Overview of real-world deployment of physical analytics systems

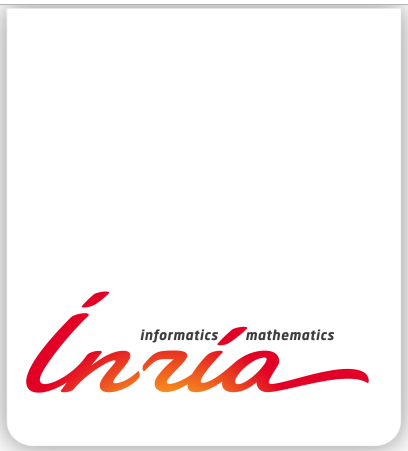
Célestin Matte, Mathieu Cunche

Overview of real-world deployment of physical analytics systems

Célestin Matte, Mathieu Cunche

RESEARCH REPORT
N° 9143
December 2017
Project-Teams Privatics

ISSN 0249-6399 ISRN INRIA/RR--9143--FR+ENG



Overview of real-world deployment of physical analytics systems

Célestin Matte, Mathieu Cunche

Project-Teams Privatics

Research Report n° 9143 — December 2017 — 14 pages

Abstract: This document studies the real-world deployment of physical analytics systems. Starting with a few real-world examples, it then discusses various aspects of such systems: privacy implication, regulation, consent, public acceptance, and engineering aspects.

Key-words: Wi-Fi, tracking, privacy

RESEARCH CENTRE
GRENOBLE – RHÔNE-ALPES

Inovallée
655 avenue de l'Europe Montbonnot
38334 Saint Ismier Cedex

Aperçu du déploiement dans le monde réel des systèmes de traçage physique

Résumé : Ce document étudies le déploiement des systèmes de traçage physique dans le monde réel. Commençant par quelques exemples réels, il discute ensuite d'aspects variés de tels systèmes: implications en terme de vie privée, consentement, acceptation par le grand public, et aspects d'ingénierie.

Mots-clés : Wi-Fi, traçage, vie privée

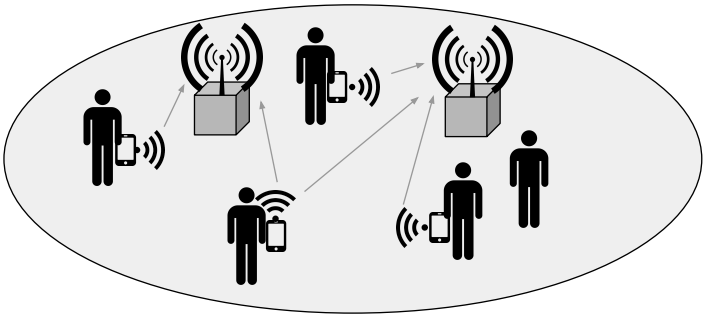


Figure 1: A Wi-Fi tracking system.

1 Introduction

The recent wide-scale spread of Wi-Fi-enabled mobile devices came with a privacy threat to their owner. In order to discover surrounding networks, these devices continuously emit signals. These signals contain a number uniquely identifying the emitting device: the MAC address. As a consequence, emitted signals may be collected by a passive attacker, which can then obtain sensitive information such as the presence of the device along time. Such a design flaw is exploited by real-world actors to perform physical tracking.

Radio-based physical tracking relies on sniffers that collect identifiers contained in messages emitted by radio-enabled devices [15]. These identifiers are used to detect users' presence and estimate their mobility. Because Wi-Fi is included in many portable devices and relatively easy to sniff, it is the main radio technology used in the physical tracking industry. Closely related, Bluetooth is another wide-spread option for device tracking.

Deploying passive sensors, one is able to collect frames of all nearby activated devices. These sensors can be cheap, as many commercial off-the-shelf Wi-Fi cards can be turned into so-called *monitor mode*, which allows them to collect frames even if they are not addressed to them[1]. Because Wi-Fi-enabled devices permanently perform active scanning, most of them can be detected by a passive tracking system (see discussion in the introduction). Figure 1 schematizes such a Wi-Fi tracking system.

Such physical analytics systems are booming in various places of the world. Due to the recent proliferation of Wi-Fi-enabled mobile devices (detailed in section 2), many companies have seen this as an opportunity to gather statistics about clients, populations or vehicles and developed systems for that matter.

We give an overview of the current deployment of Wi-Fi and Bluetooth physical analytics systems in its various forms throughout the world. We do not mean to be exhaustive, as we primarily focus on French and English-speaking resources (thus excluding many local press articles). We start by discussing the recent evolution of trackable devices in section 2. Then, we list some installations in section 3. In section 4, we discuss their actual privacy guarantees. Section 5 lists details of regulations and their applications in various countries. Section 6 talks about consent and its possible implementations. Finally, in section 7, we give evidences of the generally negative acceptance of tracking systems in public opinion.

Due to the close proximity of Bluetooth and Wi-Fi analytics systems, we group both of these technologies in this document.

[1] To be precise, the monitor mode prevents the card from dropping frames whose destination address is not either their own MAC address, a broadcast or a multicast address.

2 Evolution of the wireless landscape

First, let's study the evolution of the number of everyday-carried Wi-Fi-enabled mobile devices to justify the wide-scale privacy threat of tracking.

2.1 Number of devices

Worldwide, more than 7 billion cellular subscriptions[2] are active in 2015 [24]. Wide disparities exist, as mobile broadband subscriptions range from 86.7 for 100 inhabitants in developed countries, to 12.1 for 100 inhabitants in the lesser developed countries in 2015. Mobile cellular subscriptions keep increasing, and reach more than 100% in several parts of the world, indicating that some people are using more than one device [23].

The previously presented figure of 86.7 broadband subscriptions for 100 inhabitants in developed countries also indicates a new trend: in these countries, a huge majority of people possesses an Internet-enabled device[3]. In 2016, in France, 77% of people aged 18-75 declare possessing a smartphone [10]. As these devices integrate software necessary for internet usage (web browsing, emails, messaging...), most broadband-generation devices also integrate Wi-Fi hardware, to allow for a faster and cheaper Internet access than the cellular technologies.

Adoption of Wi-Fi-enabled mobile devices has developed rapidly in the last few years. For instance, in the U.S., the rate of adults owning a smartphone skyrocketed from 35% in 2011 to 68% in 2015 [2], reaching 77% in latest surveys [39]. Similarly, tablet computer ownership rose from 3% in 2010 to 51% in 2016. France exhibits a similar trend: smartphone ownership rate rose from 29% in 2012 to 65% in 2016 [3].

2.2 Detection possibilities

Despite their wide spread, are these devices good candidates for tracking? In this section, we will discuss the number of devices which satisfy the conditions to be *detectable*: carried by their owner, active, possessing a functioning Wi-Fi interface, and actively sending frames.

A study in the U.S. shows that 94% of smartphone owners carry their phone frequently, and 82% turn them off either rarely or never [41]. However, all of these devices are not detectable at all times: all devices do not send Wi-Fi frame periodically, or the Wi-Fi interface can be temporarily deactivated or malfunctioning. In 2017, penetration rate of mobile telephony is greater than 100% in many parts of the world [22].

Estimating how many of these devices are trackable is an unanswered question. To our knowledge, no public study of Wi-Fi activation rate on mobile devices exists. Besides, we showed that devices whose Wi-Fi switch is off can still be lead to emit Wi-Fi signals [33].

Estimating the ratio of devices over the number of people in a population is a tough question. A number of biases exist, i.e. depending on the country [24, 22], the population's distribution of ages [41], education [39], developed environment [39], income [47] or socio-professional category [22], etc [35]. Different figures have been presented regarding the number of trackable devices. In 2013, a Wi-Fi tracking company put forward the figure of 40% to 60% of a mall's visitors, depending on the location (city) [19]. In [50], authors calculate the ratio of devices over population size in a car manufacturer exhibition, using a ground-truth obtained via camera detection. Their results indicate that the targeted population is on average 1.5 times more numerous than the number of devices, this factor varying from 1.0 to 2.6. Experimental results indicate potential large differences in this factor in similar events. Performing captures in 10

[2] This encompasses all kinds of cellphones, not only (Wi-Fi-enabled) smartphones.
[3] Broadband allows a fast Internet access.

security conferences around the world in 2012-2013, Wilkinson recorded factor ranging from 0.44 to 3.75 between the number of devices and the number of conference attendees[4] [51]. A study in 2015 in Manhattan [26] using census and administrative data from several sources as ground-truth values found results within ±15% of these census data. Their estimate is even between 2 to 5% of the counts of the most reliable sources, according to them. As they do not adapt the count of Wi-Fi-enabled devices to the estimated population count, this suggests a close one-to-one correspondence between population count and Wi-Fi-enabled devices count. This result is quite surprising, considering a survey in the same city in the same year which found that only 79% of the population owned a smartphone [35]. This rate lower than 1 may be compensated by people carrying more than one device. It must be noted that this study gathers all conditions for statistics using Wi-Fi-enabled devices counting to give reliable results: number of passers-by is always great enough for results not to be affected by an important standard variation. Moreover, smartphone ownership in this city is high even among groups usually affected with a low ownership rate, such as low-income or old people [35]. According to a presentation slide for the tracking installation in the Railway museum of London (see link below), this installation reaches a 96% correlation between the number of visitors (for which they have ground truth) and the Wi-Fi-based counts, despite the fact that only 53% of visitors carry a Wi-Fi-enabled device.

Abedi et al. compared Wi-Fi and Bluetooth regarding the ability to monitor people. Their conclusion is that, due to differences in transmission range, popularity, probing rate and default configuration in popular devices, Wi-Fi is more suitable for this application. In their experiment, among around a thousand detected MAC address from both protocols, more than 90% of them are Wi-Fi addresses [1]. On a dataset of more than 6 000 addresses, Shauer et al. obtained a similar ratio of 94% in favor of Wi-Fi addresses [44].

All these numbers show that the possibility of tracking individuals on a massive scale has recently become a very real possibility, and therefore an issue.

3 Fields of application

Despite strong regulations in many countries (detailed in section 5), Wi-Fi and Bluetooth analytics installations slowly develop in many infrastructures. This section lists a few evidences of real-world analytics solutions.

Road traffic analytics:

- A Bluetooth-based vehicle tracking system in Houston provides real-time traffic information to the general public[5].
- A tracking system based on both Bluetooth and Wi-Fi is installed on Lyon's ring road [18].
- A Bluetooth-based traffic detector is installed in Maryland [52].

Retail analytics:

- In May 2017, CB Insights identified several dozens of start-ups working on location analytics for retailers [5]. See also the article by Demir et al. listing analytics companies [11].

[4] Average: 1.58; Standard deviation: 1.11

[5] `http://www.houstontranstar.org/faq/traffictech.aspx`, consulted on 2017.06.06

- In *La Défense* in Paris, a shopping mall recently installed a Wi-Fi analytics system without prior notice[6].
- In the US, a company called Nomi sold Wi-Fi analytics systems to approximately 45 clients in 2013. Some clients deployed these systems in multiple locations. According to the FTC, these different installations collected information on no less than 9 millions of individual devices between January 2013 and September 2013 [13].
- The Norwegian Data Protection Authority published a report in 2016 about tracking in public spaces, reminding concepts of consent, pseudonyms, etc. [9]. The report compares 4 tracking technologies: Wi-Fi tracking, Bluetooth tracking, beacons and Intelligent Video Analytics. The report gives two examples of Wi-Fi tracking installations in Norway:
  - at Hamar's *CC Stadion* shopping center,
  - at the Oslo airport, a Wi-Fi tracking system estimates waiting time to pass security check, using one AP before and after customs.
- A Wi-Fi and Bluetooth-based tracking system is operational in Amsterdam's airport since mid-2017[7].
- Apart from retail stores, Wi-Fi tracking is also used in other closed places. For instance, two museums in London now have permanent Wi-Fi tracking installations to get information such as the most visited rooms, or for "security concerns"[8].

Crowd analytics / population statistics:

- In the U.K., the Transport for London corporation tracked subway commuters for one month in the end of 2016 [36].
- Similarly, a wide 6-month experiment was performed in New York, using 53 APs to collect Wi-Fi information, in order to know more about population dynamics [26].
- Several Wi-Fi tracking systems are installed in various French cities: Niort since March 2017[9], Rennes since February 2017[10]. In these hybrid cases, crowd analytics is used for retail analytics, on a larger scale.
- The Chinese government made an announcement in 2011 about the installation of a tracking system in Beijing, targeting no less than 17 millions cellphones [25]. This raised international concern about the surveillance capabilities and other possible abuse of such a system [42]. We're not sure about the technology used in this case.
- In Singapore, a company is using drones to perform wardriving with the intent to create user profile to serve advertisements. In 2015, they claimed they had no less than 530 millions user profiles[11].

[6] `http://tempsreel.nouvelobs.com/rue89/rue89-nos-vies-connectees/20170711.OBS1939/vous-etes-reste-22-minutes-chez-l-opticien-jeudi-et-le-centre-commercial-le-sait.html`, consulted on 2017.07.14

[7] `https://www.schiphol.nl/en/privacy-policy/`, consulted on 2017.09.13

[8] `http://www.gizmodo.co.uk/2017/04/exclusive-heres-what-museums-learn-by-tracking-your-phone/`, consulted on 2017.09.08

[9] `http://www.lanouvellerepublique.fr/Deux-Sevres/Communes/Niort/n/Contenus/Articles/2017/03/17/Wifi-VIP-la-publicite-directe-sur-les-smartphones-3035563`, consulted on 2017.06.06

[10] `http://www.20minutes.fr/rennes/2011831-20170210-rennes-capteurs-wifi-suivre-clients-centre-ville`, consulted on 2017.08.26

[11] `https://venturebeat.com/2015/02/23/drones-over-head-in-las-valley-are-tracking-mobile-devices-locations/`, consulted on 2017.07.27

Surveillance:
Evidences exist that mobile phones tracking is performed by states-sponsored agencies to retrieve stolen phones[12], journalists [21] or war opponents[13]. The NSA[14] is suspected of performing cellphone tracking using a wide range of methods, including Wi-Fi-based tracking using pods mounted on drone to monitor data from both routers and mobile devices on a city scale (i.e., wardriving) [16, 43]. They're even suspected of using tracking for assassination by drones [43].

4 Privacy aspect in real-world installations

A general claim for these installations is that they are actually *more* privacy-preserving that other systems, such as licence plate or face recognition because of the encryption used before storing data. However, this encryption is usually weak, taking the form of the creation of a single pseudonym which can be as weak as a salt-less hashing [13]. Demir et al showed how risky this approach is. Salt-less hashing of MAC addresses can be reversed within seconds using a modern GPU, because of the small address space of used MAC addresses, mainly if the reversal attack is limited to allocated OUIs. Hashing using a salt may not be a better-suited solution, as the salt needs to be stored by the system to hash addresses on-the-fly. As a consequence, compromise of a system usually includes the compromise of the salt [11]. Kumar when further in this analysis, taking into account the OUI semantics: OUIs registered by vendors not producing mobile devices can be ignored as well [29].

Besides, data is often stored for long periods of time for debugging or analysis purposes. For instance, unlike originally planned, the Maryland installation ended up keeping perpetual online archives [52]. The Lyon installation stores identifiers for more than 1 month [18], and the one in *la Défense* for 6 months.

A 2014 analysis by Demir et al. showed how insufficient the privacy policies applied by Wi-Fi tracking companies were at that time. For many of them, they found a combination of long retention periods, data storage delegated to third-parties, weak hashing and absence of opt-out system [11].

Even more questionably, Wi-Fi tracking is performed by some public Wi-Fi providers. Some of them exploit their man-in-the-middle position to collect information of questionable interest such as age, gender, and photo on social media [28].

Despite their sensitive operations, some tracking systems eventually turn out to be poorly secured, exposing users to potential privacy breaches. Cerrudo reversed-engineered wireless sensors used worldwide for vehicle counting and found alarming vulnerabilities: lack of encryption and authentication, unencrypted and unsigned firmware updates [6].

User notifications aren't always correctly done. For instance, this was one of the topics of an administrative complaint by the FTC towards the Nomi company in 2015 [13].

Some Wi-Fi analytics systems go further into tracking by combining multiple technologies to track consumers, a technique sometimes labeled *convergence* [45]. For instance, one company goes as far as crossing at least 8 sources of information, from video camera footage to payment card data[15]. This is highly troublesome in terms of privacy, because a lot of privacy-sensitive information can be gathered from these multiple sources. Crossing them together bring even more meaningful information.

[12] `https://www.cnet.com/news/russian-police-spy-on-peoples-mobile-data-to-catch-thieves/`, consulted on 2017.07.21

[13] `https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/`, consulted on 2017.07.21

[14] National Security Agency

[15] `https://retailnext.net/en/how-it-works/`, consulted on 2017.07.16

Privacy guarantees in these systems are complicated to enforce, and weaken their usefulness for advertisers. For instance, calculating the revisit rate of customers implies that visitors' information is kept for an extended period of time using pseudonyms, at best. While pretending to anonymize collected data, the Niort system (see above) is able to calculate this revisit rate.

5 Regulation

Due to these privacy issues, Wi-Fi tracking and analytics is often limited by regulation entities.

In France, the CNIL published detailed rules that retail Wi-Fi tracking installations must respect to be authorized [8]:

- data must be deleted when the device owner leaves the shop (it can be aggregated),
- or a strong collision rate must be ensured, i.e. recorded identifiers must correspond to several devices (without precise numbers about this minimum collision rate).

Companies not respecting these rules can be fined or have their installations rejected or forbidden. For instance, the CNIL rejected in July 2015 a proposition of an installation in *la Défense* in Paris[16], on the basis that pseudonymization is not sufficient to provide anonymity. To be more precise, they noted that MAC addresses hashing with a salt does not prevent the processing manager to cross recordings with other sources of information, or to infer other information about users. Despite the fact that a counter-procedure by the company was rejected[17], an installation is present as of July 2017 (see section 3).

In Sweden, the Swedish Data Protection Authority amended a company to modify or cease a Wi-Fi tracking installation in the city center of Västerås because MAC addresses were stored in cleartext[18]. The installation was later accepted in exchange of modifications in the systems: MAC addresses are deleted after a few seconds, and information about the system is displayed on boards in the city and on the company's website[19].

In the United States, the Federal Trade Commission (FTC), while not as strict as in other countries, is also careful about the privacy aspect of tracking installations [17]. The Electronic Frontier Foundation (EFF), an international non-profit digital rights group, also reminded that it might be illegal to capture MAC addresses [20].

In the U.K., Wi-Fi tracking bins were removed due to privacy concern after an order from the City of London Corporation [48].

6 Consent in physical tracking

Consent is an important aspect for privacy protection. It basically states that users give their agreement to share information about them. As we define privacy as the ability to choose which personal information someone shares with whom, there cannot be privacy without consent.

Two approaches exist for a user to indicate whether they want to be part of a system:

[16] `https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000031159401`, consulted on 2017.07.14

[17] `http://arianeinternet.conseil-etat.fr/arianeinternet/getdoc.asp?id=209297&fonds=DCE`, consulted on 2017.07.14

[18] `http://www.datainspektionen.se/press/nyheter/2015/besoksflodena-i-vasteras-mats-for-noggrant-/`, consulted on 2017.06.07 (in Swedish)

[19] `http://www.datainspektionen.se/press/nyheter/2015/gront-ljus-for-besoksmatning-i-vasteras/`, consulted on 2017.06.07 (in Swedish)

- Opt-in: the users explicitly announce that they want to be part of the system (and are therefore not part of the system by default).
- Opt-out: the users are considered part of the system by default, and can indicate that they do not want to.

To prevent oneself from being tracked, real-world installations offer either an opt-out system, or nothing at all. For instance, we did not find any possibility to opt out of the existing vehicle tracking systems listed above. When existing, the opt-out system is sometimes poorly advertised [17]. In the Nomi-FTC case, one of the complaints was that the opt-out was global to all installations of Nomi's system, and not store-relative, and not possible inside stores. We found no evidence of existing systems using an opt-in method. When tracking is performed by Wi-Fi providers, information of the fact that users will be tracked may be hidden in the contract's details, sometimes even erroneously pretending that keeping location information is a legal requirement [28]. While this can be considered as a form of opt-in, one must remember that these terms are almost never read entirely (if at all) by users [37].

Opt-out mechanisms typically involve a webpage on which the user needs to enter their device address[20] (see Figure 2). In the Niort installation, users can opt out by scanning a QR code[21]. In *La Défense*, users have to send an email to oppose tracking. A problem with all of these systems is that it requires the user to be able to access its MAC address. While this is already a complex operation for a non-tech-savvy user, it is (almost) impossible for devices such as fitness trackers, which do not provide easy access to this piece of information. In a shopping center in Paris, it's even been reported that customers are invited to turn Wi-Fi off altogether so as not to be tracked[22]. This is also written in the privacy policies of Amsterdam's airport's system (see link above). This method is not sufficient: we showed that Android devices having the "always allow scanning" option activated will keep sending probe requests even if Wi-Fi is deactivated. Moreover, we have observed a device not proposing any way to deactivate this option [33].

One of the problems in Wi-Fi analytics is that Wi-Fi frames are not stopped by walls. A tracking system will then record information on people not entering the place (e.g. walking in nearby streets). This is problematic when entering a place is considered a form of consent (which justifies the opt-out strategy)[23].

Tracking using other technologies than Wi-Fi or Bluetooth may be even more problematic regarding the consent question. Soltani made a summary of consent and notice in various technologies [46].

Possible improvements to opt-out mechanisms are discussed in my thesis [32].

7 Public acceptance

Wi-Fi tracking systems are generally not accepted by the population. A 2014 survey by OpinionLab on 1000 customers found a rejection rate of tracking in retail stores of 80% [38]. Primary cited concerns are "data security" and "spying". Fawaz et al. found a similar result of 70% of rejection in a survey on 200 Amazon Mechanical Turk participants [12]. The latter study found that only 10% of participants accepted full gathering of their Wi-Fi broadcast information. While

[20] `https://smart-places.org/`, `http://flux-data-vision.com/optout.html` for the Niort installation, both consulted on 2017.06.06

[21] We assume this QR code redirects to the related opt-out webpage.

[22] `http://www.lefigaro.fr/secteur/high-tech/2017/08/02/32001-20170802ARTFIG00264-le-bhv-aspire-les-donnees-de-ses-clients-mais-il-est-loin-d-etre-le-seul.php`, consulted on 2017.08.04

[23] Some companies actually advertise this issue as a feature: `http://www.libelium.com/products/meshlium/smartphone-detection/`, consulted on 2017.07.27

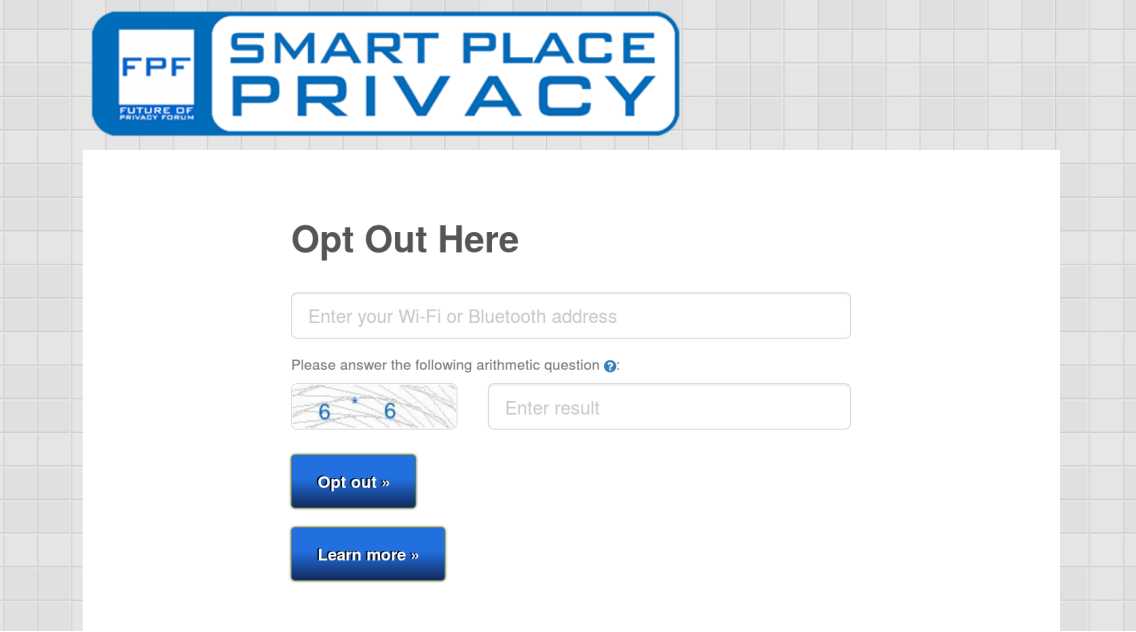


Figure 2: Screenshot of the opt-out webpage set up by the Future of Privacy Forum: `https://optout.smart-places.org/`. Users entering the address of their device opt out of Wi-Fi analytics systems deployed by most major Wi-Fi analytics companies in the US.

modifying the question to state that the store explicitly asks user consent for tracking, these numbers moved to respectively 61% and 15%, which suggest that consent plays a key role regarding user acceptance of tracking.

When the public is aware about existing Wi-Fi tracking installations, strong concern often rises from local association or political parties, as shown in the Niort case[24] or for an installation in Rennes[25]. The latter has lead to a suspension of the installation until the CNIL gives its opinion[26]. In the U.S., customers got unnerved about tracking in retail stores [7]. Politician interventions against Wi-Fi analytics lead to the redaction of a code of conduct[27] for mobile location analytics [20, 31]. The latter advocates use of an opt-out system and explicit notice.

It can be noted that common users may have a bias towards accepting systems they do not understand, or if they do not understand the extent of leaked information. Kowitz and Cranor showed how users changed their attitude when shown some information leaked by their personal device on a local network [27].

Acceptance of physical tracking is best understood when compared to the perception of other forms of tracking, notably online (web) tracking. Studies have shown that this form of tracking is widely rejected. A study found that 66% of adult Americans reject targeted advertisement, and would not allow advertisers to track them online if they had a choice. This number rises to

[24] `http://deuxsevres.eelv.fr/12/wifi-vip-un-dispositif-couteux-qui-porte-atteinte-a-la-vie-privee-des-niortais-e-s/`, consulted on 2017.06.06

[25] `http://www.ouest-france.fr/bretagne/rennes-35000/commerce-rennes-dominique-fredj-demissionne-du-carre-rennais-4860890`, consulted on 2017.06.07

[26] `http://www.20minutes.fr/rennes/2027787-20170309-rennes-commercants-reportent-mise-service-capteurs-wifi-suivant-smartphones`, consulted on 2017.07.14

[27] `https://fpf.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf`, consulted on 2017.06.08

86% when they're explained how data is collected, and to 90% if targeting is the result of their offline activities [49]. Another study found a similar rejection rate of online tracking of 68% [40]. It can be noted, however, that users' behaviour often differs from their privacy statements [4], and that they often have strong misconceptions about tracking [34].

8 Conclusion

We saw in this document various real-world examples of Wi-Fi-based tracking systems. Most of them present shortcomings in terms of privacy, when it comes to gathering user consent, presenting an easy-to-use opt-out system, or simply following regulation guidelines.

We state that all these systems should be built following the privacy-by-design principle. The latter is a core concept when it comes to building privacy-preserving systems. It basically states that systems should integrate privacy mechanisms in their core structure, and not treat it as an optional feature. Basic concepts that ubiquitous computing-related systems must integrate are clear notices, explicit user consent, adequate security and anonymity [30].

Some readers may be interested in the engineering aspect of physical tracking system. A part of Young's report on the Bluetooth-based traffic detector in Maryland [52] gives interesting insights about the problematics of a permanent deployment of such a system. The solutions to these issues chosen by this system's designers are the following. For the necessary resistance to temperature and humidity extremes, the sensors respect the NEMA TS2 standard, a standard for traffic control assemblies. To get a sufficient source of energy, each sensor is equipped with a 30 Watt solar panel. For data communication, cellular communication using a GDM modem is used. The final cost of the installation is 7 200$ per sensor, including hardware, installation, and data cost. On the whole, the life-cycle of the system is 5 years. Additionally, Grolleau published a report discussing various aspects of Lyon's ring road's system. Similarly to the previous one, sensors are powered with 70 Watt solar panels [18]. More information on this installation can be found in a presentation by Purson et al. [14].

References

[1] Naeim Abedi, Ashish Bhaskar, and Edward Chung. Bluetooth and Wi-Fi MAC address based crowd data collection and monitoring: benefits, challenges and enhancement. In *Australasian Transport Research Forum (ATRF), 36th, 2013, Brisbane, Queensland, Australia*, 2013.

[2] Monica Anderson. Technology device ownership, 2015. `http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/`, consulted on 2017.05.15, 2015.

[3] ARCEP. L'État d'internet en france 2017, 2017.

[4] Bettina Berendt, Oliver Günther, and Sarah Spiekermann. Privacy in e-commerce: stated preferences vs. actual behavior. *Communications of the ACM*, 48(4):101–106, 2005.

[5] CB Insights. The store of the future: 150+ startups transforming brick-and-mortar retail in one infographic, 2017.

[6] Cesar Cerrudo. Hacking us traffic control systems. In *DEFCON*, 2014.

[7] Stephanie Clifford and Quentin Hardy. Attention, Shoppers: Store Is Tracking Your Cell. `http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html`, 2013.

[8] CNIL. Mesure de fréquentation et analyse du comportement des consommateurs dans les magasins. http://www.cnil.fr/linstitution/actualite/article/article/mesure-de-frequentation-et-analyse-du-comportement-des-consommateurs-dans-les-magasins/, consulted on 2017.05.05, 2014.

[9] Datatilsynet. Tracking in public spaces, 2016.

[10] Deloitte. Usages mobiles. https://www2.deloitte.com/fr/fr/pages/technology-media-and-telecommunications/articles/usages-mobiles-2016.html, 2016.

[11] Levent Demir, Mathieu Cunche, and Cédric Lauradoux. Analysing the privacy policies of Wi-Fi trackers. In *Proc. of the 2014 workshop on physical analytics*, 2014.

[12] Kassem Fawaz, Kyu-Han Kim, and Kang G Shin. Privacy vs. reward in indoor location-based services. *Proceedings on Privacy Enhancing Technologies*, 2016(4):102–122, 2016.

[13] Federal Trade Commission. Complaint. https://www.ftc.gov/system/files/documents/cases/150423nomicmpt.pdf, consulted on 2017.07.14, 2015.

[14] Atec ITS France, editor. *Evaluations simultanées de différentes technologies innovantes de recueil de données trafic pour le calcul de temps de parcours en temps réel*, 2015.

[15] Julien Freudiger. How talkative is your mobile device? An experimental study of Wi-Fi probe requests. In *WiSec*, 2015.

[16] Barton Gellman and Ashkan Soltani. NSA tracking cellphone locations worldwide, Snowden documents show. *The Washington Post*, 2013.

[17] Megan Geuss. Creepy but legal phone-tracking company gets wrist slap for empty privacy promise. https://arstechnica.com/tech-policy/2015/04/creepy-but-legal-phone-tracking-company-gets-wrist-slap-for-empty-privacy-promise/, consulted on 2017.06.08, 2015.

[18] Guillaume Grolleau. La captation bluetooth au service des aménagements urbains, 2015.

[19] Quentin Hardy. Technology turns to tracking people offline. https://mobile.nytimes.com/blogs/bits/2013/03/07/technology-turns-to-tracking-people-offline/?referer, 2013.

[20] Parker Higgins and Lee Tien. Mobile tracking code of conduct falls short of protecting consumers. https://www.eff.org/deeplinks/2013/10/mobile-tracking-code-conduct-falls-short-protecting-consumers, 2013.

[21] Bunnie Huang and Edward Snowden. Against the law: Countering lawful abuses of digital surveillance, 2016.

[22] Insee. Tableaux de l'économie française, 2017.

[23] International Telecommunication Union. Ict facts and figures. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf, 2013.

[24] International Telecommunication Union. Ict facts and figures. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf, 2015.

[25] Cecilia Kang. China plans to track cellphone users, sparking human rights concerns. `http://voices.washingtonpost.com/posttech/2011/03/china_said_it_may_begin.html`, consulted on 2017., 2011.

[26] Constantine E Kontokosta and Nicholas Johnson. Urban phenology: Toward a real-time census of the city using Wi-Fi data. *Computers, Environment and Urban Systems*, 64:144–153, 2017.

[27] Braden Kowitz and Lorrie Cranor. Peripheral privacy notifications for wireless networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 90–96. ACM, 2005.

[28] Krowdthink. They know where you are - an investigation into the contracts, policies and practices of mobile and Wi-Fi service providers in relation to location tracking, 2016.

[29] Amrit Kumar. *Security and Privacy of Hash-Based Software Applications.* PhD thesis, Université Grenoble Alpes, 2016.

[30] Marc Langheinrich. Privacy by design—principles of privacy-aware ubiquitous systems. In *International conference on Ubiquitous Computing*, pages 273–291. Springer, 2001.

[31] Jennifer Martinez. Franken still unsatisfied with Euclid's privacy practices. `http://thehill.com/policy/technology/291299-franken-still-unsatisfied-with-euclids-privacy-practices`, consulted on 2017.05.17, 2013.

[32] Célestin Matte. *Wi-Fi Tracking: Fingerprinting Attacks and Counter-Measures.* Thesis, Université de Lyon, December 2017.

[33] Célestin Matte, Mathieu Cunche, and Vincent Toubiana. Does disabling Wi-Fi prevent my Android phone from sending Wi-Fi frames? Research Report RR-9089, Inria - Research Centre Grenoble – Rhône-Alpes; INSA Lyon, August 2017.

[34] William Melicher, Mahmood Sharif, Joshua Tan, Lujo Bauer, Mihai Christodorescu, and Pedro Giovanni Leon. (do not) track me sometimes: Users' contextual preferences for web tracking. *Proceedings on Privacy Enhancing Technologies*, 2016(2):135–154, 2016.

[35] New York City Department of Consumer Affairs. New york city mobile services study: Research brief, 2015.

[36] James O Malley. Here's what tfl learned from tracking your phone on the tube. `http://www.gizmodo.co.uk/2017/02/heres-what-tfl-learned-from-tracking-your-phone-on-the-tube/`, consulted on 2017., 2017.

[37] Jonathan A Obar and Anne Oeldorf-Hirsch. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *The 44th Research Conference on Communication, Information and Internet Policy 2016*, 2016.

[38] OpinionLab. New study: consumers overwhelmingly reject in-store tracking by retailers. `https://www.opinionlab.com/newsmedia/new-study-consumers-overwhelmingly-reject-in-store-tracking-by-retailers/`, consulted on 2017.06.08, 2014.

[39] Pew Research Center. Mobile fact sheet. `http://www.pewinternet.org/fact-sheet/mobile/`, consulted on 2017.05.15, 2017.

[40] Kristin Purcell, Joanna Brenner, and Lee Rainie. Search engine use 2012. *Pew Internet & American Life Project Washington*, 2012.

[41] Lee Rainie and Kathryn Zickhur. Americans' views on mobile etiquette. `http://www.pewinternet.org/2015/08/26/chapter-1-always-on-connectivity/`, 2015.

[42] Rainey Reitman. China deputizes smart phones to spy on beijing residents' real-time location. , consulted on 2017., 2011.

[43] Jeremy Scahill and Glenn Greenwald. The NSA's secret role in the U.S. assassination program. *The Intercept*, 2014.

[44] Lorenz Schauer, Martin Werner, and Philipp Marcus. Estimating crowd densities and pedestrian flows using Wi-Fi and bluetooth. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pages 171–177. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2014.

[45] Ashkan Soltani. Technological overview. `https://www.ftc.gov/system/files/documents/public_events/182251/mobiledevicetrackingseminar-slides.pdf`, consulted on 2017., 2014.

[46] Ashkan Soltani. Privacy trade-offs in retail tracking. `https://www.ftc.gov/news-events/blogs/techftc/2015/04/privacy-trade-offs-retail-tracking`, consulted on 2017.05.17, 2015.

[47] Statista. Share of adults in the united states who owned a smartphone from 2011 to 2013, by household income. `https://www.statista.com/statistics/195006/percentage-of-us-smartphone-owners-by-household-income/`, 2013.

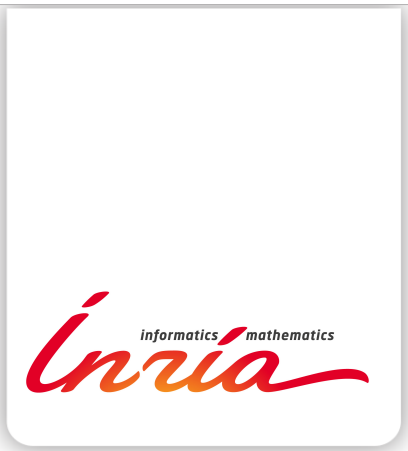
[48] The Guardian. City of london corporation wants 'spy bins' ditched. `https://www.theguardian.com/world/2013/aug/12/city-london-corporation-spy-bins`, consulted on 2017.05.16, 2013.

[49] Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. Americans reject tailored advertising and three activities that enable it. *Departmental Papers (ASC)*, 2009.

[50] Jens Weppner, Benjamin Bischke, and Paul Lukowicz. Monitoring crowd condition in public spaces by tracking mobile consumer devices with wifi interface. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, pages 1363–1371. ACM, 2016.

[51] Glenn Wilkinson. Digital terrestrial tracking: The future of surveillance. *DEFCON*, 22, 2014.

[52] Stanley Young. Bluetooth traffic detectors for use as permanently installed travel time instruments. *State Highway Administration Research Report*, 2013.



RESEARCH CENTRE
GRENOBLE – RHÔNE-ALPES

Inovallée
655 avenue de l'Europe Montbonnot
38334 Saint Ismier Cedex

Publisher
Inria
Domaine de Voluceau - Rocquencourt
BP 105 - 78153 Le Chesnay Cedex
inria.fr

ISSN 0249-6399