-out list to control collection. This could operate similarly to the Telephone Preference Service whereby users consent to adding their MAC address to record a preference to be, or not be to, tracked.

Contracting out

33. Organisations looking to use a third-party product or service to perform Wi-Fi analytics will need to ensure that they are processing personal data in an appropriate manner. This will include knowing which privacy-friendly mechanisms described in this guidance are in place.

34. The ICO's guidance of outsourcing for small and medium-sized businesses describes in more detail the restrictions and obligations in relation to outsourcing the processing of personal data.

More information

35. Additional guidance is available on our guidance pages if you need further information on other parts of the DPA.

36. This guidance has been developed drawing on ICO experience. Because of this it may provide more detail on issues that are often referred to the Information Commissioner than on those we rarely see. The guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.

37. It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

38. If you need any more information about this or any other aspect of data protection, please contact us, or visit our website at www.ico.org.uk.