WiFi tracking

Research internship – Final report

Gerdriaan Mulder <gmulder@science.ru.nl>
Radboud University, Nijmegen

January 11, 2019

This research internship was supervised by dr. Jaap-Henk Hoepman.

1 Introduction

Protecting privacy while on-the-go can be difficult. Modern devices, such as smartphones, are typically not designed with privacy in mind. Recently, a report revealed[32] that an idle Android phone sends about 40 requests per hour to Google, of which 35% are location-related. In comparison, an idle iPhone sends less than one request per hour to Google on average, and roughly 4 requests per hour to Apple (1% location-related)[32, p. 14].

Smartphones have several wireless connectivity options: Bluetooth for small file transfers and wireless headphones, WiFi to connect to the internet, and Near-field Communication (NFC) to interact with RFID cards or terminals (e.g. contactless payments). These methods do not require physical contact. Consequently, the owner may never notice their smartphone made contact, at all.

Unfortunately, smartphones typically lack physical switches that (partially) disable wireless functionality, making it difficult to control that behaviour. Furthermore, these wireless capabilities make it possible for external observers to *also* collect data that is emitted autonomously by your device. One collection technique that has become more widespread in the last decade is WiFi tracking.

Retailers are interested in the behaviour of their customers, such that they can improve their sales and revenue, or simply increase their customer's satisfaction. Loyalty cards and WiFi tracking are a few methods that can achieve this goal for the retailer. Whereas a plastic loyalty card of a supermarket (e.g. Albert Heijn's "Bonuskaart"[11]) gives the consumer easy physical protection (hide the barcode), controlling a mobile device is more difficult.

Although mobile phones have a software-based switch to turn off WiFi, I have had a Huawei Windows Phone where that switch doesn't *entirely* disables off WiFi. I found out when I disabled WiFi at home, stayed at university for the day, and when I switched on WiFi again at home, suddenly 'eduroam' appeared for a short instance. Moreover, in Android smartphones, there is a feature called "WiFi scanning": "Improve location for apps and services by scanning Wi-Fi networks even when Wi-Fi is off."[32, fig. 4]. This gives an incomplete idea of 'disabling WiFi'. One solution, of course, is 'airplane mode', but this entirely shuts off any form of wireless communication, comparable to enclosing your smartphone in aluminium foil.

The main thought behind this research internship is: "Think of ways how you can use a mobile

device to protect your privacy". We try to switch the role of a smartphone from data harvester to data *collector* such that you can be informed of other parties tracking your whereabouts.

In the following sections you will find background information about several wireless interaction options and their properties. We provide privacy context to embed the problem at hand and give a short overview of the current capabilities of mobile devices (specifically smartphones). Next, we dive deeper into the world of WiFi tracking and show the state of affairs. We show issues regarding data protection and why Bluetrace got fined by the Dutch privacy authority for running such a system. Next, we explore ideas for *detection* of these trackers. Finally, we propose future work.

2 Background

We examined the state of the art of electronic article surveillance and compared it with the state of the art shown in 'The Privacy Coach'[22]. In a couple of blog posts[13], we showed three methods: acousto-magnetic (AM), radio frequency (RF), and radio frequency identification (RFID)[2].

The first method uses two metal strips that are close together and oscillate mechanically when it receives bursts of 58 kHz tones. These tags are found in clothing as anti-theft measure. The second method (RF) comprises a *resonant circuit*[1] that resonates between 1.75 MHz and 9.5 MHz. These tags are commonly found on books, along with a barcode: the barcode is for identification, the RF tag is an anti-theft measure. The third method (RFID) is comparable to RF, but it also contains an identifier. Depending on the type of RFID card, it may contain some programmable memory or even processing capabilities.

Figure 1: Examples of an AM (left) and RF tag

Examples of the latter technique are described with 24 use cases in RFID & Identity Management[28]. For example, RFID implants are used at the *Baja Beachclub* to enable personnel to check their customer's info, and the customer to pay for their drinks. Another example is the *Selexyz* bookstore that used RFID stickers to track their 38 000 books from store delivery, placement in the store, and arrival notification for interested customers.

Finally, we examined WiFi tracking in The Netherlands, specifically on train stations[15]. The Dutch Railway uses this method for crowd management and improvements on reachability. According to a news report[35], the Dutch Railway saves the hash of a MAC address for five years, and analyses indefinitely. Allegedly, the hashing function ensures that the Dutch Railway cannot see you revisited the same spot a day later. The Dutch Privacy Authority noted that hashing a MAC address is not necessarily the same as anonymization.

[1] `https://en.wikipedia.org/wiki/LC_circuit`

2.1 Privacy context

The question arises whether MAC addresses[2] can be considered as personal data. In Europe, Regulation 2016/679 (commonly known as the General Data Protection Regulation, or GDPR) gives the following definition for personal data:

> "(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, *an identification number*, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;" — Article 4[20], emphasis added.

Smartphones are typically owned and used exclusively by a single person for a longer period of time. The Article 29 Working Party's Opinion 13/2011[17] argues that "[a] smart mobile device is very intimately linked to a specific individual", and "[it] seldom happens that a person lends such a device to another person". Furthermore, it is common in The Netherlands to acquire a smartphone with a one- or two-year mobile phone subscription. We can then fairly assume that the MAC address of a smartphone corresponds to a single person for at least one year.

Breyer vs. Germany An interesting parallel can be seen in Breyer vs. the German government[3] that concerned the question whether a dynamic IP address should be seen as personal data. In short, Breyer argued that the German government unlawfully retained his visits to German federal websites through logging records containing his dynamic IP address and time of visit. The CJEU[4] was consulted for the explanation of Directive 95/46/EC[16], specifically Article 2a and Article 7f. The court concluded that, although the German government does not have the necessary information to determine the identity of a user, the German government *can* acquire this information through legal means (i.e. request the information from the ISP through a German court). Therefore, a dynamic IP address is considered personal data, even though the entity collecting this data does not have the means to directly identify a user!

This ruling could have consequences for entities that collect MAC addresses in order to provide insight in crowd movements, e.g. on train stations. If, somehow, the MAC address collecting party can easily acquire information that links a MAC address to an individual, the storage of MAC addresses may be considered unlawful (without proper purpose, consent from the data subject etc.). Considering the fact that MAC addresses are static, rather than dynamic, once a MAC address can be coupled to an individual, all previously collected "anonymous" records suddenly become personal data.

Achieving linkability? Hashing prevents *immediate* linkability from MAC addresses to individuals. However, directly hashing MAC addresses without extra information is considered unsafe[29]: recovery of a MAC address given an MD5 or SHA256 hash can be done in about 4 and 13 minutes respectively. If this form of hashing is used, it is rather trivial to acquire the original MAC address, thus potentially revealing someone's personal data.

Still, we miss the link between a MAC address and an identifiable or identified person. There is no 'central register' that maps MAC addresses to an individual (although mobile operators *could* have this information when they rent a smartphone to an individual as part of a subscription).

[2] Per-device unique identifier used in communication with a (wireless) network

[3] `ECLI:EU:C:2016:779`

[4] Court of Justice of the European Union

In that sense, we cannot simply conclude that MAC addresses are personal data. However, we do like to note that smartphones actively emit data, as we will see in the section on WiFi tracking. This data may contain additional information that could lead to identification of a natural person.

In conclusion, there is no *direct* link between a MAC address and a natural person, although we see possibilities to use additional information such that a natural person *can* be identified. In that sense, a MAC address *should* be considered personal data.

Data protection authority The Dutch data protection authority ('Autoriteit Persoonsgegevens', or *AP*) enforces the regulation on the protection of personal data (GDPR). Besides that, it aims to (amongst others) improve data protection awareness amongst governments, companies, and citizens; stimulate the usage of privacy-friendly systems and processes; guard compliance of the law by doing independent research[14]. Since January 1, 2016, the *AP* has the means to fine companies up to €20.000.000,00 or 4% of the global turnover if they are in violation of the GDPR[20, Article 83.5].

Coincidentally, while writing this paper, the *AP* has published their views on WiFi tracking[21]. They argue that applying WiFi tracking (or other digital means) for following people is only allowed under strict conditions, since the usage of such techniques nearly always means the processing of personal data. Furthermore, they confirm that simply hashing MAC addresses without extra data is a reversible process[6], which means that already stored tracking data is considered personal data!

3 WiFi tracking

Smartphones periodically emit signals when WiFi is activated[30]. These signals (*probes*) are used to find known WiFi networks. Both connected ("associated") and disconnected smartphones can be tracked[24]. In the first case, the wireless coverage of the network should be large enough such that the devices stay connected. In the second case, WiFi monitors should be placed in such a way that the devices' movement stay within range of the probes. We say that tracking is *active* when a smartphone needs to be connected to a WiFi network; it is called *passive* when this is not the case.

We will now explore Freudiger's experiments[26] in order to get an idea of the amount of WiFi signals a smartphone emits. Freudiger tested four devices from different vendors[5], and collected the number of probes sent by the smartphones. Four experiments were conducted, we will look at two specifically. In each experiment, data is collected for one hour and the experiment is repeated five times. The measurements were then averaged.

"Experiment 3" contained eight device configurations. The iPhone and two Android-based devices behaved differently in various configurations, as we can see in Figure 2. Most notable is the Samsung S3 in the configurations *ScreenOn*[6] and *KnownInProximity*[7], sending roughly 3700 and 4200 probes[26, Section 3.4] per hour on average.

"Experiment 4" observed a feature called 'MAC randomisation'. Smartphones have a static WiFi MAC address. iOS 8.1.3 contains a feature uses a randomised MAC address instead of

[5] iPhone 6, Google Nexus 5, Samsung Galaxy S3, and Blackberry Q10, with operating systems iOS 8.1.3, Android L 5.0.1, CyanogenMod 11 (based on Android KitKat 4.4.2), and BlackBerry OS 10.3.1, respectively

[6] "The device is unlocked every 5 minutes and locked again;"

[7] "One known SSID appears in proximity of mobile devices every 5 minutes for 10 seconds."

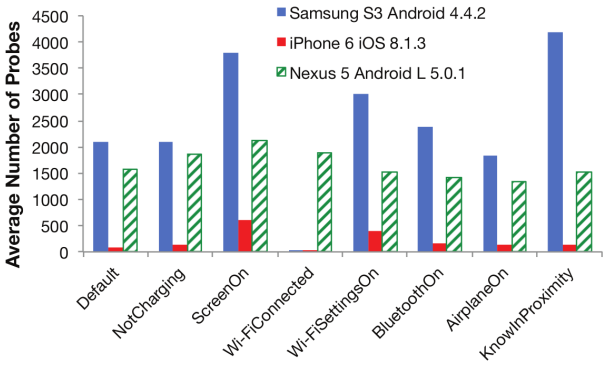

Figure 2: "Effect of device configuration on average number of probes[..]"[26, Figure 6]

the static one. Freudiger found that randomised MAC addresses can be detected: the organisationally unique identifier (*OUI*, first 3 bytes of a MAC address) is not allocated to an organisation. Moreover the sequence number in the probe is not reset when switching from/to randomised MAC addresses. It is very likely that two consecutive probes (the first one with a randomised MAC address, the second with a real MAC address) belong to the same device when the sequence numbers are also consecutive (see Figure 3). The researchers confirmed that this could be observed in their *Default* configuration.

```
324 2.922240000  2a:21:fd:74:38:aa     Broadcast  Probe Request, SN=1035 SSID=Broadcast
328 2.923264000  2a:21:fd:74:38:aa     Broadcast  Probe Request, SN=1034 SSID=Broadcast
331 2.923264000  2a:21:fd:74:38:aa     Broadcast  Probe Request, SN=1035 SSID=Broadcast
338 2.995396000  2a:21:fd:74:38:aa     Broadcast  Probe Request, SN=1039 SSID=Broadcast
538 4.896581000  Apple_74:16:d4        Broadcast  Probe Request, SN=1040 SSID=Broadcast
539 4.896585000  Apple_74:16:d4        Broadcast  Probe Request, SN=1042 SSID=Broadcast
541 4.915017000  Apple_74:16:d4        Broadcast  Probe Request, SN=1043 SSID=Broadcast
```

Figure 3: "Illustration of randomized iOS 8.1.3 MAC addresses."[26, Figure 7]

Next to MAC addresses used as identifiers, Vanhoef *et al.* showed that there are (optional) fields in WiFi probes that can be used as profiling information[34]. These fields are called *information elements* (IEs) and are defined in the IEEE 802.11 standard[19, §9.4.2.1]. Examples of such elements are *SSID* (service set identifier, commonly known as network name), *Supported Rates*, *Country*, and *Supported Channels*. Vanhoef *et al.* call a set of these information elements an "IE fingerprint"[8].

For each IE fingerprint, they formed the *anonymity set* comprising all devices that matched this fingerprint. Given the datasets they researched, a lot of devices (ranging from ±100 to ±3200 in different datasets) have a unique fingerprint (i.e. anonymity set size of 1), but extremities also exist: an anonymity set size of 700+ with 400 devices; an anonymity set size of nearly 40 000 with 20 000 devices. These extremities tend to indicate a popular brand or model that share the same fingerprint.

Smartphones typically send probes that contain their configured SSID(s)[9]. This information can be used to setup a fake access point that tricks a mobile device (using MAC randomisation) into sending an association request using their real MAC address[23]. Another trick is to visually

[8]They also noted a discrepancy between the standard and its implementation in devices: "[..]the 802.11 standard states that the IEs must be sorted[..], several devices ignore this[..]". This discrepancy opens up a "potential source of information"[34, §3.1]

[9]Additionally, WiFi access points announce their presence. This is also used by companies like Google to link an SSID to a specific location. See also (in Dutch) `https://tweakers.net/nieuws/78093/ssid_nomap.html`

identify a person carrying a smartphone, record the MAC addresses with a WiFi monitor, and follow the person for some minutes. After analysis, the MAC address that had the longest "contact length"[23, Section 5.2] most likely belongs to the target followed.

In conclusion, we have seen that WiFi tracking can occur *actively* (established connection with a WiFi network) and *passively* (by eavesdropping on WiFi channels). Even passive tracking is useful, because smartphones tend to broadcast their presence regularly. Privacy protecting mechanisms such as MAC address randomisation can be circumvented by looking at the probe sequence counter, or creating a fake access point.

3.1 Case study: Bluetrace

We will now take a closer look at a company that offers WiFi-based services. *Bluetrace* aims to "[i]mprove business results of organisations"[12]. In 2014 and 2015, the Dutch 'College Bescherming Persoonsgegevens'[10] investigated one of their services: WiFi tracking in retail. We take a look at their implementation (as far as this information is publicly available), and a couple of aspects that were lacking according to the CBP.

In 2014, the website of Bluetrace mentioned the following about WiFi tracking:

> "Visitors are counted and tracked individually by following the Wi-Fi signal of their mobile phone. The visitor remains anonymous because only the phone's MAC address is recognized. So it's nothing personal. Just an amazing opportunity to maximize efficiency, security, service and revenue. By dealing flexibly and smart with the available data about location, product, personnel and people. Gathering data for predictive analysis of costumer and crowd behavior: now available for the offline world." — retrieved from the Internet Archive[3]

According to the report[18], Bluetrace offered WiFi tracking technology that could be installed in and around retail shops. Their devices could both collect MAC addresses from inside a retail shop, as well as people passing by on the public road.

Bluetrace collects information in the passive way (this solely relies on the probes sent by the mobile device, as we have seen earlier). This information is sent to a server. Upon installation of their tracking device at a customer, the sensors' sensitivity is modified such that the system can can distinguish between a device *inside* or *outside* the customer's premises. The following raw data is collected: the *MAC address* and *signal strength* of the device, serial number of the sensor, and date and time of the measurement.

These data form the basis for further analysis. Bluetrace offers several analyses: the *number of unique devices* that passed by a sensor; the *mobility* of a device[11], and *visiting frequency*.

Bluetrace uses a hashing algorithm to obfuscate the collected MAC address. It can do this in two spots: on the sensor (data collection), or on the server (data storage/modification). The MAC address is typically stored on the server, and hashed after three weeks. Bluetrace hashes with a granularity of one day. This means that the identical MAC addresses map to the same hash on one day, but map to a different hash on another day. The default interval is 24 hours, but customers can request another interval.

Unfortunately, the exact hashing algorithm is marked as confidential in the report. *CBP* reports, however, that the used algorithm is *not* sufficient enough to speak of 'anonymised' data[18,

[10] CBP, named 'Autoriteit Persoonsgegevens' since 1 January 2016

[11] Movement of a device, e.g. whether the device is inside or outside the premises

p. 32–34]. There still exists a (reversible) relation between the hashed value and the MAC address. They argue that Bluetrace possesses the hashing algorithm, and that the chance of hash collisions is negligible. Therefore, Bluetrace still processes personal data, and should be treating it as such under the *Wbp*[12].

3.2 Detecting trackers

We searched for actual implementations of WiFi trackers and found BlipTrack (BLIP Systems) via [30] and [33]. We also found an accompanying presentation[1] that suggests BLIP Systems is the WiFi tracker supplier of the Dutch Railways. This presentation gives insight in the type of reports BlipTrack's systems can provide. We see flow analysis (i.e. a number of people and their direction, such as entering or exiting the bicycle storage), distinction between people travelling by train (passengers) and people using the train station to go to/from the city (non-passengers), and, within the passengers category, whether they arrive on, depart from or transfer in the train station.

Figure 4: WiFi and Bluetooth tracker (device left[5, p. 6], MAC addresses right[4, p. 6])

Furthermore, BlipTrack's installation guides are publicly available[8]. These manuals contain high resolution photographs that clearly show MAC addresses[5, p. 6], as well as a list of MAC addresses belonging to one WiFi/Bluetooth tracker (see Figure 4). Given the MAC address of the wired network interface (starting with `00:12:CA`), we found the *System-on-Chip* manufacturer "Mechatronic Brick Aps". They provide "Electronics, software and technology in one solution"[10]. Moreover, the organisationally unique identifier of the MAC addresses in Figure 4 reveal that the Bluetooth sensors (`00:0E:A5`) are registered BLIP Systems, but the WiFi sensors' MAC addresses (`17:0B:47` and `17:0B:48`) are not registered to any entity[7]. Besides not being registered, it's remarkable that the OUIs differ. Typically, two similar devices from a manufacturer have the same OUI. This also gives opportunities for detecting WiFi trackers (given that they broadcast their MAC address): passively listen on WiFi frequencies, filter out all MAC addresses that have a OUI registration, and you could be able to detect WiFi trackers (or iOS devices, as we've seen in section 3).

4 Future work

In [25], the authors use smartphones as passive receivers for collecting information about WiFi coverage and quality in Edinburgh. It would be interesting to adapt that concept and use it for WiFi trackers, such that independent passive WiFi monitors (for example, capable smartphones) can be used to actually 'detect WiFi trackers'.

Mechatronic's website contains downloadable firmware images and manuals[9] of their products that appear to be present in BlipTrack's hardware. This is interesting for further investigation, because this publicly available information gives very low-level insight into the systems used.

[12] 'Wet bescherming persoonsgegevens', superseded by the GDPR since 25 May 2016

5 Conclusion

We have seen that protecting privacy on-the-go can be difficult. On the one hand, smartphone operating systems regularly 'phone home'. On the other hand, WiFi monitors collect data from WiFi probes emitted by smartphones. It is difficult for smartphone owners to control this behaviour, especially when the operating system offers to disable WiFi, but keeps it activated for "location services". WiFi tracking systems collect these probes—often without properly informing smartphone owners—such that the system's owner can gain insight in the mobility of a crowd on their premises.

The collection of WiFi-related data raised the question whether that data can (partially) be seen as personal data. Although MAC addresses are unique, there is no *direct* link between a MAC address and a natural person. However, MAC addresses *should* be considered personal data. The Dutch data protection authority confirms this conclusion. Furthermore, we have seen that different smartphones leave different WiFi 'footprints', thereby exposing potential profiling information. Finally, we showed that smartphones using randomised MAC addresses can be tricked into revealing their real MAC address.

We examined the report from the Dutch 'College Bescherming Persoonsgegevens' about Bluetrace. Bluetrace's sensors could collect MAC addresses from both inside as well as outside the customer's premises. Although they used a (confidential) hashing algorithm to "anonymise" their collected data, the *CBP* concluded that, since Bluetrace knew the algorithm, they could reconstruct the original data.

Finally, we explored ideas for detecting WiFi trackers. We found a supplier of WiFi trackers and the reports they deliver to (in this case) the Dutch Railways. We also found details—such as MAC addresses of the System-On-Chip hardware—about these WiFi trackers that could be useful for future research into *detecting WiFi trackers*.

References

[1] Advances in measuring pedestrians at Dutch train stations using Bluetooth, WiFi and Infrared technology. https://d1rkab7tlqy5f1.cloudfront.net/CiTG/Over%20faculteit/Afdelingen/Transport%20%26%20Planning/Conferences/TGF15/vandenHeuvel_TGF15.pdf, via https://www.tudelft.nl/citg/over-faculteit/afdelingen/transport-planning/news-agenda/conferences-courses/tgf15/presentations/.

[2] Background reading: electronic article surveillance. https://moeilijklastig.nl/ri/blog/2017-05-25-rfid-background.html.

[3] Bluetrace. http://web.archive.org/web/20141217022546/http://bluetrace.nl/.

[4] English - WIFI Sensor Installation manual - BTTS-WF. http://blipsystems.com/wp-content/uploads/2018/04/V_Installation-manual-BTTS-WF.pdf.

[5] Indoor Sensors Installation – BLN2I-WF. http://blipsystems.com/wp-content/uploads/2018/04/V_Installation-manual-%E2%80%93-Indoor-Sensor-%E2%80%93-Blip-Node-L2i.pdf.

[6] Internet en telecom — Autoriteit Persoonsgegevens. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/

internet-en-telecom#ik-pas-bij-wifitracking-en-bluetoothtracking-hashing-toe-dan-zijn-het-toch-geen-persoonsgegevens-meer-6964.

[7] List of Organisationally Unique Identifiers (MAC address prefixes) and their registered owners, IEEE. http://standards-oui.ieee.org/oui.txt.

[8] Manuals (English) - BlipTrack. http://blipsystems.com/manuals-english/.

[9] Mechatronic Brick (downloads). http://download.mechatronicbrick.dk/.

[10] Mechatronic Brick (profile page). http://www.mechatronicbrick.dk/profile.html.

[11] Mijn bonuskaart — ah.nl. https://www.ah.nl/bonuskaart.

[12] Mission statement - Bluetrace Bluetrace. https://bluetrace.nl/en/about-us/mission-and-vision/.

[13] Research internship: privacy coach. https://moeilijklastig.nl/ri/.

[14] Toezichtkader Autoriteit Persoonsgegevens — Autoriteit Persoonsgegevens. https://www.autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/toezichtkader-autoriteit-persoonsgegevens.

[15] Tracking people at railway stations and ultrasonic concert tickets (1). https://moeilijklastig.nl/ri/blog/2018-02-01-recent-technologies.html.

[16] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *OJ*, L 281:31–50, 1995-11-23.

[17] Opinion 13/2011 on Geolocation services on smart mobile devices. 2011-05-15.

[18] Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapport_db_bluetrace.pdf, 13, 2015.

[19] Ieee standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pages 1–3534, Dec 2016.

[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). *OJ*, L 119:1–88, 2016-05-04.

[21] Bedrijven mogen mensen alleen bij hoge uitzondering met wifitracking volgen — Autoriteit Persoonsgegevens. https://autoriteitpersoonsgegevens.nl/nl/nieuws/bedrijven-mogen-mensen-alleen-bij-hoge-uitzondering-met-wifitracking-volgen, November 30, 2018.

[22] Gerben Broenink, Jaap-Henk Hoepman, Christian van't Hof, Rob Van Kranenburg, David Smits, and Tijmen Wisman. The privacy coach: Supporting customer privacy in the internet of things. *arXiv preprint arXiv:1001.4459*, 2010.

[23] Mathieu Cunche. I know your mac address: targeted tracking of individual using wi-fi. *Journal of Computer Virology and Hacking Techniques*, 10(4):219–227, Nov 2014.

[24] Yuchuan Du, Jinsong Yue, Yuxiong Ji, and Lijun Sun. Exploration of optimal wi-fi probes layout and estimation model of real-time pedestrian volume detection. *International Journal of Distributed Sensor Networks*, 13(11):1550147717741857, 2017.

[25] A. Farshad, M. K. Marina, and F. Garcia. Urban wifi characterization via mobile crowdsensing. In *2014 IEEE Network Operations and Management Symposium (NOMS)*, pages 1–9, May 2014.

[26] Julien Freudiger. How talkative is your mobile device?: An experimental study of wi-fi probe requests. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '15, pages 8:1–8:6, New York, NY, USA, 2015. ACM.

[27] Jaap-Henk Hoepman. In things we trust? towards trustability in the internet of things. *CoRR*, abs/1109.2637, 2011.

[28] Christian Cornelis Gerardus Hof. *RFID & Identity Management in Everyday Life: Striking the Balance Between Convenience, Choice and Control*. Rathenau Instituut, 2007.

[29] Matthias Marx, Ephraim Zimmer, Tobias Mueller, Maximilian Blochberger, and Hannes Federrath. Hashing of personally identifiable information is not sufficient. In Hanno Langweg, Michael Meier, Bernhard C. Witt, and Delphine Reinhardt, editors, *SICHERHEIT 2018*, pages 55–68, Bonn, 2018. Gesellschaft für Informatik e.V.

[30] A. B. M. Musa and Jakob Eriksson. Tracking unmodified smartphones using wi-fi monitors. In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*, SenSys '12, pages 281–294, New York, NY, USA, 2012. ACM.

[31] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. Rfid guardian: A battery-powered mobile device for rfid privacy management. In *PROC. 10TH AUSTRALASIAN CONF. ON INFORMATION SECURITY AND PRIVACY (ACISP 2005)*, pages 184–194. Springer-Verlag, 2005.

[32] Douglas C. Schmidt. Google data collection. Technical report, Vanderbilt University, Aug 2018.

[33] Jeroen van den Heuvel, Danique Ton, and Kim Hermansen. Advances in measuring pedestrians at dutch train stations using bluetooth, wifi and infrared technology. In Victor L. Knoop and Winnie Daamen, editors, *Traffic and Granular Flow '15*, pages 11–18, Cham, 2016. Springer International Publishing.

[34] Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo S. Cardoso, and Frank Piessens. Why mac address randomization is not enough: An analysis of wi-fi network discovery mechanisms. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '16, pages 413–424, New York, NY, USA, 2016. ACM.

[35] Daniël Verlaan. NS volgt mensen op stations met wifi-trackers — RTL Nieuws. `https://www.rtlnieuws.nl/tech/artikel/7311/ns-volgt-mensen-op-stations-met-wifi-trackers`, 2017.