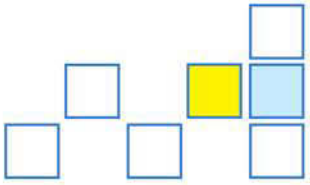
www.datenschutzzentrum.de

Location Services can Systematically Track Vehicles with WiFi Access Points at Large Scale



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Table of Contents

Location Services Can Systematically Track Vehicles with WiFi Access Points at Large Scale

Bud P. Bruegger <uld613@datenschutzzentrum.de>
Harald Zwingelberg <uld6@datenschutzzentrum.de>
Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein, Germany

May 2019

1 Executive Summary

The risk of WiFi Tracking has been well recognized. New trends in the automotive industry promise a rapid growth of the number of mobile access points (and thus affected data subjects). While tracking of WiFi-users has been recognized as high potential risk, the risk has already been realized at large scale today for users of mobile access points. In particular, two major location services are already operational today across Europe and systematically report the locations of a large percentage of mobile access points to central collection points controlled by entities outside of Europe. Considering the high data protection risk inherent in location tracking of individuals, this raises the need for mitigation to a new level of urgency.

Location services that come with modern smartphones routinely send the identifiers of visible WiFi networks to servers. This additional source of location information significantly improves the estimate of the current location as compared to using only satellite navigation and visible cellular network. Normally, WiFi access points in fixed known locations are used. The risk that this is also done for access points that move with persons is substantial, however. Such moving access points are for example built into vehicle infotainment systems or are personal hotspots activated in smartphones.

The location of such mobile access points is then picked up world-wide and systematically by a dense network of bystanders who use location services on their smartphones. This can involve devices of pedestrians or smartphones used in vehicles for navigation. The identifiers of visible access points are then predominantly sent to the servers of two non-European location service providers, possibly with storage in third countries.

In this situation, the risk arises that the location of persons is being tracked and complete movement profiles can be collected. The risk is amplified by the fact that some identifiers of access points rarely change. Those of access points built into vehicles are even considered to be "secondary vehicle identifiers"[1]. Considering the sensitive nature of location data in general and long-term movement profiles in particular, the data protection risk represented by location services must be considered high.

[1] Markus Ullmann, Tobias Franz, Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier -- Analysis, and Measurements, in Proc. VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, France, July 23 to 27, 2017, pages 32-37.

The described risk has to be seen in the context of the European Cooperative Intelligent Transport Systems (C-ITS)[2] where the avoidance of tracking of vehicle locations has reached ample attention[3]. This is for example evident in the system design that foresees frequent changes of the identifiers of vehicle2x communications. In contrast, the risks described here have fallen out of scope of C-ITS data protection studies, are likely already verified at large scale today, involve long-term stable identifiers, and it is unclear whether any mitigation measures are implemented.

The issue of tracking mobile WiFi access point has already previously been pointed out by the Article 29 Data Protection Working Party as part of their opinion on the draft of the ePrivacy Regulation[4]. In particular, in the paragraph on "WiFi-tracking" on page 3, the party states that "The European Commission is invited to promote a technical standard for mobile devices to automatically signal an objection against such tracking." In the same context, it states on pages 11 and 12: "Therefore the Working Party calls on the European legislator to promote the development of technical standards for devices to automatically signal an objection against such tracking, and to ensure that adherence to such a signal is enforceable."

The present report researches the corresponding technical situation in more detail with a particular focus on vehicles. It takes up the Article 29 Data Protection Working Party's opinion in its recommendations. It further recommends taking the case of WiFi tracking of vehicles into considerations in the negotiations of the ePrivacy Regulation.

Due to the ongoing revision of the ePrivacy Directive (2002/58/EC, amended by 2009/136/EC), specific regulations for the processing of metadata that cover such processing activities as described in this paper are not yet in place. Therefore the lawfulness of these processing activities can only be assessed against the background of the GDPR and its general legal provisions--especially the provision from Art. 6(1) GDPR. An initial assessment raises doubts whether the processing of personal data could be carried out lawfully without further measures to mitigate the high risks for the concerned data subjects.

The report discusses a wide range of possible technical mitigation measures. It considers two possible mitigation strategies, (i) one based on opt-in/consent by operators of access points and (ii) one based on opt-out/objection. The former (i) requires the creation of an additional communications channel between operators of access points and some consent management service(s). Details of this strategy are left to future work and its feasibility and uptake from business side may depend on an acceptable way to verify that issuers of consent and consent revocation are indeed the legitimate operators of the claimed access points. The latter strategy (ii) is clearly feasible and depends to a large part on existing practices (even if they are used for other purposes).

---

[2] https://ec.europa.eu/transport/themes/its/c-its_en

[3] The EU C-ITS Platform has a dedicated "Data protection and Privacy" working group chaired by DG MOVE. This working group has also asked the opinion of the Article 29 Data Protection Working Party which was issued as WP 252, 03/2017.

[4] Article 29 Data Protection Working Party, WP247, 4 April 2017, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), https://ec.europa.eu/newsroom/document.cfm?doc_id=44103 (last visited 08/03/2019).

In either strategy, no technical option seems to exist through which operators of access points can self-enforce their protection. Any mitigation solution that eliminates the tracking of WiFi equipped vehicles (and other mobile access points) in Europe requires actions taken by a range of stakeholders, including producers of access points, producers of location service clients, and operators of location service servers.

2 Acknowledgements

The presented issue was discovered as part of a data protection impact assessment[5] conducted within the iKoPA project funded by the German Federal Ministry of Education and Research[6]. The experience of how to best handle an unexpectedly discovered major data protection issue during ICT research is being used for the EC-funded PANELFIT project[7].

3 Scope

While location services may utilize other location sources such as cell towers of mobile telephony or Bluetooth beacons, the present discussion is limited to using WiFi access points as location source. Location services can track both, users of the location service and operators of WiFi access points. The scope of the present discussion is limited to the latter.

4 Main Purpose of Processing

Location services that involve WiFi access points pursue the following main purpose:

> Translate a set of identifiers of visible WiFi networks with their respective signal strengths into the coordinates of a location by trilateration[8] between known network locations.

For this purpose, it is necessary to compile, maintain and access a database of the locations of WiFi networks since these are the basis for the necessary trilateration computations.

Apple clearly documents this under the heading "Crowd-sourced Wi-Fi and cellular Location Services"[9]:

---

[5] Bud P. Bruegger (ULD), iKoPA Deliverable 3.3, Data Protection Impact Assessment of Mobility-Related Communications, https://ikopa.de/wp-content/plugins/download-attachments/includes/download.php?id=516, last visited 18/02/2019.

[6] Funded by the German Federal Ministry of Education and Research (BMBF) under FKZ 16EMO0131; https://ikopa.de/ (last visited 18/02/2019).

[7] PANELFIT is supported by the European Commission under the Horizon 2020 – Research and Innovation Framework. Grant Agreement number: 788039 -PANELFIT- H2020-SwafS-2016-17/H2020-SwafS-2017-1; https://panelfit.eu/ (last visited 08/05/2019).

[8] https://en.wikipedia.org/wiki/True_Range_Multilateration (last visited on 15/01/2019).

[9] About privacy and Location Services in iOS 8 and later, web page, https://support.apple.com/en-us/HT203033 (last visited 14/01/2019).

If Location Services is on, your device will periodically send the geo-tagged locations of nearby Wi-Fi hotspots and cell towers to Apple to augment Apple's crowd-sourced database of Wi-Fi hotspot and cell tower locations. …

In order to construct a database of network locations, the identifiers of networks need to be "geo-tagged" or otherwise related to a location. This can be achieved directly by relating coordinates from satellite navigation with the set of visible networks, or indirectly by relating a network of yet unknown location with networks or cell towers of known location.

5 Components of Location Services

Figure 1 illustrates among others the basic components of location services, namely (i) the WiFi access points on the left, (ii) a location service client app running on a smartphone in the middle, and (iii) the location service server(s) on the right. Usually, the smartphone receives also signals from navigation satellites as additional source of location information. In the sequel, these major components are described in further detail:

5.1 WiFi Access Points

WiFi access points provide wireless access to either a local network or the Internet (e.g., via a wired connection or an LTE wireless uplink). In the former case, the local area network typically enables WiFi enabled devices to access some service such as printing on an attached printer or the playing of audio and video on an attached (or combined) car head unit or infotainment system. In the latter case, connecting to the access point provides Internet access to local WiFi enabled devices. The cases can obviously also be combined.

For the present discussion, two types of access points are relevant:

- Fixed-location access points,
- Mobile access points.

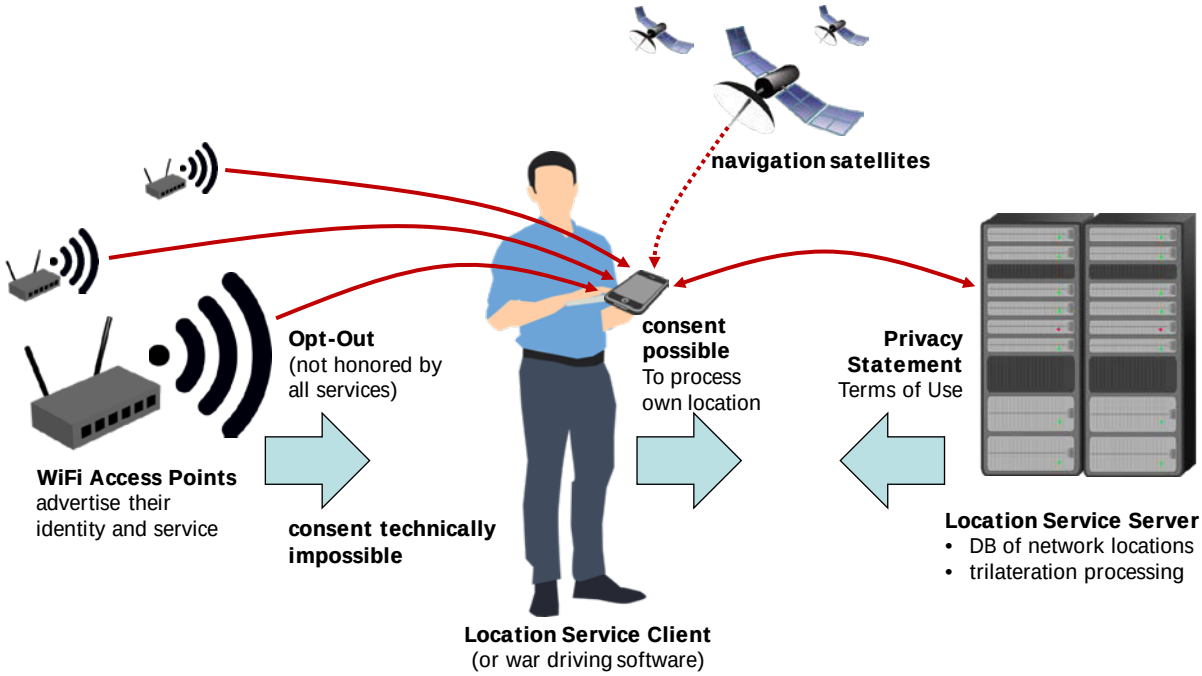


Figure 1: Basic components and flows of a location service.

Examples for fixed access points include WiFi capable home routers, access points of company networks, and hotspots of public access WiFi networks in supermarkets or airports.

Currently, there seem to be two main types of mobile access points:

- Smartphones acting as personal hotspots through tethering and
- vehicle-based WiFi access points.

While the trend first started with luxury vehicles[10], built-in WiFi access point become ever more common in modern cars. These are typically part of the infotainment systems or head units. One driver for this is the connection of smartphones to vehicle head units via Google's *Android Auto*[11] and Apple's *CarPlay*[12], respectively. Both are now supported by all major car manufacturers[13]. For both, the bandwidth of Bluetooth is insufficient for wireless operations and they therefore require WiFi access points[14].

---

[10] Rick Popely, Which 2017 Cars Offer In-Car Wi-Fi?, December 2, 2016, cars.com, https://www.cars.com/articles/which-2017-cars-offer-in-car-wi-fi-1420692490461/(last visited 14/01/2019).
[11] https://www.android.com/auto/
[12] https://www.apple.com/ios/carplay/
[13] For Android Auto, expand the *Compatible Vehicles* Tab at https://www.android.com/auto/ (last visited 14/01/2019); for CarPlay see https://www.apple.com/ios/carplay/available-models/ (last visited 14/01/2019).
[14] For Android Auto, see Jeremy Laukkonen, Android Auto Wireless: What It Is and How To Use It, lifewire, November 07, 2018, https://www.lifewire.com/android-auto-wireless-4176354 (last visited 14/01/2019), section "How Does Android Auto Wireless Work?"; for CarPlay see CarPlay Life, How to make CarPlay wireless, April 29, 2018, http://www.carplaylife.com/feature/how-to-make-apple-carplay-wireless/ (last visited 14/01/2019).

This trend can be further confirmed by looking at the infotainment options of major car manufacturers or the available after-market infotainment systems that commonly feature WiFi access points starting from a medium price range[15] .

Besides infotainment-oriented offerings, telecommunication service providers and third party vendors offer after-market solutions for in-vehicle Internet connection at contained prices. Examples include Telekom's CarConnect[16] that plugs in the car's OBD II port and Huawei's HiLink CarFi LTE Router WiFi Hotspot[17] that plugs in the cigarette lighter.

The most common form factors of in-vehicle WiFi access points are visualized in Figure 2.

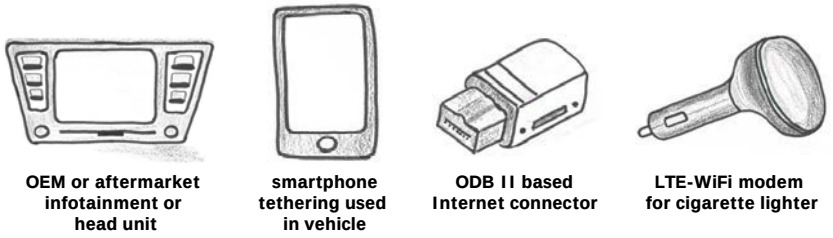


Figure 2: Common form factors of in-vehicle WiFi access points [18].

5.2 Location Service Clients and Servers

This section discusses both, clients and servers since they are usually closely linked.

A variety of possible location service clients exist. The most common are those that are packaged as integral parts of smartphone operating systems. In particular, Android devices incorporate Google's location service and iOS devices incorporate Apple's. Both clients are intrinsically linked to the matching servers. Most users are unaware that any alternatives to these integrated location services exist.

Smartphone users who want to choose alternative location services can do so on Android by downloading, installing, and configuring the App called *Unified Network Location Provider*[19] plus a backend for the chosen server. This does not seem to be possible on iOS[20]. Wikipedia currently lists eight potential alternatives[21] to Google's and Apple's servers. Backends for the *Unified Network*

[15] For example, two out of four infotainment options offered by Skoda contain built-in WiFi hotspots: http://master.skoda-auto.com/models/new-superb/new-superb-infotainment-phase-2#ColumnRepeaterLiteWebPart_2 (last visited 14/01/2019).
[16] https://www.telekom.de/unterwegs/telekom/telekom-carconnect-adapter (last visited 14/01/2019).
[17] https://www.amazon.com/d/Cell-Phones-Accessories/Huawei-E8377s-153-HiLink-Router-Hotspot/B00PICUNRA (last visited 14/01/2019).
[18] Graphics by Angelika Martin, ULD.
[19] https://github.com/microg/android_packages_apps_UnifiedNlp (last visited 15/01/2019).
[20] https://wiki.mozilla.org/CloudServices/Location/Software#iOS (last visited 15/01/2019).
[21] https://en.wikipedia.org/wiki/Wi-Fi_positioning_system#Public_Wi-Fi_location_databases (last visited 15/01/2019).

Location Provider are available for some, for example the *Mozilla location service*[22] and *Radiocells.org*[23]. A backend to access the *Apple location server* from Android is also available[24].

Figure 1 above shows the architecture of location services where the main purpose is the estimation of client locations. The very same components and interactions can also be used to compile databases of WiFi network locations for other purposes, however. This is usually called *war driving*[25]. The only difference is that clients do not expect to receive trilaterated locations in response to an upload of network data. Instead, the network location database can for example be queried independently of uploads to find freely accessible WiFi networks.

There is an ample selection of dedicated client software for war driving[26]. War driving capability can also be integrated with software for other purposes. For example, *Firefox for Android* has a war driving functionality that interacts with the Mozilla location service[27] . Like in the case of location services, also in war driving, bundling with software that has a significant market share seems to benefit the compilation of a database.

The war driving severs include those eight listed by Wikipedia (see above). Their diversity is considerable. Services like *Combain*[28] and *Navizon*[29] seem to be purely commercial. The same goes for *Skyhook Wireless*[30]. *Radiocells.org*[31] is a community project based on free licenses and supports besides geolocation also scientific research by providing also raw measurement data. Also *WiGLE* states among its possible uses everything from a fun hobby over finding usable networks to educating the public, research projects, and journalism[32]. The *Mozilla location service* is interesting since one of two stated goals is to "*improve the privacy aspects of the geolocation service compared to the current market offerings*"[33].

For readability, this report often simplifying uses the term *location service*, where *location service and war driving* would be technically more precise.

---

[22] https://github.com/microg/IchnaeaNlpBackend (last visited 15/01/2019).
[23] https://f-droid.org/en/packages/org.openbmap.unifiedNlp/ (last visited 15/01/2019).
[24] https://f-droid.org/en/packages/org.microg.nlp.backend.apple/ (last visited 15/01/2019).
[25] https://en.wikipedia.org/wiki/Wardriving (last visited 15/01/2019).
[26] See for example https://en.wikipedia.org/wiki/Wardriving#Software, https://wiki.mozilla.org/CloudServices/Location/Software, and https://wigle.net/faq/ (all last visited on 15/01/2019).
[27] https://wiki.mozilla.org/CloudServices/Location/Software#Firefox_for_Android (last visited on 15/01/2019).
[28] https://combain.com/ (last visited on 15/01/2019).
[29] https://www.navizon.com/ (last visited on 15/01/2019).
[30] https://en.wikipedia.org/wiki/Skyhook_Wireless (last visited on 15/01/2019).
[31] https://www.radiocells.org/ (last visited on 15/01/2019).
[32] https://wigle.net/faq (last visited on 15/01/2019).
[33] https://wiki.mozilla.org/CloudServices/Location#Goals (last visited on 15/01/2019).

6 Functionality and Data Flows of Location Services

Still referring to Figure 1, this section describes the functionality and data flows of a location service. It is organized by components.

6.1 WiFi Access Points

WiFi access points constantly advertise their services in beacon frames[34]. These advertisements contain among others two network identifiers:

- The *Basic Service Set Identifier* (BSSID) that (in infrastructure mode) is the same as the access points Media Access Control (*MAC*) address[35]. Its format follows the IEEE EUI-48 specification and is thus 48 bits or 6 Bytes long[36]. The first 3 Bytes, the organizationally unique identifier (OUI), is unique for the manufacturer. It also contains one bit that indicates, whether the address is *globally unique*, i.e., set in hardware, or *locally administered*, i.e., assigned by software[37]. *Globally unique* addresses are invariant over time; *locally administered* addresses can change, as is for example used in MAC address randomization[38]. An example for a BSSID/MAC is *fc:f5:28:d4:cd:f0*.
- The *Service Set Identifier* (SSID) that identifies the network. This name is human readable, initialized to a default value by the manufacturer, and then freely set by the network administrator. An example for an SSID is *Privacy4free*.

A single network, identified by the SSID, can have multiple access points, identified by their BSSIDs/MAC addresses. Access to the network is administrated at network level. Thus, no matter which access point of a network is the closest, the same password can be used. The automatic connection feature of smartphones is organized by SSID. This means that it is possible to add or exchange access points with unknown BSSIDs to a network, without affecting how clients connect.

In the context of location services, the entity that can be located is the access point identified by its BSSID/MAC. A network, identified by its SSID, that has multiple access points, fails to have a well-defined location and it is not possible to measure the signal strength of a network.

At least Apple uses the *globally unique/locally administered* bit in the MAC address to distinguish between fixed access points (such as AirPort models) and client devices operating in hotspot mode[39]. In particular, fixed access points use *globally unique* MAC addresses while personal

[34] https://en.wikipedia.org/wiki/Beacon_frame (last visited on 15/01/2019).
[35] https://www.juniper.net/documentation/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-ssid-bssid-essid.html#jd0e46 (last visited on 15/01/2019).
[36] https://en.wikipedia.org/wiki/MAC_address (last visited on 15/01/2019).
[37] https://en.wikipedia.org/wiki/MAC_address#/media/File:MAC-48_Address.svg (last visited on 15/01/2019).
[38] https://www.airsassociation.org/airs-articles/item/19456-mac-randomization-a-massive-failure-that-leaves-iphones-android-mobes-open-to-tracking (last visited on 15/01/2019).
[39] Jeremy Martin et al., Decomposition of MAC address structure for granular device inference, ACSAC, 2016, https://www.cmand.org/furiousmac/furiousMAC.pdf (last visited on 15/01/2019), section 3.2.1, page 4, "Apple hotspots".

hotspots seem to use *locally administered* addresses. A quick experiment showed that also some versions of Android seem to use *locally administered* MAC addresses for personal hotspots.

Whether this method for tagging mobile access point is used in any vehicle-based access point remains a topic of future research. The single WiFi MAC address described by Ullmann et al[40] (from an Opel Insignia) is a *globally unique* address although the access point is obviously mobile.

WiFi access points initiate the data flow in a location service by broadcasting the mentioned two identifiers in clear text to every recipient in radio range. This also includes location service and war driving clients. These receive both, the BSSID/MAC and the SSID. In addition, they can measure the signal strength of the access point.

The collection of WiFi network identifiers by the Google *Street View* campaign was met with criticism[41]. As one of the consequences, Google introduced the possibility to opt-out from being added to their access point database[42]. More precisely, they exclude all WiFi networks whose SSID ends with the string "*_nomap*". Some, but not all location services honor this opt-out mechanism[43]. A search on opt-out mechanisms offered by Apple came up empty.

This opt-out mechanism coded into the SSID is specifically designed for location services. It is the only mechanism available to access point owners to influence how their network identifiers are processed in by the location service. Since not all location services honor the mechanism, its effectiveness is limited, however.

6.2 Location Service Clients

When location service clients are enabled and configured to use WiFi, they periodically assess the visible access points and their respective signal strengths. Both, the access point's BSSID/MAC and SSID are received.

Now the clients filter the access points they want to process. Clients that honor the opt-out mechanism exclude access points whose SSID ends in "*_nomap*" from processing.

In addition and optionally, location service clients also acquire their current position from the satellite navigation module.

Depending on the location service client, a specific subset of the acquired data is sent to the server in order to receive back the trilaterated position. The purpose (i) of estimating a position through

---

[40] Markus Ullmann, Tobias Franz, Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier – Analysis, and Measurements, in Proceedings, VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, France, July 23 to 27, 2017, page 36.

[41] See for example https://www.wired.com/2012/05/google-wifi-fcc-investigation/ and https://www.engadget.com/2013/04/22/google-street-view-fine-germany/ (both last visited on 24/01/2019).

[42] https://googleblog.blogspot.com/2011/11/greater-choice-for-wireless-access.html (last accessed on 15/01/2019).

[43] https://en.wikipedia.org/wiki/Wi-Fi_positioning_system#Public_Wi-Fi_location_databases (last accessed on 15/01/2019).

trilateration requires that at the minimum, the BSSIDs/MAC addresses[44] and signal strength of access points (that don't opt out) are sent. Sending also the current satellite navigation position greatly aids[45] the purpose (ii) of compiling and refining a database of access point locations.

Several location service clients send also the full or hashed SSID to the server. Other data that is sent is the security setting of the network, the mode (managed or ad-hoc), the channel, the frequency, and the noise level.

6.3 Location Service Servers

When a location service server receives data on visible WiFi access points from a client, it executes the following steps:

In a first, optional step, the server can further filter to exclude additional WiFi access points from processing. For example, it could exclude personal hotspots that it recognizes from BSSIDs/MAC addresses with the *locally administered address* bit set. Whether any existing server performs such a filtering step is a question of further research.

In a second step, a position is trilaterated[46] between known access points and sent as a response back to the client. For this purpose, the server needs to compare the submitted BSSIDs/MAC addresses to its data base to find out which of them have a known location.

In a third step, the server decides whether the data sent from the client are suited to maintain the database of WiFi access point locations. Maintenance can consist of adding new access points to the data base, refining their location, validating the correctness of a known location, or classifying the access point as unreliable.

An examples for classifying access points as unreliable were given by Google and Skynet in 2011. Both examples are responses to a request for comment from cnet's Declan McCullagh to an article on tracking with locations services[47].

Google stated that "We collect the publicly broadcast MAC addresses of Wi-Fi access points. If a user has enabled wireless tethering on a mobile device, that device becomes a Wi-Fi access point, so the MAC address of such an access point may also be included in the database. Wi-Fi access points that move frequently are not useful for our location database, and we take various steps to try to discard them."

---

[44] Note that also a pseudonym for the BSSID/MAC address would suffice but the limited length of 48 bits, the predictability of the first half and the systematic assignment of the second possibly render the generation of pseudonyms little effective for the purpose of data protection.

[45] Note that even in absence of satellite navigation data, the location of a new access point can be estimated based on other access points that are also visible and whose location is already known.

[46] https://en.wikipedia.org/wiki/True_Range_Multilateration (last visited on 15/01/2019).

[47] See https://www.cnet.com/news/exclusive-googles-web-mapping-can-track-your-phone/ under the heading "Companies respond" (last accessed 15/01/2019).

Mike Shean, co-founder of Skyhook Wireless, states: “Do we see access points in several places? Are they mobile? If so, we'd rank that access point in a way that marked it as mobile, and reduced our level of confidence in using it in our system.”

7 Parties Involved and How They Influence Processing

Location services involve a multitude of parties who exercise different kinds of influence on the data processing. These are described in the following structured by the component shown in Figure 1 that they are associated with.

7.1 WiFi Access Points

Access Point Manufacturers

Manufacturers of fixed or mobile WiFi access points determine the hardware, software, and default configuration of their products. They further provide manuals, instructions, and dialogs in the user interface that guide *operators* on how to use and configure their device. Of particular interest for this discussion are mobile access points. Manufacturer decisions that influence the processing of a location service include the following:

- Manufacturers assign MAC addresses to their devices. This includes the decision whether the MAC address shall be *locally administered* or *globally unique*. At least some manufacturers use this to distinguish fixed location and mobile access point models (namely Apple, see *Functionality and Data Flows of Location Services/WiFi Access Points* above).
- Manufacturers determine the features of the software that controls the hardware device. This includes the decision whether MAC address randomization shall be supported and what strategy shall be used to change *locally administered* MAC addresses. While currently used MAC address randomization[48] focuses on probe requests by smartphones, a similar mechanism could be used as mitigation measure if it is provided by manufacturers (see below).
- By setting a default value, providing a user interface dialog, and through instruction manuals, manufacturers influence the value of SSIDs. Since one of the possible mitigation measures is that mobile access point opt-out of being used by location services, manufacturers affect the overall processing.

Access Point Operators

The operator of the access point is the smartphone user in case of tethering or usually the owner or driver in the case of vehicle-based WiFi access points. Operators can decide when they enable the access point. They usually also have the possibility to set the SSID of the access point. The authors lack experience to judge how easy the access to this functionality is in vehicle-based systems, for example in LTE/WiFi modems that plug into cigarette lighters and basically lack a user interface.

[48] https://www.airsassociation.org/airs-articles/item/19456-mac-randomization-a-massive-failure-that-leaves-iphones-android-mobes-open-to-tracking (last visited on 15/01/2019).

Through adding the string "*_nomap*" to the end of the chosen SSID, access point operators can proclaim their wish to opt-out of supporting in location services.

7.2 Location Service Clients

Smartphone Operating System Provider

Smartphone operating system providers, i.e., Google for Android and Apple for iOS, usually determine the selection of location services. This is done by the decisions to bundle a given client software that works with a specific server with the operating system. It is further influenced by the decision of whether providing an interface for third party providers of alternative location services.

Both Google and Apple bundle/integrate their own client software that works exclusively with their own servers in the operating system. In contrast to Apple, Google provides an interface that permits third parties to provide client software for alternative location services (see above).

Location Service Client Provider

Providers of location service client software can take only limited influence on the processing since most is determined by the application programmers interface (API) provided by the server. The relevant decisions are thus restricted to the following:

Which visible WiFi access points are filtered out and thus excluded from further processing, in particular from transfer of its data to the server. This includes the honoring of opt-out conventions in the SSID. It could involve additional filter criteria (see mitigation measures below). Since these clients run on smartphones, the capabilities of filtering may be limited by the available processing power (battery) and storage.

Client software also determines which mix of location sources the service uses and whether users can select this. For example, the Android location service supports a *device only* mode that uses only satellite positioning and avoids communications with any server.

Client software may also support the APIs of multitude of servers and leave users a choice of which to use.

Client Operator/User of the Location Service

The operator of the client is the user of the smartphone and the person who actually uses the resulting position from the location service.

Non-expert users have hardly any possibilities to influence processing. It is mostly limited to turning the WiFi-based location service on or off. This can happen through turning the whole location service on or off, or selecting a mode that uses only satellite positioning without reporting WiFi identifiers to the server.

Expert users, where supported by the smartphone operating system (i.e., only on Android), can select both location service client and server. In this way, they have the possibility of choosing a particularly privacy-preserving service. This requires considerable technical skills and effort, however.

Users also have to provide **consent** as a basis for using the location service. This is important since they also continuously report their own location to the server[49]. If servers create sufficient transparency, this consent is informed. For example, users need to be aware whether interaction with the server is anonymous or whether it requires a username or unique identifier. Whether this consent can be considered free is a subject of debate. When users really need a location service, but they lack choice because only one service is possible with a given device, then they may consent to any conditions that are imposed by the monopolistic server.

7.3 Location Service Servers

The following assumes that the provider of the server software is also its operator. Therefore the server is seen here as a single party.

Through its API, the operator determines the data that is mandatorily and optionally sent to the server. This includes decisions on whether the minimal necessary data set can be sent or whether the service requires data that are not necessary for the trilateration of a position. For example, BSSIDs/MAC addresses are necessary while SSIDs are not. It also determines whether the identifiers are transmitted in their original form or only after being substituted by a pseudonym with a one-way-function (i.e., hashed). It also decides whether the service can be used anonymously or requires a username or otherwise unique identifier from clients.

The server further determines whether and how it filters received access points before storing them in its WiFi location database. Note that even if a client already filters access points (e.g., by dropping those that opt out), additional filtering may be useful where certain client versions fail to filter correctly or where filtering requires resources that are not available on clients (see mitigation measures below).

The server further determines whether it only allows clients to use the trilateration service or whether additional parties are allowed to query the WiFi location database. In the latter case, it may be possible to query the data stored on individual networks based on a BSSID[50]. Evidently, the possibility to download the complete database is equivalent to permitting queries. Some location servers avoid individual queries for privacy reasons. For example, Mozilla's FAQ[51] contains:

> ***Can I download the entire raw database?***
>
> *No. While we try to make the service as open as possible, the underlying data contains personally identifiable information from both the users uploading data to us and from the owners of WiFi devices. We cannot publicly share this data without consent from those users.*

[49] Note that this is not the main focus of this paper, however. This paper analyses tracking of (mobile) access points, not tracking of users of location services.
[50] This is for example supported by WiGLE, see https://api.wigle.net/swagger#/Network_search_and_information_tools/detail (last visited on 16/01/2019).
[51] https://wiki.mozilla.org/CloudServices/Location/FAQ#Can_I_download_the_entire_raw_database.3F (last visited 22/2/2019)

According to our privacy policy we can and do publicize the aggregated data set of cell locations at http://location.services.mozilla.com/downloads

Servers further provide transparency about their processing towards location service users to enable informed consent. They further manage consent as a prerequisite for service access. Servers should also provide transparency to access point operators whose personal data they process.

7.4 Third Parties with Access to WiFi Location Database

If servers support individual queries or the download of their WiFi location database, arbitrary third parties can access the potentially personal data.

8 Data Protection Risks

Figure 3 shows a situation that illustrates data protection risks of location services in the presence of mobile WiFi access points. The server of the location service is shown at the top. On the middle layer below are two users who run location service clients. One is a person with his phone's location service enabled; the second is a person driving a car and using a smartphone to navigate. Predominantly, these location service clients collect the identifiers of fixed WiFi access points that are not shown in the figure. They also collect identifiers of mobile access points, one of which is shown in the in the bottom layer of the figure by a car icon.

This car is equipped with a WiFi access point but doesn't knowingly participate in a location service. This means, the situation doesn't require the driver to use a smartphone for navigation or that a location service client is present in the car.[52] The driver has not been asked to consent to any processing of her personal data and is highly likely totally unaware that her access point location data is processed, by whom, and for what purposes. The situation would be very similar with a pedestrian using her smartphone as a personal hotspot but this is not shown in the figure.

The car is shown twice in two distinct points in time to visualize its movement. From the car's perspective, the location service users in the middle layer of the figure are bystanders, i.e., they happen to be in a location close to the car.

The figure depicts the risk that if there is a sufficiently dense network of bystanders, the location of the mobile access point can be continuously tracked. At nearly every point in time, at least one bystander's location service client sends the car's WiFi identifiers and location to the server where it is potentially stored with a timestamp in the WiFi access point location database. Considering the popularity of using smartphones for navigation, it is very likely that--except in remote areas--almost complete movement profiles can be collected in this fashion. In the case where WiFi identifiers remain constant over the life time of a vehicle, i.e., act as secondary vehicle identifiers,

[52] But even if the driver would have location services deployed and enabled this would not be relevant for the legal evaluation under GDPR. As being object of a processing (WiFi-Hotspot location) is essentially different from processing data and at best the terms and conditions of the deployed location service may include a permission to process the driver's visible access points it cannot constitute consent for the benefit of other location service providers.

long term movement profiles can be compiled. The risk for the affected persons increases further when the location server is operated under a legislation that offers lower levels of protection for individuals than the GDPR.

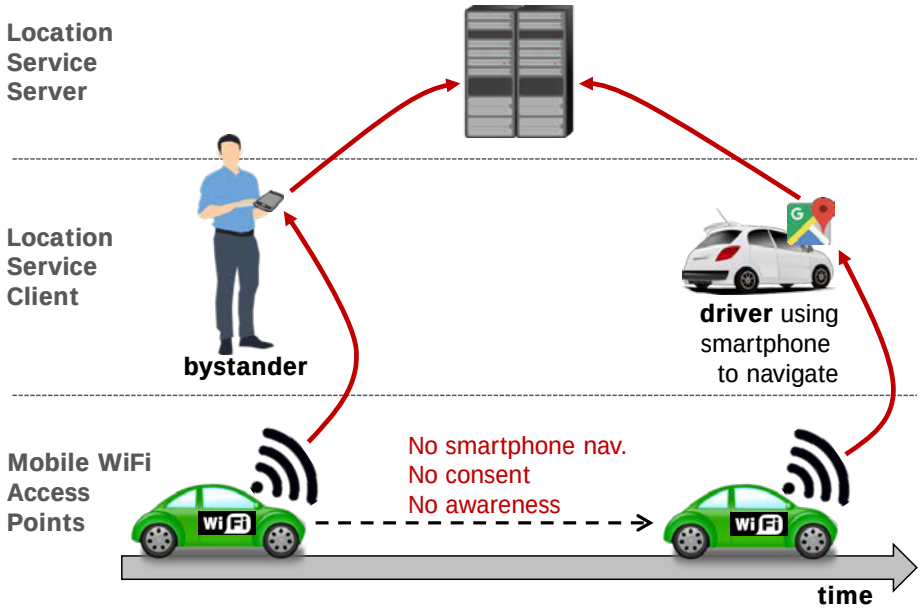


Figure 3: Tracking of vehicles via bystanders.

In data protection, location has long been identified as a sensitive type of data. This has two reasons:

- Location has a high potential of identifying persons. This becomes evident when considering that knowing the location where a person spends the night (the residence) and where a person is located during working hours (the work place) usually uniquely identifies the person.
- Location has a high potential to link to other kinds of information. Time and location may reveal an employer, sportive activities and hobbies, stores a person shops at, events a person participates in, etc. This may well also include special kinds of personal data as those related to health (a visit at a specific clinic), religion (presence in a place of worship), political conviction (participating at a reunion or demonstration), or criminal conviction (spending the night in prison). Linking can also be based on co-location and reveal relationships with other persons. For example co-location during the night may be highly sensitive and a joint movement pattern of two persons typically indicates a strong relationship.

For these reasons, the data protection risk of location services tracking mobile WiFi access points must be considered high. This tracking is likely to take place today, systematically, with a dense network of collection points, and across Europe.

While the tracking of mobile access points is highly critical, also location changes of fixed access points may pose risks. This is in particular the case when personally owned access points are moved to a new residence. Since BSSIDs are assigned by manufacturers and cannot be changed by

the owners of access points, location services can reveal the new residence address, often unknown to their owner. In certain cases[53], this can have even severe impact on the data subjects.

9 Assessment of the Risk

This section assesses how high the described risk is. For this purpose, the nine criteria[54] listed by the Article 29 Data Protection Working Party to assess whether processing is "likely to result in a high risk" are applied. The following discusses the matching criteria.

Systematic monitoring (criterion 3)
Location services represent a systematic monitoring of a large percentage of the territory world-wide.

Sensitive data or data of a highly personal nature (criterion 4)
This criterion explicitly mentioned location data whose collection questions the freedom of movement. In the case of vehicle-based WiFi access points, knowing that one's location is tracked limits the freedom of choosing this means of transportation.

Data processed on a large scale (criterion 5)
This criterion applies since the number of data subjects is a significant percentage of all persons world-wide who operate mobile access points, location service clients have a relatively high frequency of assessing locations, both data acquisition and storage seems to be unlimited in duration, and the geographic extent is basically unlimited.

Data concerning vulnerable data subjects (criterion 7)
Since also children own smartphones and may operate personal hotspots while they move, they are also affected by the tracking. Likewise children may be logically linked to vehicle access points, e.g. to a car commuting locations specific for a particular child (home, school, sport).

In addition to the criteria discussed above, one may reason that the use of WiFi access points in vehicles is a new technical solution that is now starting to be used at large scale in our society.

The lack of awareness of being tracked on part of operators of mobile access points, the lack of consent, the fact that today, the difficult to use opt-out solution is not honored by all location services, and the inability of access point operators to exercise their right as data subjects further aggravates the risk.

For the given reasons, the risk must be considered high.

---

[53] For example, when a data subject moves to interrupt stalking or participates in a witness protection program.
[54] Article 29 Data Protection Working Party, 17/EN, WP 248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (last visited 23/01/2019), pages 9-11.

This assessment seems to be supported by the Article 29 Data Protection Working Group. In in particular, in their opinion on the draft of the ePrivacy Regulation[55] they state on page 11: "Recital 25 further unhelpfully notes that some of the WiFi-tracking functionalities do not entail high privacy risks, while others – such as tracking individuals over time – do. While the Working Party appreciates the recognition that the latter has high privacy risks, it is not useful to already decide upfront that certain other functionalities do not...."

10 Legal Considerations

This section discusses first the question of whether the data collected by location services on mobile access points actually constitutes personal data. It then considers the possible legal ground of processing and derives limitations on processing.

10.1 Are Identifiers of WiFi Access Points Personal Data?

Location service clients collect the BSSID/MAC and SSID of access points together with location information and a time stamp. Optionally they exclude SSIDs from further processing.

There has been ample and international discussion on whether this data constitutes personal data in various legislations[56]. While there have been arguments against[57], the data protection authorities of the Netherlands and France confirmed in the context of the Google Street View scandal (based on the then applicable national implementations of the Data Protection Directive) that this data constitutes personal data[58, 59]. When considering mobile access points, as represented by personal hotspots of smartphones or vehicle-based access points, the arguments that the data is indeed personal are even stronger as the tracking of location allows the derivation of additional information. Tracking of devices based on WiFi or Bluetooth has been intensively discussed as part of the considerations on the draft of Art. 8(2)(b) of the Commissions Draft on the ePrivacy-regulation and it had been clear throughout the legislative process that WiFi identification data

[55] Article 29 Data Protection Working Party, WP247, 4 April 2017, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), https://ec.europa.eu/newsroom/document.cfm?doc_id=44103 (last visited 08/03/2019).

[56] See overview of findings in the context of Google Street including the United Kingdom, Canada, Hong Kong, The Netherlands, France Australia and New Zealand at p. 706 et seq.: Mark Burdon, Alissa McKillop, The Google Street View Wi-Fi Scandal and its Repercussions for Privacy Regulation, Monash University Law Review Vol. 39 No. 3, 2013, https://www.monash.edu/__data/assets/pdf_file/0011/141230/vol-39-3-burdon-and-mckillop.pdf (last visited on 16/01/2019).

[57] Mark Watts, James Brunger, Kate Shires, Do European data protection laws apply to the collection of WiFi network data for use in geolocation look-up services?, International Data Privacy Law, Volume 1, Issue 3, 1 August 2011, pages 149-160, https://doi.org/10.1093/idpl/ipr013 pdf (last visited on 16/01/2019).

[58] Final Findings: Dutch Data Protection Authority Investigation into the Collection of WiFi Data by Google Using Street View Cars' (Report, 7 December 2010), p. 29 et seq., https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_pb_20110811_google_final_findings.pdf (last visited on 16/01/2019).

[59] CNIL, decision n° 2011-035, 17 March 2011, https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000023733987 (last visited on 16/01/2019).

constitutes personal data with a special need for mitigation measures such as immediate anonymization in particular when linked to location data.

The opinion by the Article 29 Data Protection Working Party on C-ITS[60] is also interesting for all mobile Access Points since it addresses the question whether data qualify as personal in a very similar setting. The opinion focuses on C-ITS's Cooperative Awareness Messages (CAMs) that contain location data together with a frequently changing pseudonymous vehicle-specific identifier contained in certificates. The opinion confirms that this data must be considered personal data. It states in section 4.2 on page 6 that:

> "The C-ITS Working Group has correctly identified that data transmitted via C-ITS is personal data, since it relates to identified or identifiable data subjects. The data subjects can be identified in various ways. First, by the certificates they are provided by the PKI, since those certificates will be unique by design, in order to disambiguate the vehicle in which they are installed. Second, by the location data themselves, since the power of identification of location data is well known[61]: just a few points in a path are enough to single out an individual in a population with a high degree of precision, taking into account the mostly regular patterns of people's mobility."

The data collected about vehicles by location services and during war driving is very similar; it is again a location plus vehicle-specific identifiers, namely those of the mobile WiFi access point. The arguments given by the Article 29 Data Protection Working Party thus apply also to the question at hand. A major difference is that the WiFi identifiers, unlike identifiers in C-ITS, fail to change over their lifetime and can be therefore be considered to be persistent secondary vehicle identifiers[62]. This significantly increases the risk of identification of the person and thus further reinforces the argument that this indeed constitutes personal data.

We therefore come to the conclusion that Identifiers of WiFi access points constitute personal data.

10.2 Legal Grounds and Limitations of the Processing of Access Point Data

According to the GDPR, the processing of personal data requires a valid legal ground[63]. While the present discussion falls short of a comprehensive legal analysis, it identifies some limitations. These are consequences of the technical inability to ask for consent and the only legal basis remaining being that of legitimate interest pursued by the controller.

---

[60] Article 29 Data Protection Working Party, WP252, 4 October 2017, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), httphttps://ec.europa.eu/newsroom/just/document.cfm?doc_id=47888 (last visited 16/01/2019).

[61] Article 29 Data Protection Working Party, WP216, Opinion 05/2014 on Anonymisation Techniques, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (last visited 25/01/2019).

[62] Markus Ullmann, Tobias Franz, Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier – Analysis, and Measurements, in Proc. VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, France, July 23 to 27, 2017, pages 32-37.

[63] Art. 6 GDPR.

Location services have two possible data subjects: The user of the location service client (called bystander in Figure 3) and the operator of (mobile) access points. In accordance with scope of this report (see section1) only the latter data subject is considered.

Controllers: The entities involved in the data collection are thus the user of the location service client and the operator of the server. The present discussion refrains from going into the merit of their roles as controllers, joint controllers, or processors. This could only be answered if the precise contractual relationship between the parties was specified. For simplicity, the following denotes all parties that are involved in the data collection and thus determine the purposes and means as well as the "what" and "when" of the processing simply as *controller*.

Independently of who the controller actually is, the choice of legal basis is restricted by the technical fact that no communications channel exists between the parties collecting the data and the data subject (i.e. the operator of the mobile access point). In particular, this eliminates the possibility of requesting consent by all data subjects operating a WiFi access point (Art. 6(1)(a) GDPR). Similarly, the technical situation also renders the stipulation of a contract with the data subject impossible (Art. 6(1)(b) GDPR). Also no legal obligation to collect the data exists (Art. 6(1)(c) GDPR), the processing is not necessary to protect the vital interests of the data subject (Art. 6(1)(d) GDPR), and the controller usually is not an official authority acting in the public interest (Art. 6(1)(e) GDPR). The use of the metadata of WiFi access points for the purpose of providing location services can also not be considered compatible with the initial purpose of negotiating WiFi connections (Art. 6(4) GDPR). Finally, as location data of access points constitutes communication metadata in the sense of the ePrivacy Regulation's drafts, a legal ground for processing such data may be included in the planned regulation. This is currently difficult to foresee[64], however. This exclusion of alternatives leaves legitimate interests pursued by the controller or by a third party as only remaining possible legal basis (Art. 6(1)(f) GDPR). Such legitimate interests are valid unless they are overridden by the interests or fundamental rights and freedoms of the data subject (Art. 6(1)(f) GDPR). The following considerations weigh the interests of the controller versus those of the data subjects who operate access points.

Interest of the controller: Users of location service clients have an interest to improve existing positioning through the use of WiFi access point data; server operators have an interest to provide such a service and to fill and update their respective databases. The ubiquitous use of location services demonstrates its demand on the side of users. And supplementing satellite- and cell-based location services with WiFi may contribute to accuracy and speed of positioning, as well as potentially reduce overall battery consumption. Considering that determining the location is also possible based solely on satellites and cell-based trilateration, it must be recognized that positioning based on WiFi access points has only a supplementary much rather than essential role.

[64] In the different draft versions Art. 6(2) of the ePrivacy Regulation foresaw the processing of communications metadata for specific listed purposes or based on consent. So far the permissions discussed in the course of the legislative process would likely not account for the processing for the purpose of providing location services.

While the acquisition of WiFi access point data is a prerequisite for the functioning of a WiFi based location service, the necessity of access point data has to be considered in a more diversified manner:

- Knowledge of the location of **fixed** access points is the basis for the trilateration of users' positions.
- Excluding a small percentage of fixed access points from processing (for example those signalling the wish to opt out) affects the operations of the location service only in areas where the access point density is very low. Since access point data are used to improve the estimated location relative to that available solely from satellite navigation, excluding some access points cannot disrupt operations of location estimation altogether.
- Knowledge of the location of **mobile** access points fails to contribute anything to the operations of the service. In other words, it is unnecessary for the main purpose of providing a location service (see section 4). Hence, it already lacks a legitimate interest of the controller to process information on mobile access points.

Interests and fundamental rights and freedoms of the data subject: The data collection of location services affects above all operators of mobile access points. In particular, location services can potentially perform a systematic large-scale tracking and the construction of long-term movement profiles of individuals. It is well known that location data can provide critical insight into the life of individuals and that complete movement profiles are particularly sensitive[65,66,67,68]. This is due to the fact that simple combination with maps can give insight into the activities and interest of persons. This can include special categories of data (Art. 9 GDPR). For example, regular presence in a health care facility can inform about the health of a person, visits of a place of worship about religious beliefs, and participation at a demonstration about political opinions. Similarly, the place where a person spends the night may inform about potentially intimate relation to other persons. Location tracking thus affects particularly sensitive areas of the life.

The risk of being tracked can exert a chilling effect on persons that restrict their free choices of life. For example, a person may refrain from participating in a political demonstration out of fear of discrimination. This directly affects freedoms guaranteed by the Charter of Fundamental Rights, in particular Articles 7 and 8.

---

[65] Hui Zang, Jean Bolot, Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study, MobiCom 2011, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.651.44&rep=rep1&type=pdf (last visited 22/2/2019).
[66] Rinku Dewri et al., Inferring Trip Destinations from Driving Habits Data, WPES 2013, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.397.4204&rep=rep1&type=pdf (last visited 22/2/2019).
[67] Xianyi Gao et al., Elastic Pathing: Your Speed is Enough to Track You, UbiComp 2014, http://www.winlab.rutgers.edu/~janne/elasticpathing-ubicomp14.pdf (last visited 22/2/2019).
[68] Article 29 Data Protection Working Party, WP216, Opinion 05/2014 on Anonymisation Techniques, see footnote 61 above.

In the course of the balancing of the interests, available protective technical and organisational measures can be considered. Highly effective measures may reduce the risks for data subjects and therefore benefit controllers' side. For compliance it is necessary that data controllers implement appropriate technical and organisational measures ensuring that, by default, only the data necessary for a specific purpose is processed (Art. 25(2) GDPR). Where design and architecture of the processing could allow for an opt-in, this should be integrated in the design. Given the ample availability of public WiFi networks that are likely to opt in, it seems possible to restrict processing of location services to only those access points. Public and private organisations offering such services, as well as natural persons, could register to express their willingness to opt-in. In the current setup, data subjects lack means to effectively express their choice of their willingness to have their data processed.

According to Art. 21 GDPR, when processing is based on Art. 6(1)(f) GDPR, controllers are obliged to support the data subjects' right to object[69]. Such objection requires the possibility for data subjects to communicate their wish to object to controllers. In location services[70], the only technically possible means to convey a message to the controller is through the SSID. In particular, data subjects can indicate their wish to opt-out in the SSID or hide the SSID. A possibility to communicate the particular situation that is the basis for objection is not technically available. This poses the question, whether in absence of other technical possibilities, the controller must consider such an opt-out indication by the operators of access points as objections according to Art. 21 GDPR.

Considerations on the required balancing test: The use of Art. 6(1)(f) GDPR as a legal ground "requires a balancing of the legitimate interests of the controller, or any third parties to whom the data are disclosed, against the interests or fundamental rights of the data subject."[71] The following makes some considerations for such a balancing test for three different cases: (i) mobile access points, (ii) access points that express the wish to opt out, and (iii) fixed access points that refrain from expressing a wish to opt out.

(i) Mobile access points fail to contribute to the main purpose of location services and therefore, there can't be a legitimate interest by the controller to process them. In addition, the tracking of the location of mobile access points can significantly impact the freedoms of their operators (e.g., through chilling effects) and in some cases permit to derive sensitive data (see above) or track

[69] "Under Article 21(1) the data subject can object to processing (including profiling), on grounds relating to his or her particular situation. Controllers are specifically required to provide for this right in all cases where processing is based on Article 6(1) (e) or (f).", cited from page 18, section 4 of Article 29 Data Protection Working Party, WP251rev.01, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826 (last visited 19/02/2019).

[70] As defined in sections 5 and 6 above.

[71] Cited from Executive Summary, 2nd paragraph, page 3, in Article 29 Data Protection Working Party, WP217, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (last visited 19/02/2019).

children. For this reason, in the balancing test, the data subjects' interests and fundamental rights prevail over the interests of controllers. In absence of a legal basis, information on mobile access points must not be processed.

(ii) Since the exclusion of few access points only slightly degrades the accuracy of the estimated location and in no case leads to a complete interruption of location estimation (see above), it is difficult to reason that the processing of access points that express the wish to opt out are indeed necessary for the main purpose. Since controllers who base their processing on Art. 6(1)(f) GDPR are obliged to support the data subjects right to object, their only feasible option to comply with this is to consider any given opt-out indication[72] as an objection. In this case, Art. 21(1) GDPR states that "The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims." Since the data subjects lack the technical possibility to communicate their specific situation that is the basis for their objection, controllers are also unable to reason about compelling legitimate grounds that override the objection. While on one hand, the purpose of processing can also be reached when excluding the objected data, there is a significant risk that the specific situation of the data subject who opts out indeed prevails. Given the missing necessity to process such data at all and the further lack of a procedure for duly considering a data subjects' grounds for an objection, controllers must exclude access points that signal the wish to opt out from processing.

(iii) Finally, considering the ubiquitous use of location services by a reasonable percentage of the population and for a wide range of usages, the processing may seem to be beneficial for a broad number of users of location based services. The processing of data of fixed access points is also necessary for the main purpose of location services (see section 4). In the prototypical case, operators of fixed access points may be affected by the processing to different extends. Where access points are operated by organizations the intensity may be considered less severe. In the case where natural persons operate fixed access points, the collected data (even if the SSID is not collected) may reveal relevant information on the data subjects e.g. where data subjects change the access point location due to moving their home address or the device is available only when data subjects are home and thereby revealing personal habits. Location data and movement profiles reveal interests and allow conclusions about social relations. Overall, without proof of additional specific safeguards effectively mitigating the risks for data subjects of being tracked by location service providers, in our opinion, the interests and rights and freedoms of data subjects override the interest of controllers who provide WiFi-based location services.

In our understanding, there is no legal ground to process information on WiFi access points for the purpose of obtaining one's location. Given the broad use and demand of WiFi based location services, we point to potential mitigation measures in the following section.

[72] An opt-out indication can take the form of including a specific string in the SSID or to hide the SSID.

11 Possible Mitigation Measures

The following describes possible mitigation measures that can reduce the described risk. They are ordered along the components of location services that are shown in Figure 1. The enumeration of measures is not necessarily exhaustive. We do not intend to imply that the use of these measures is sufficient to comply with the requirements of the GDPR.

11.1 WiFi Access Points

Possibility of Access Points to Opt-In

This measure aims at providing the possibility to access point operators to explicitly opt in. This can be achieved in two ways: (i) By indicating the wish to opt-in in the SSID or (ii) by indicating opt-in to *each location service server or* a third party. They are discussed in the sequel.

(i) *Indication in the SSID*:
In the same way as opt-out is supported today through adding a string to the SSID an opt-in may be accomplished. For example, the string "_OptIn" could be added at the end of the SSID. The SSID is well suited for this purpose since it is actually chosen by the operator of the access point, i.e. the party making the opt-in decision. Obviously, it is necessary to create a general consensus of which string is actually used.

The **pros** of this option are its simplicity; the **cons** is that users of the WiFi network need to newly log in their devices after an opt-in is either newly given or revoked.

(ii) *Indication to each location service server or a third party:*
Since WiFi itself fails to offer suitable possibilities of communications beyond the SSID, a side channel could be established over which operators of access points can indicate their intention to opt-in to participate in location services to each location service server or a third party. For example, the servers or the third party could provide a web server that permits access point operators to newly opt-in or to revoke a previously given opt-in.

This option would have to find answers to a multitude of challenges. Among them are the question, which third parties would operate the necessary infrastructure and services, whether they partition the territory such that only one third party is responsible for a given area, and how they can verify that the person who communicates an opt-in is indeed the legitimate operator of the claimed access point.

Marking Access Points as Mobile and Opting Out

While an explicit opt-in of access points is highly preferable from a data protection point of view, should that not be feasible, the fall back to an opt-out solution is thinkable and may also be a blueprint for non-European jurisdictions with lesser requirements. The corresponding mitigation measure aims at communicating to location service clients that the access point is unsuited to participate in location services. The effectiveness of this measure depends on the willingness of location service clients to honor this opt out.

There seem to be two variants of how the wish to opt out can be communicated to location service clients: (i) By indication in the SSID and (ii) by indication in the BSSID/MAC address. They are discussed in the sequel.

(i) *Indication in the SSID*:
Several location services foresee that access points can indicate their wish to opt out by adding the string "*_nomap*" at the end of their SSID. This can be supported by **manufacturers** by setting a default values[73] for SSIDs ending in this string, by a user interface that recommends users to add this string at the end of their choice of SSIDs, and by user manuals and instructions that inform users about the importance of opt-out and how to achieve it. **Other parties** can use different means of creating awareness among users about the risks of not opting out.

This option is only **effective** for location services that honor this opt-out indication.

The **pros** of this option are its simplicity and the possibility that users can apply it even in absence of support from manufacturers, at least as long as there is a user interface through which the SSID can be set.
The **cons** include that the indication makes the SSIDs considerably longer, and that unaware users are likely to drop the opt-out when setting their own SSID.

(ii) *Indication in the BSSID/MAC address*:
It seems that some access point manufacturers (at least Apple) use *globally unique* and *locally administered* addresses in the MAC to distinguish between fixed location and mobile access points, respectively (see *Functionality and Data Flows of Location Services/WiFi Access Points* above). In particular, device models suited as fixed access points use *globally unique* MAC addresses, while device models suited for mobile deployment use *locally administered* MAC addresses. Since mobile access points are useless for trilateration, location services could use this MAC-based indication to filter out mobile access points. Such exclusion from further processing is preferably already performed already on clients, before transferring the data to the server.

This option is only **effective** if the manufacturer of the mobile access point uses this distinction mechanism and protects only from location services that honor this opt-out indication. The authors have not found any information of a current location service using this mechanism.

The **pros** of this option are its simplicity and likely low cost of implementation, both for access point manufacturers and location services.
The **cons** are the possibly significant effort to get all relevant manufacturers of mobile

[73] This would comply with the principle of data protection by default and should be the preset for devices targeted to the European market, see Art. 25(2) GDPR.

access points and all location services across the board on board. Preliminary experiments with smartphones give the impression that personal hotspots already use this mechanism. This leaves the diverse field of manufacturers of vehicle based WiFi access points, however.

Randomization of BSSIDs/MAC Addresses in Mobile Access Points

Privacy issues of WiFi-enabled smartphones have received ample attention. As a result, later versions of smartphone operating systems use randomized WiFi MAC addresses for probe requests at least in some situations (e.g., during sleep mode)[74] [75]. While this randomization is used on WiFi clients during network discovery, a similar mechanism could be used by WiFi access points. In particular, preliminary experiments indicate that connecting devices are unaffected by the change of BSSID/MAC addresses of an access points, as long as the SSID and access credentials remain invariant. A change of BSSID/MAC address is likely only possible when no device is connected. Mobile access points can be expected to shut down and restart frequently, however. In vehicles, such a measure would avoid that MAC addresses become secondary vehicle identifiers[76]. In other words, this measure fails to prevent to compile a movement profile of a single trip but will render it more difficult (but likely not impossible) to link across multiple trips.

This measure is only **effective** for location services that refrain from processing SSIDs of access points.

The **pros** of this measure include that it offers some effectiveness even for location services that fail to implement the other mentioned measures.

The **cons** of this measure are the probably high cost of implementation and that it fails to protect against location services that process the SSID. For this reason, it is questionable whether its cost is justified by the possible benefit.

11.2 Location Service Clients

Filtering of WiFi Access Points

In this measure, location service clients use filters that either limit access point to the ones who opted in or exclude mobile access points and those opting out from further processing.

In an opt-in approach, there are two different criteria for how to recognize access points to include:

---

[74] Mathy Vanhoef et al., Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms, 2016, pages 413-424, 10.1145/2897845.2897883. https://papers.mathyvanhoef.com/asiaccs2016.pdf (last visited on 17/01/2019).

[75] Jeremy Martin et al., A Study of MAC Address Randomization in Mobile Devices and When it Fails. Proceedings on Privacy Enhancing Technologies, 2017, 10.1515/popets-2017-0054. https://arxiv.org/pdf/1703.02874.pdf (last visited 17/01/2019).

[76] Note that this fails to prevent that invariant SSIDs can be used as secondary vehicle identifiers.

(i) *Opt-In indicated in SSID:*
Access points whose SSID contains the string that indicates opt-in (e.g., "_OptIn") can be further processed.

(ii) *Querying the server or third parties that manage opt-in declarations:*
To determine whether a visible access point shall be further processed, the location service client would have to identify the server and/or third parties relevant for the area of operation and query the status of each access point. For efficiency and possibly even for data protection, it may be preferable for location service clients to regularly download lists of opting-in access points much rather than querying individual access points at the third party service.

In an opt-out approach, there are three different criteria for how to recognize access points to exclude:

(i) *Opt-Out indicated in SSID:*
In this option, location service clients determine whether the access point's SSID contains the string "*_nomap*" and if so excludes it from processing. Networks with a hidden SSID should also be considered to opt out.

(ii) *Access Point marked as Mobile in BSSID/MAC Address:*
In this option, location service clients determine whether the *locally administered* bit is set in the access point's BSSID/MAC Address and if so exclude it from processing.

(iii) *Access Point's unmarked MAC Occurs in Database of MACs of Mobile Devices:*
In this option, location service clients have access to knowledge of how different manufacturers assign MAC addresses to different models of devices. It uses then uses this knowledge to determine whether the access point at hand is mobile and if so excludes it from processing.

Martin, Rye and Beverly have studied the systematics of how MAC addresses are assigned and shown mechanisms to predict device models[77]. A similar approach could be taken. In case the necessary processing and storage are excessive for a location service client running on a smartphone, this option is only suited for use on servers.

Substituting WiFi Identifiers by Pseudonyms[78]

It seems that currently, some location service providers store digests of WiFi identifiers[79]. Here, the more general concept of substituting identifiers by pseudonyms is discussed with special focus[80] on BSSIDs/MAC addresses.

---

[77] Jeremy Martin et al., Decomposition of MAC address structure for granular device inference, ACSAC, 2016, https://www.cmand.org/furiousmac/furiousMAC.pdf (last visited 17/01/2019).

[78] Note that Art. 4 No. 5 GDPR provides a legal definition of "pseudonymisation" that is not fulfilled by all technical procedures that substitute identifiers by other identifiers (pseudonyms).

If supported by the server's API, location service clients could send pseudonyms of BSSIDs/MAC addresses to the server. For example, instead of sending the BSSID/MAC address, a digest of the BSSID/MAC address could be sent. The algorithm to generate pseudonyms for a BSSID/MAC address obviously would have to be the same across all clients and remain unchanged over time in order for the server to find locations for these access points in its database. This also implies that the algorithm must be documented in the API description of the server and thus cannot be kept a secret.

With a known algorithm for generating pseudonyms, it remains unclear against what undesirable use or linking a pseudonym of the BSSID/MAC address could protect. Also, the effectiveness of such a measure would be low since the length of a BSSID/MAC address is only 6 bytes and the first 3 thereof are predictable. The construction of rainbow tables to reconstruct the original BSSIDs/MAC addresses from the pseudonyms would therefore be feasible.

Use of pseudonyms for SSIDs may protect against cases where names of persons or similar identifying information are contained. Substituting the identifiers by pseudonyms offers an inferior protection compared to exclusion from processing, however (see *Data Minimization* below).

Data Minimization

According to this measure, location service clients should transmit only the minimum necessary personal data to the server. Most prominently, this excludes the transmission of **SSIDs**[81] to the server since they are irrelevant for the main purpose of location services stated above. Whether any data beyond a recurring identifier for the access point and its signal strength is really used in the trilateration processing of location servers is a question of further research. Location servers would have to justify in what way additional data such as channel, frequency, or security settings are relevant for the purpose.

Transparency for WiFi Access Point Operators

With this measure, providers of client software create transparency about the processing also to operators of WiFi access point. This goes beyond the transparency for users of the client that is obviously also necessary but falls out of scope of this report. Due to technical limitations, a clear, easy to reach and understand documentation of what access point data is processed in what way on the provider's web site is likely the best possible approach. Given the international scope of the data collection all adequate means should be taken to make the information available and understandable including the use of illustrating graphics and multi-language versions of the explaining texts.

---

[79] For example, Radiocells.org uses an MD5 hash of the SSID, see https://radiocells.org/default/wiki/wifi-format (last visited on 25/01/2019).

[80] The focus lies on BSSIDs/MAC addresses since the processing of SSIDs is not necessary for trilateration of locations.

[81] Note that transmission of SSIDs also renders the possible efforts of BSSID/MAC address randomization by access points mute.

GDPR Certification
With this measure, providers of client software create additional transparency about their level of data protection towards both, operators of access points and actual users.

11.3 Location Service Servers

Transparency for WiFi Access Point Operators
This measure is organizational and creates transparency about the processing towards the operators of (mobile) WiFi Access Points. Since technically, the request of consent and provision of data subject rights[82] is likely impossible, creating at least transparency is of utmost importance. Transparency includes a clear statement of the purposes. In case that these purposes go beyond the minimum as states in the section on purposes above, a justification why additional or wider purposes are in fact necessary. Further, transparency demands a clear statement of what data about access points is processed and stored and how this data is necessary to fulfill the stated purposes.

Data Minimization
Considering that data of operators of WiFi access point is used without consent, it is hard to justify processing more data than the minimum necessary for the main purpose. Data minimization affects in particular the definition of the API, the storage in the access point location database, access to the data by any third parties, or use for purposes different from those stated.

Among the critical point of this measure are the avoidance of acquisition (implemented in the API) and storage (implemented in the database) of SSIDs. SSIDs may contain additional personal data such as names of persons and they enable linking of mobile access point locations even if BSSIDs/MAC addresses are changed. SSIDs cannot contribute to trilateration since the network identified by the SSID may have multiple access points (with distinct BSSIDs/MAC addresses) in different locations.

Further, data shall be deleted[83] as soon as it is no longer needed for the purpose. This applies in particular to mobile access points that are unable to contribute to trilateration and may have entered the database possibly in earlier versions of the system before fully effective filters were in place.

Substitution of WiFi Identifiers by Pseudonyms
One aspect of data minimization is substituting WiFi identifiers by pseudonyms. This was described above for clients. It was reasoned there, that the generation of pseudonyms for BSSIDs/MAC

[82] For example, operators of access points have the right to know what data is stored about them or to request deletion of their data. These rights can likely not be granted due to a lack of mechanism to verify that the requesters are indeed the legitimate operators of that access point. In absence of such a mechanism, requests about stored data corresponds to individual queries that should be avoided due to data protection considerations; requests for deletion could come from anybody and could impede the provided service.
[83] It may be that in order to avoid storing the location of mobile access points that are not recognizable as such by any of the discussed indicators, the storage of a salted digest of the BSSID/MAC address is anyhow necessary.

addresses fails to offer protection and that its application to SSIDs, while offering certain protection, is yet inferior to excluding SSIDs from processing altogether.

Filtering of WiFi Access Points

The measure of filtering out mobile access points and access points that wish to opt out was already described above for location service clients. This measure also has to be implemented by the server since it cannot be certain that the client filtered correctly and since filtering options that require more resources are possible on a server but might be overly onerous for the client.

Preventing Use for Different Purposes including Access by Third Parties

This family of measures prevents that the personal data collected for a precise and explicitly stated purpose, namely the trilateration of locations, is used for other purposes. It excludes use for undeclared purposes both, by the server itself and by third parties. For this reason, individual queries of access point specific data and the possibility of downloading complete access point location databases have to be avoided. The importance of this measure becomes more evident when considering that a 100% effective filter to exclude mobile access points may be difficult to implement.

Selecting a Processing and Storage Location in Europe

This organizational measure avoids transfer of personal data on European data subjects to countries with a potentially lesser protection standard than that provided by the GDPR.

Publication of a Data Protection Impact Assessment

Since the processing necessary for location services likely to result in a high risk (see *Assessment of the Risk* above), the GDPR requires the controller to conduct a data protection impact assessment[84]. The publication of such an impact assessment can create further transparency for operators of mobile access points.

GDPR Certification

With this measure, operators of servers create transparency about their level of data protection towards both operators of access points and users of the location service.

Measures for Location Service Users (who run clients)

While the focus of this report is on risks for the operators of mobile WiFi access point, for completeness, additional measures important for users who operate location service clients are briefly mentioned. They include transparency and consent management. It is highly desirable that location service users remain fully anonymous[85]. This ensures that the linking of individual locations of users is prevented. This implies the avoidance of any kind of username or API key. Should authorization be necessary, a technology such as anonymous credentials[86] could be used to protect users.

---

[84] Art. 35 GDPR.
[85] Pseudonymity is not sufficient here.
[86] https://abc4trust.eu/

11.4 Situation Summary

Two main strategies of mitigation exist, one implementing an opt-in/consent, the other an opt-out/objection. The former has only been sketched and requires further work to be better understood; the latter approach is technically clearer.

In an **opt-in strategy**, a new communication channel between operators of access points (i.e., data subjects) and a service that manages opt-in/consent is established. The mentioned service can either be operated by each location service or by some third party/parties that act as single point of access across multiple location services. A single point of access is preferable particularly in the case where a data subject has reasons to revoke a previously given consent and where the effort of revocation should not be excessive.

In this strategy, the location service client needs to obtain information about opting-in access points from the opt-in management service(s). The protection of the data subjects is then based on filtering out all access points without opt-in from being sent to the location service server.

Implementation of this mitigation strategy requires answers to the following open questions:

- How many services to manage opt-in/consent shall there be and who implements and operates them?
- If opt-in management services cater to multiple location services, what is the technical standard for exchanging information with location service clients?
- Is there an acceptable verification procedure to make sure that the parties issuing an opt-in or revocation thereof are actually the legitimate operators of the concerned access points?

A migration from the current status quo to a mitigation solution based on this opt-in strategy requires finding answers to the above questions, setting up the necessary infrastructure for the opt-in management services, mobilizing a sufficient number of fixed access point operators to opt-in, roll out opt-in capable location service clients to all location service uses, and then switch from the current location service client behavior to opt-in.

In an **opt-out strategy**, no additional infrastructure components/services are necessary. It relies on:

- Operators of fixed access points being able to indicate their intention to opt-out/object through the inclusion of a standardized string in the SSID.
- Producers of mobile access points indicating an opt-out/objection in the MAC address of the device.
- Producers of location service client software to honor the two opt-out intentions stated above.
- Operators of location service servers to refrain from supporting individual queries and generally implementing adequate safeguards.

A migration from the current status quo to a mitigation solution based on this opt-out strategy requires the action of a multitude of stakeholders. The most critical ones are the producers of location service client[87] software, in particular the producers of Android, iOS, and possibly Firefox Mobile that together cover the majority of the market. In addition, a large number of producers of mobile access points need to indicate opt-out/objection in their products. The transition from the status quo to a mitigated solution is then gradual with the diffusion of compliant access point products on the market. In some cases, aware data subjects may be able to opt out manually through indicating opt-out in the SSID.

As nevertheless a legal ground for such processing will be missing, legislative measures may be necessary. If such considerations should be taken up e.g. as part of the further development of the ePrivacy Directive, such a legal ground must provide sufficient protection. This can be accomplished by following one of the aforementioned approaches for opt-in or – less favorable – for opt-out clearly specifying the minimum of required safeguards.

[87] And in addition, producers of war driving clients.

12 Recommendations

In the following, we propose initial recommendations on activities to address the combined risks faced by operators of mobile access points. As illustrated above, this requires actions by a multitude of parties including manufacturers of access points and client software, as well as operators of location servers.

A Clear and Undisputed Set of Requirements

The availability of a clear and undisputed set of technical and possibly organizational requirements for different components of location services would significantly ease the adoption of the necessary mitigation measures by all involved parties. For many players, this would save substantial effort and cost of interpreting the GDPR (and future ePrivacy Regulation) and thus lower the hurdle to implement good data protection.

Awareness on the Part of All Involved Parties

The success of implementing sufficient mitigation measures for the described risks directly depends on the awareness of the major involved parties. Since the number of such parties is limited, a direct or indirect engagement could help to trigger the necessary actions. The following examples shall illustrate this:

- Only a limited number of car manufacturers and telecommunications service providers who provide vehicle-based WiFi access points exist. They could directly or indirectly be engaged to become aware of the described risks and receive guidance of how to avoid them. An indirect engagement could address the relevant industry associations, conferences, or be bundled with initiatives such as the C-ITS platform.
- An indirect engagement may also be possible via standardization bodies. IEEE that provides the EUI-48 specification that is used in BSSIDs/MAC addresses may be able to recommend setting the *locally administered* bit for mobile access points.
- The landscape of after-market manufacturers of vehicle head units may be more diverse and thus more difficult to engage. Considering that a significant number of these head units run Android, an indirect engagement through the Android project could be beneficial.
- The market of location services has two clear leaders, Google and Apple. A relatively small investment in an engagement on the issue could thus yield a respectively large effect.
- Among the alternative location service providers, Mozilla states that data protection is one of two goals of their service. Engaging them may find open doors and create a champion that other services can follow.

Assistance with Data Protection Impact Assessment and Certification

Due to the assumption, that the processing is likely to result in a high risk to the rights and freedoms of natural persons, controllers are obliged to carry out a Data Protection Impact Assessment pursuant to Art. 35 GDPR. Pursuant of Art. 36(1), controllers shall consult their supervisory authority prior to processing where the data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Policy action that provides assistance to key players to conduct data protection impact assessments or to certify their software or service under the GDPR may further help to roll out the necessary risk mitigation measures.

Necessity of Legislative Regulation of Specific Processing Situations

We emphasize the recently published statement of the EDPB on an ePrivacy regulation[88] to call on the lawmakers to intensify their efforts towards the adoption of the new ePrivacy Regulation that replaces the current Directive. This is necessary as soon as possible to protect the privacy of end-users in every relevant context and prevent distortions of competition by providing controllers with legal requirements for specific processing situations such as the one described in this report.

[88] Statement 3/2019 on an ePrivacy regulation, adopted on 13 March 2019, https://edpb.europa.eu/our-work-tools/our-documents/other/statement-32019-eprivacy-regulation_en.