International Working Group
on Data Protection
in Telecommunications

675.51.12

# Working Paper
# on Location Tracking from Communications of Mobile Devices

*58th Meeting, 13-14 October 2015, Berlin (Germany)*

## Scope

1. The Working Group has previously identified risks related to "*the capture of location and other personal data about the network user*"[1]. The Working Group has also adopted a common position on privacy and location information in mobile communications services[2] and discussed the use of deep packet inspection for marketing purposes[3].

2. This Working Paper specifically examines the data protection and privacy risks associated with the collection of device-related information and deriving location data from communications data. An example would be the use of Wi-Fi probe requests originating from devices such as smart phones for the analysis of footfall and traffic routes within a retail environment.

## Background

3. Communication networks require the regular broadcast of certain data packets in order to discover or maintain a connection with the network controller or other devices on the network. Furthermore, devices must have a unique address assigned in order to be differentiated on that network such that data packets can be routed to and from the correct device.

4. A single wireless base station (i.e., a transmitter and receiver), such as a mobile cellular base station or a Wi-Fi access point, has a specific range. Outside of this range (or the range of any signal repeater), the device and base station are not able to communicate with each other. A single base station is connected to compatible devices that are within range by virtue of the fact that it receives communications from the device (assuming the network connections are active). The strength of the signals can be used to infer the distance between base station and device. In order to increase the range of the network, a set of base stations is required (which may or may not have an overlapping range). Movement of a device can be inferred as it comes in and out of range of a particular base station. Where the range of the base stations overlap,

[1] Working Paper on Potential Privacy Risks Associated with Wireless Networks, 2004. http://www.datenschutz-berlin.de/attachments/197/1_en.pdf

[2] Common Position on Privacy and Location Information in Mobile Communications services, 2004. http://www.datenschutz-berlin.de/attachments/193/local_neu_en.pdf

[3] Working Paper on the Use of Deep Packet Inspection for Marketing Purposes, 2010. http://www.datenschutz-berlin.de/attachments/726/WP_DPI_07_09_2010_675_41_10__2_.pdf

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

the distance between the device and each base station can be used to calculate a more precise position using trilateration[4].

5. Communication protocols generally contain a range of different signal types for specific purposes. For example, the IEEE 802.11 wireless standards[5] define Management Frames, Control Frames and Data Frames. Each frame originating from the user's device contains the unique MAC address of the device's Wi-Fi network interface controller (NIC). A specific type of Management Frame is the Probe Request which is actively broadcast by the NIC in order to search for available networks in the area. An organisation can therefore install a set of Wi-Fi access points (e.g., as part of an in-store Wi-Fi network) or frequency scanner and collect the MAC address of any device within range (assuming the Wi-Fi feature of the device is switched on). Given that the MAC address of a particular NIC is normally static, monitoring for the re-occurrence of a particular MAC address indicates the return of that particular device.

6. Many of these types of device, especially smartphones, can be intimately linked to a specific individual. Therefore the collection of the MAC address, in combination with data such as date and time, could easily lead to the direct or indirect identification of the device owner.

7. Other wireless communication protocols such as Bluetooth and cellular telephone standards similarly involve the broadcasting of active signals containing unique identifiers. In the case of Bluetooth, this is the MAC address of the Bluetooth NIC. The International Mobile Station Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI) and Temporary Mobile Subscriber Identity (TMSI) are broadcast at varying intervals in the case of GSM (Groupe Speciale Mobile, a global standard for mobile communications).

8. Device identifiers such as the MAC address and IMSI also contain information relating to the device itself. For example, the first three octets of the MAC address identify the organisation which issued the NIC which may reveal information about the device manufacturer or the type of device being tracked. The first three digits of the IMSI relate to the country code which is followed by the mobile operator code. Bluetooth and Wi-Fi devices also have a configurable device name which can be transmitted.

9. Service providers have emerged who do not act as a communications network offering internet access but exclusively offer location tracking services based on the use of scanning equipment to collect the traffic data described in this working paper, for example, collecting Wi-Fi probe requests without the associated internet connectivity or solely to collect Bluetooth signals. The risks emerging from location tracking technologies are also not exclusively confined to the traditional retail environment (i.e., individual stores or shopping centres). Many other business premises including railway stations and airports utilise the technology to monitor or track individuals.[6] Law enforcement agencies may also make use of such technology.

---

[4] Trilateration is the process of determining location using distances from known points. This differs from triangulation which uses the measured angle from known points.

[5] http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[6] For example, Schiphol Airport (https://www.schiphol.nl/SchipholGroup/ NewsMedia/PressreleaseItem/AmsterdamAirportSchipholFirstAirportInEuropeWithFullBeaconCoverage.htm), Barcelona/Madrid Airports (http://cdn1.pps-publications.com/airport-business-archive/2015/ab-summer-2015.pdf), "*allows passengers to get real-time information on flights, transition times, commercial offers and other services through the implementation of iBeacons based on Bluetooth wireless technology*"), London City Airport (http://annual.aci-na.org/sites/default/files/Collier-ACI-NA%20September%208%202014%20v2.pdf, see slides 'Passenger Journey Measurement'), New York JKF (http://www.citylab.com/navigator/ 2015/08/your-phone-could-help-make-airport-lines-

10. Furthermore, the advent and incorporation of Bluetooth 4.x NICs (also known as Bluetooth Low Energy or BLE) has given rise to so-called “hyper-local” geolocation services. Operating with a short range, BLE beacons can be used by a device to calculate its location (or have its location calculated) with a high degree of accuracy.

11. An increase in the number of mobile devices equipped with Wi-Fi together with an increase in the prevalence of in-store Wi-Fi and a desire from organisations for greater insight into customer behaviour has created a momentum for the development and deployment of location tracking technologies. This is not limited to Wi-Fi as Bluetooth may also be switched on by default or being used by an individual for their own purposes (e.g., to enable handsfree voice calls, smartwatch/wearable device connectivity or wireless headphones).

12. As communication capabilities are incorporated into an ever growing number of devices the potential for tracking these devices will increase. In some cases, multiple device identifiers can be associated with a single individual to further increase the effectiveness of tracking (e.g. a single individual could carry multiple smart phones, tablets, a smartwatch, a fitness band, and drive a connected vehicle).

**Data Protection and Privacy Risks**

13. A significant number of the risks to data protection and privacy arise from the fact that location tracking of mobile devices (technically) operates in a covert manner. As is the case with Wi-Fi, simply being present within a particular location and carrying a device with Wi-Fi enabled is sufficient to allow data to be collected and processed. The device owner does not have to make an active choice to connect, or attempt to connect to the network. Even though some technologies such as BLE may require an action by the user to enable the function, the function can remain switched on, or is even enabled by default by the operating system. In these circumstances, the user is likely unaware of the location tracking potential.

14. These risks are especially prevalent when location tracking is active in public spaces as the opportunities to provide adequate information in a timely manner may prove to be limited.

15. The invisible nature of the tracking and a desire by an organisation to perform such tracking behind the scenes so as to not interrupt the consumer experience presents privacy challenges with regard to transparency, accountability, individual awareness and user choice.

16. These privacy and data protection risks include:

    a. The covert collection of a range of information such as device specific identifiers that can easily be linked to specific individuals;

    b. The monitoring of an individual’s location, route and dwell time;

    c. The tracking of an individual over time, including repeat visits to a specified location[7] or location within range of the Wi-Fi network;

---

shorter/401942/), Helsinki Airport (https://www.finavia.fi/en/news-room/news/2014/a-global-first-helsinki-airports-new-technology-to-develop-the-travel-experience/) and Middle East airports (http://www.arabianaerospace.aero/middle-east-airports-going-smart-for-seamless-travel-experience.html)

[7] Location in this context could include inside and outside an organisation’s premises and include the tracking across multiple premises.

d. The potential sensitivity of the data collected or information which can be inferred from an individual's location;

e. The collection and combination of tracking data from different networks and/or locations to build a comprehensive picture of an individual's movements across a wide scale (e.g., data combined from different retailers or collected by a third-party network controller operating across multiple premises);

f. The combination of tracking data with other online and offline information, including but not limited to, loyalty card account, social media, (inferred) demographic data, payment card and transaction history or CCTV (with or without additional video analytics technology), which could lead to excessive collection of data;

g. The challenges of adequately de-identifying or anonymising the collected data;

h. A lack of transparency and information given to the user. This is further compounded if a device is limited by size or display capability;

i. The lack of a simple and effective means for the user to control the collection of data by either opt-in or opt-out depending on the legal requirements in the respective jurisdiction[8];

j. Creation of blacklists or whitelists based on the collected information;

k. The collection of employee data or data about other individuals frequently present in the area and the potential for the data to be used for unspecified or incompatible purposes including monitoring of workplace performance or disciplinary action;

l. Data being subject to access by law enforcement;

m. Poor network security failing to protect against the interception of communications or failure to adequately protect the collected data;

n. The use of information for profiling, advertising or direct marketing; and

o. A lack of clear accountability by the organisations involved given the number of stakeholders that may be involved.

17. When a device does connect to the network (e.g., obtaining internet access via Wi-Fi rather than a network operator monitoring for probe requests), then there is also potential for the monitoring or interception of the communications.

18. Location tracking technology can be used to collect information which may not be protected by telecommunications secrecy in the classical sense.

[8] Cf. Federal Trade Commission, Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices, https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers (Company did not deliver promised in-store opt-out).

**Recommendations**

19. Organisations considering the use of location tracking technology should determine whether and/or under which specific conditions the application of location tracking of mobile devices is permitted according to the applicable privacy legislation in their respective jurisdiction.

20. In light of the above risks to privacy and data protection, it is recommended that organisations conduct a Privacy Impact Assessment (PIA) in order to ensure that they consider, and minimise, all applicable risks before deploying such a system.

21. Organisations considering the use of location tracking technologies should also be aware of existing codes of conduct[9,10,11] developed by industry associations appropriate to the intended use and application. Organisations are reminded that compliance with a Code of Conduct may not translate to immediate compliance with all requirements of a national applicable law including the necessary level of information and user choice.

22. Providers and other users of such analytics technologies including product manufacturers, operating system manufacturers and app developers must consider the privacy intrusion arising from the use of location tracking, seek to minimise the data collection, limit data retention periods and choose privacy friendly default settings.

23. In addition to compliance with applicable privacy legislation, taking into account the results of the PIA, including determining if there is a less privacy intrusive technology that could be used, the following safeguards should be considered:

    a. **Notification to individuals** – Organisations must ensure that there is sufficient information, including a range of physical and digital signage, to clearly inform individuals that location technology is in operation. The information must clearly state the purpose for collection and identify the organisation responsible. It is recommended that the industry develop a standard symbol which can be distributed throughout an area to remind individuals that the technology is in operation, similar to the effect from CCTV signage. Specific consideration must be given to staff, employees or other individuals who, if not excluded from the tracking, may be subject to extensive data collection;

    b. **Limiting the bounds of data collection** – Collection should only take place once the individual has been suitably informed and organisations must not seek to collect and monitor outside their premises. This can be achieved through careful placement of receivers, limiting data collection through a sampling method and to specified time periods or times of day (e.g., during store opening hours). The frequency of collection should also be limited to that which supports the specified purpose. The use of air-gaps to create a non-contiguous data collection area and ensuring that collection only takes place in areas which are relevant to the specified purpose should also reduce the risk of privacy intrusion. Organisations should also seek to identify "privacy zones" where no tracking can take place as a result of technical or physical measures. This can be important in areas which have particular sensitivity such as toilets or

[9] Future of Privacy Forum, Mobile Location Analytics Code of Conduct. http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf

[10] Network Advertising Initiative, Mobile Application Code. http://www.networkadvertising.org/code-enforcement/mobile

[11] Digital Advertising Alliance, Application of self-Regulatory Principles to the Mobile environment. http://www.aboutads.info/DAA_Mobile_Guidance.pdf

rooms set aside for first-aid or worship. In jurisdictions where tracking outside of the organisation's premises can be carried out in compliance with the law, sufficient safeguards should be in place to protect individuals' privacy;

c. **Anonymise data without delay** – Organisations should seek to delete or anonymise data as soon as the data is no longer required in its original form;

d. **Appropriate retention of individual level data** – In cases where there is a clear legal basis for the processing of personal data, organisations should apply methods to convert unique identifiers, such as MAC addresses, into a form which reduces the potential for privacy intrusion. For example, if the identification of repeat visits is not envisaged then pseudonymising the identifier would prevent this possibility yet still provide sufficient analytics of daily footfall and routes taken. At the end of the legally permissible retention period, the relevant data should be anonymised or securely destroyed. An analysis comparing events over multiple reporting periods (e.g., percentage change in visitors in a given period of time) can be performed by comparing individual period aggregates;

e. **Consent for the combination with other information** – Individuals should be fully informed when location data is intended to be combined with other information such as transaction history. This is especially relevant when location tracking is added as a feature to an existing loyalty scheme, for example, adding BLE beacon functionality to an existing retailer's smart phone app. The user's acceptance of an update via the app store is unlikely to be sufficient to qualify as being fully informed. Legislation in some jurisdictions may also require explicit consent for certain types of personal data[12];

f. **Consent for the sharing of individually identifiable data with third parties** – Organisations should not share data which could be used to identify an individual with third parties without the valid informed consent of the individual concerned (this would include sharing data with other clients of a single third-party location analytics provider) unless there is a lawful exception; and

g. **Implement a simple and effective means to control collection -** Organisations should also establish a system which allows individuals to control the collection of such data even in cases where this is not explicitly required by applicable privacy legislation. Organizations should prominently display the existence of choice and control options in the area of data collection. This should include an easily accessible, clearly communicated and effective means to exert control. It is recommended that a single mechanism be supported by all operators of location analytics services such that an individual is only required to express their preference once. If the tracking is based on informed consent then individuals must be enabled to revoke their consent in an easy and persistent manner. Where technically possible, clear audit trails allowing end users to know when and for what purpose data has been collected about their devices and by whom would also be recommended. Users should also be enabled to delete all or part of the previously collected data.

[12] E.g. the European Data Protection Directive 95/46/EC requires consent to be explicit for the processing of special categories of data such as revealing racial or ethnic origin or concerning health or sex life. Similar requirements for consent may also appear in the legislative frameworks of other jurisdictions.

24. Location tracking technology may not be used to intercept communications contents. In view of the strictly personal use of most smartphones, there is a need for a high level of protection for communications data generated by these devices beyond the traditional scope of telecommunications secrecy.

25. Device manufacturers and network protocol designers should consider the potential for privacy intrusion arising from the use of persistent identifiers and other publically broadcast signals. It is recommended that, where technically feasible, a mechanism be provided for such identifiers to be reset at user-defined intervals and that other privacy protecting measures be enabled by default.

**About the International Working Group on Data Protection in Telecommunications ("Berlin Group")**

The International Working Group on Data Protection in Telecommunications (IWGDPT, a.k.a. "Berlin Group") includes representatives from Data Protection Authorities and international organisations dealing with privacy matters from all over the world. It was founded in 1983 in the framework of the International Conference of Data Protection and Privacy Commissioners at the initiative of the Berlin Commissioner for Data Protection, who has since then been chairing the Group. The Group has since 1983 adopted numerous recommendations ("Common Positions" and "Working Papers") aimed at improving the protection of privacy in telecommunications. Since the beginning of the 90s the Group has in particular focused on the protection of privacy on the Internet. More information about the Work of the Group and the documents adopted by the Group are available for download on the website of the Group at http://www.berlin-privacy-group.org .