To appear in: C. Eckert, S. K. Katsikas and G. Pernul, eds. (2014): Trust, Privacy and Security in Digital Business: 11th International Conference. Heidelberg etc.: Springer Verlag, 168–179.

User Acceptance of Footfall Analytics with Aggregated and Anonymized Mobile Phone Data

Alfred Kobsa

Donald Bren School of Information and Computer Sciences, University of California
Irvine, CA 92617-4055, U.S.A.
kobsa@uci.edu

Monitoring and analyzing pedestrian traffic in and around retail stores has become an important tool for discovering underutilized operational and marketing opportunities of retail localities. Since a large proportion of pedestrians nowadays carry mobile phones, visual observation methods of the past could give way to cell-tower and WiFi based capture of passers-by, optionally augmented by aggregated or anonymized demographic data about them coming from their service providers. A major mobile phone operator recently announced the introduction of such a service in Germany, the U.K. and Brazil, but had to cancel its plans for Germany since the revelation caused nationwide privacy uproar.

We conducted an exploratory interview study to gauge whether and under what conditions German consumers would accept if their mobile phone providers disclosed their personal data to retail stores they walk by, in aggregated and anonymized individual form. Virtually all respondents wanted their data to remain private at an extent that goes considerably beyond the protections afforded by current privacy laws. Nearly everyone however also indicated an interest in financial incentives in return for their consent to the transfer of their data, and many of them at seemingly very reasonable terms.

Keywords: Footfall analytics, privacy, mobile phones, personal data transfer, data aggregation, data anonymization, privacy laws, compensation

1 Introduction

Monitoring and analyzing pedestrian traffic inside and outside of retail stores has become an important means for understanding and improving customer catchment, marketing effectiveness, sales staff allocation, and the influence of external factors such as weather, time and nearby events. Tracking pedestrians' movements can also help town planners, event organizers and emergency services to analyze the behavior of crowds on different days of the week and at different times or occasions, and to validate the effectiveness of urban developments.

Traditionally, footfall analytics has relied on visual observations by humans, either directly or indirectly through video [1], or people-counting cameras and sensors based on various technologies [2]. The fact that a large majority of people nowadays carry mobile phones when they leave their homes enables new and more powerful technical

solutions for foot traffic monitoring: cell-tower based positioning [e.g., 3] which is currently coarser-grained but available outdoors, and WiFi-based positioning [e.g., 4–6] which is currently finer-grained and mostly available indoors. Both technologies can deliver value beyond people counts and location information if positioning is carried out by, or in cooperation with, pedestrians' mobile network operators or WiFi access point operators. Those providers typically possess personal data about their customers, which they can convey to interested recipients together with location and time stamps, individually per pedestrian or in aggregated statistical form.

These new wireless-based technologies for footfall analytics, and specifically their potential for personal data transfer, seem however problematic from a privacy point of view. In the fall of 2012, a subsidiary of Telefónica announced its plans to introduce a "Smart Steps" footfall analytics service in Germany, the United Kingdom and Brazil, based on the location and demographical data of its mobile phone customers. The service would allow subscribers to find out, e.g., "how many customers visit an area by time, gender, and age" and to determine "the movement of crowds at any given place by hour, day, week or month" [3]. The announcement lead to a public privacy outcry in Germany [7, 8]. Telefónica thereupon pulled its plans for Germany, but introduced this service later that year in the U.K.

The applicability of data protection laws to such business models is limited, since "personal information" that is protected by these laws is narrowly defined: it denotes "any information relating to an identified or identifiable natural person" [9] or "refers to any data, including aggregations of data, which is linkable to a specific individual" [10]. Processing of data about an individual is not regulated any longer when this data is "de-identified", i.e., anonymized, pseudonymized, or compiled into statistics in such a way that it cannot be related to an individual with reasonable efforts [11–13]. Also the proposed new European General Data Protection Regulation [14] continues to maintain that "the principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable".

It is possible to anonymize both individuals' location data from cell phone towers and personal data from customer files in such a way that both can still be merged in this anonymized form [15, 16]. Individuals' consent to the disclosure of such merged anonymized data to third parties is then no longer required. In the UK, Telefónica does not even seem to allow its customers to opt out of the Smart Steps service [17]. The situation is somewhat different in Germany where the protection of location information in telecommunications networks and services is regulated both by the Federal Data Protection Act [18] and also by the German Telecommunications Act [19]. The latter mandates a separate written (i.e., non-electronic) agreement if location data are used for value added services to third parties [20], even if the data is anonymized.[1] Users also must be alerted each time when this happens.

Against this background, we conducted an exploratory interview study among mobile phone users in Germany, to gauge to what extent they would accept if their providers disclosed their customer data to retail stores they pass by, in aggregated or in individualized but anonymized form. To the best of our knowledge, this is the first such empirical study on this topic. We aimed at answering the following questions:

[1] The German Telecommunications Act is stricter in this regard than the EU Directive 2002/58/EC that it implements.

RQ1. Do mobile phone users agree with the disclosure of *aggregated* demographic data to retailers they pass by, and are there differences between individuals?
RQ2. Do mobile phone users agree with the disclosure of *anonymized* demographic data to retailers they pass by, and are there differences between individuals?
RQ3. Are there differences between types of personal information in the levels of agreement with disclosure?
RQ4. What is the relationship between users' levels of agreement with data disclosure in the case of aggregated and anonymized individual data?
RQ5. Will mobile phone users agree to the disclosure of personal data to retailers they pass by if they receive compensation from their mobile phone providers?
RQ6. If so, what discount is expected for their permission to the disclosure of personal data to retailers?
RQ7. What is the relationship between consumers' expected discount and their agreement with personal data disclosure?
RQ8. Finally, we also aimed to collect participants' rationales, and their general view on footfall analytics and personal data transfer by their mobile phone providers.

2 Study Procedures

In spring 2013, announcements of a phone study on "Customer Information Through Mobile Phones" were posted on several German classifieds websites and Internet forums, and in a print weekly listing magazine. Readers could dial a German phone number, with a callback option. A €15 Amazon gift card was offered as a reward.

20 people participated in the study (13 male, 7 female), with a wide range of professional backgrounds. Their ages ranged from 20 to 60 years, with a median of 20-30 years. Their mobile phone providers spanned nearly the full breadth of pertinent German companies. 25% used resellers (virtual mobile network operators) and prepaid plans. Reported monthly mobile phone expenses ranged from €10 to €60, with €20-€30 as the median (prepaid subscribers estimated their monthly expense).

The interviews lasted between 20 and 30 minutes and were semi-structured: they contained the fixed set of questions discussed below, and participants were also encouraged to explicate and elaborate their answers. We first explained business rationales that could prompt retail stores to desire not only a numeric count of passers-by but also some of their demographic characteristics. We pointed to targeting product offerings and advertisements to the demographics of the people who tend to pass by a certain store. The remainder of the interview was then contextualized to each interviewee's personal situation [21]: the respondent's mobile phone provider and a well-known retail store in the respondent's city (typically a Karstadt or Kaufhof department store) were used as examples.

Study participants were then asked whether they would accept if their mobile phone provider disclosed eight pieces of personal data to the retail store whenever they passed by. Those pieces of personal data were chosen based on the independent opinion of two domain experts about the maximum set of personal data available to German mobile phone providers that could be currently used for data-enriched footfall analytics. We asked about the disclosure of the following pieces of data:

1. Age group (namely "below 20", "20-30", "30-40", etc.)
2. City of residence
3. Monthly mobile phone expense ("less than €20", "€20-€30", "€30-€40", etc.)
4. Payment history ("whether or not you paid your mobile phone bills on time")
5. Gender
6. Whether or not the interviewee holds a university diploma
7. Number of children[2]
8. Private or business use of the phone (based on the customer's phone plan)

We posed these questions in two rounds. First, we asked interviewees to assume that the retailer would be informed every hour about the data of all passers-by "including yourself", but only in *aggregated statistical* form ("e.g., in the past hour, 50 passers-by were less than 20 years old, 70 between 20 and 30, etc."). In the second round, we asked participants to assume that the data of every passer-by of the past hour would be disclosed individually, but in *anonymized* form ("i.e., no name, no address, no phone number")[3]. In the third part of the interview, we asked participants to indicate what discount on their monthly phone bill they expected in return for their agreement that all their data could be given to any retailer they walk by, in anonymized and in aggregated form. Finally, we encouraged participants to tell us any other comments or suggestions that came to their minds. Throughout the interviews, we used open coding, purposeful sampling, and constant comparison to generate grounded theory [22].

3. Results

3.1 Willingness to agree with data transfer to retailer (RQ1 - RQ4)

As far as the aggregated transfer of data to retailers is concerned (RQ1), 30% felt that this is o.k. for all of the polled types of personal information, while the majority (55%) gave different responses depending on the data type. 15% of participants wanted to disclose a single piece of information only (namely age group or gender), or none at all. Participants in latter group found footfall analytics "frightening", felt "like they are being followed", and deemed this data transfer "dreadful". On average, participants were willing to disclose 5.55 of the 8 polled pieces of personal data (σ = 2.53). Females agreed less than males to the disclosure of their data (4.29 versus 6.23 of 8 polled items), but the difference is not statistically significant.

As far as the individual but anonymized transfer of data to retailers is concerned (RQ2), 10% felt that this is o.k. for all polled data (all those respondents also agreed with aggregated transfer), but 30% of the interviewees felt that this was not appropriate for any of their personal data. The rest gave different responses depending on the data type. On average, participants were willing to disclose 4.08 of the 8 polled items

[2] Information about a diploma and about children may be available to mobile phone providers if the customer has or had a student discount rate or a family/children's plan, respectively.

[3] We did not also ask subjects about the transfer of pseudonymous data (that could be linked over time) since we felt we could not easily explain its difference to anonymous data.

(σ = 3.14). Female participants' agreement with disclosure was lower than that of males (2.14 versus 5.11 out of 8 items polled). An Independent-Samples Kruskal-Wallis test confirmed that this difference is statistically significant (p=0.048). City of residence and payment history were the two pieces of information for which female and male willingness to disclose differed the most.

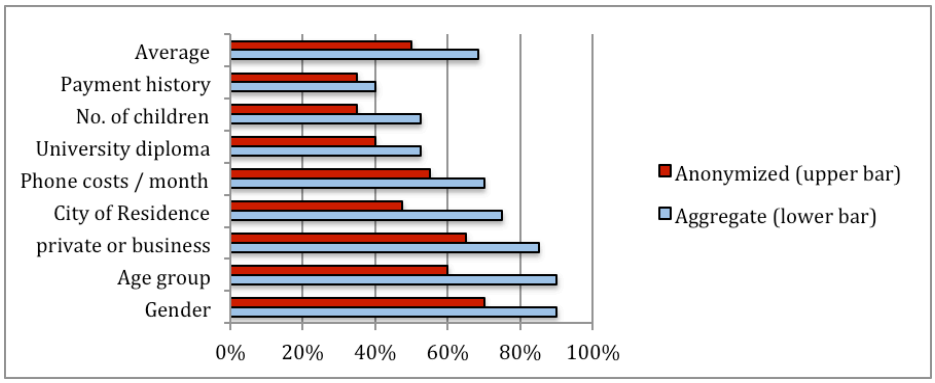

Fig. 1. Rate of consent that personal data may be disclosed to retailers passed by, by type of data and form of de-identification

Fig. 1 shows participants' average agreement rates per type of personal information requested, ordered roughly by increasing agreement (the order in which questions were posed can be gathered in Section 2). The upper bars (red) indicate the average agreement with disclosure for anonymized transfer, and the lower bars (blue) the agreement for aggregated transfer. The average agreement with disclosure clearly differs per type of personal information, in both conditions (RQ3). Agreement with disclosure is generally higher in the aggregated condition than in the anonymized individual condition (RQ4). A Generalized Estimated Equations model with data type and the form of anonymization as within-subjects factors and agreement with disclosure as binary dependent variable confirms overall statistically significant effects both for data type (Wald Chi-Square = 6.68, p=0.01) and for anonymization form (Wald Chi-Square =29.83, p<0.001). Further on RQ4, Kendall's tau shows a moderate correlation of agreement with disclosure in the two different conditions (τ=0.47, p<0.01).

3.2 Willingness to Accept Compensation for Personal Data (RQ5 - RQ7)

85% of respondents would accept a discount on their monthly phone bills in return for their agreement that the 8 items of personal data that we polled may be transferred to retailers they pass by, in aggregated or anonymized individual form (RQ5).

Fig. 2 plots the compensation requested by those 17 participants, ordered by the amount expressed as a percentage of their monthly phone bill (RQ6). Averages were chosen when participants quoted a value range, and occasionally quoted Euro amounts were put in proportion to participants' monthly phone expenses.

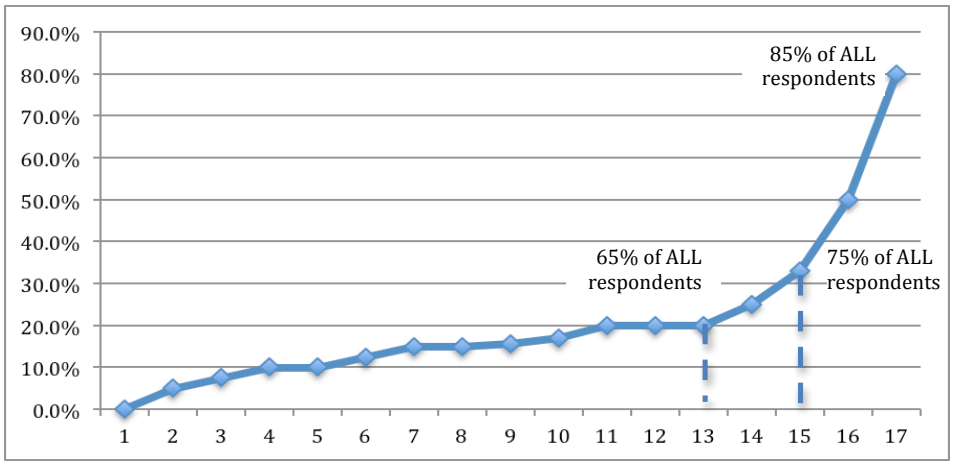

Fig. 2. Expected monthly discount for agreeing to data transfer, ordered by amount (3 respondents refused a discount)

The average requested discount is 20.9%, and the median 15.6%. As can be seen in Fig. 2, a discount of 20% would make 65% of all study participants agree to the disclosure of their data, while a discount of 33% would sway 75% of participants. With regard to RQ7, Kendall's tau shows a medium to weak negative correlation (τ=-0.35, p=0.067) between respondents' expected discount and their willingness to disclose personal data in aggregated form. The correlation between expected discount and agreement with disclosure in anonymized individual form is even weaker and not statistically significant (τ=-0.28, p=0.141).

30% of respondents indicated that they would not accept the disclosure of any of their polled data in anonymized form (see Section 3.1), and one of them not even in aggregated form. This equals roughly the proportion of "privacy fundamentalists" in Alan Westin's surveys [23]. Of those 30%, half stated that a discount on their mobile phone bill would not sway them to agree to the transfer of their personal data. The others expected discounts of 7.5%, 10% and 80%, respectively. At the opposite end, 10% of respondents had indicated that they would be o.k. with the disclosure of all of the polled data in anonymized or aggregated individual form. When asked later about a discount in compensation for their willingness, one of them did not expect any discount while the other chose 17% (pointing out this corresponds to German VAT).

3.3 Themes from grounded theory analysis (RQ8)

We performed a grounded-theory analysis of the free-form part of the interviews, to collect themes relating to participants' decisions on whether or not to agree to data disclosure to retailers they pass by. We used open coding, purposeful sampling, and constant comparison [22]. While we aimed to focus on footfall analytics, i.e. the topic of this study, participants often offered their opinions on disclosing their personal data to businesses in general. The following themes emerged:

- *Personal benefits:* Participants wanted to see some benefits in return for their data: "it depends on the benefit – where is my profit?" Personalization was mentioned as one such benefit (e.g., for advertisements or tailored offers), and financial compensation as another.
- *Fair share in profit:* A subtheme of the aforesaid was the notion of participation in profits that a company makes from selling one's personal data. As one participant put it, "if my phone company profits from selling my data, then I also want to get some part of it". None of the interviewees went further though and brought up notions like property rights in one's data [24–26] or selling/renting one's data on personal data markets [27, 28].
- *"A la carte" offers*: A few participants not only wanted a financial offer for their consent to the disclosure of *all* their data discussed in the interview (i.e., a disclosure "flat rate", as one interviewee called it), but additionally also "a la carte" offers for each individual piece of data, and even offers per third-party recipient.
- *Anonymity set:* Three participants brought up that their agreement to the disclosure of their city of residence would depend on the city size. Their motivation was to hide in a sufficiently large anonymity set. City size is unimportant when walking in one's own city since the anonymity set during an hour of observation (as we had indicated) is far smaller than the population of even the smallest city. It might make sense though when walking in a different city far away from home.
- *Perceived relevance of data for recipient:* A few participants found it "daft" that a mobile phone provider would convey to retailers whether or not a passer-by holds a university diploma, as well as the number of their children ("who would need that?"). This doubt in the relevancy of these two data types for retailers aligns well with participants' low willingness to agree to its disclosure (see Fig. 1).

4. Discussion

4.1 Expected Protection of Anonymized and Aggregated Data

Footfall analytics via smartphones augmented by customer data would provide a valuable resource to retailers that can help them in their marketing and catchment efforts with regard to passers-by. The transfer of demographic data from mobile phone providers to retailers falls largely outside the scope of existing data protection laws if the data remain anonymized or aggregated (an exception is Germany since location data is involved, see Section 1). Footfall analytics may therefore be performed without notifying the data subjects or asking for their prior consent.

Our study shows however that a substantial majority of our respondents would ordinarily disagree with the disclosure of *all* their data to retailers (namely 70% of participants if it is done in aggregated form and 90% if it is done in anonymized individual form). On average, people were only willing to give out 69% of the polled data in aggregated and 50% in anonymized form. People's disclosure proclivity also varied considerably by data type, with a low of 35% disclosure for university diploma, number of children and payment history. If data protection laws are meant to

reflect people's subjective desires for the protection of their personal data, then it would be worthwhile to consider widening the scope of protected data in future privacy legislation [e.g., in 10, 14], beyond the realm of identifiability. Unfettered protection of aggregated and anonymized individual data is probably out of discussion since this would have too many negative repercussions for innovations that are based on the analysis of anonymized data, ranging from value-added services to scientific research. It might be worthwhile though to give data subjects more protection in cases where data collectors reap financial gains when selling aggregated or anonymized individual data to third parties. As detailed in Section 3.3, several participants objected to such data usage unless there was some profit-sharing in place. The protections of privacy laws could be extended in such a way that data collectors would have to ask data subjects for permission before they could resell aggregated or anonymized individual data to third parties. Alternatively, mobile phone providers could voluntarily decide to ask customers for their permission that their demographic data may be used for footfall analytics. In the next section, we will discuss the implications of our study results on such a scenario.

4.2 Willingness to accept compensation in return for consent to data transfer

Asking mobile phone customers for permission to use their personal data for footfall analytics is likely to lead to a low rate of consent: in our study, only 30% / 10% felt that this is o.k. for all the polled types of data when done in aggregate or anonymized individual form, respectively. Our study shows that quite a few people could be swayed to agree to give out all their data if they were offered monetary compensation. The "capture rate" obviously depends on the offered amount. In our case, a 20% discount on their monthly phone bill would have swayed 65% of participants, and a 33.3% discount 75% of participants. The average requested discount was 20.9%, the median 15.6%, and the maximum 80%. Given that the median monthly phone expense was €20-€30, this roughly corresponds to average/median amounts in the 3-6 Euro range per month.

Prior studies aimed at determining the compensation people would demand for their willingness to disclose their data[4] encountered considerably higher requests:

- [33] let British university students bid on their expected compensation for their permission that precise information about their location may be collected over one month. Participants requested £32.8 on average, with a maximum bid of £300.
- [34] and [35] let European students bid on compensation for three types of location data usage: one-month academic usage, one-month commercial usage, and one-year commercial usage. The average bids were in the range of €30, €60 and €200, respectively (with a maximum bid of about €900 in the third scenario).
- [36] presented to Singaporean students websites that had different privacy characteristics, were visited in different frequencies, and offered different levels of compensation for personal data. The authors calculated that disallowing secondary

[4] A very different question is how much people would be *willing to pay* for increased privacy. The results from behavioral experiments investigating this issue lie between 3% and 10% [29] or up to 17% [30] of the purchase price, or nothing at all [31, 32].

use (like footfall analytics) represents a value of SGD 39.83-49.78 for subjects (equivalent to €24.65-€30.81 in April 2002).
- [37] let U.S. participants submit bids for disclosing personal data to all other auction participants. The average bid was US$ 57.56 for age and $74.06 for weight.
- [38] asked German participants what compensation they expected to "allow other companies to use data anonymized". Bids averaged €20 a month per data type.

A direct comparison between those results and ours are obviously difficult, due to differences in the types of disclosed data, the number of recipients (from one to an unspecified number), and frequency of payment. Overall though, our study participants made comparatively modest requests. We attribute the sizeable difference of our responses to those in earlier studies to three factors:

- We emphasized that data would be given to the retailer in aggregated or anonymized individual form. All earlier studies except [38] assumed identified transfer.
- We introduced a point of reference or anchor [39], namely the monthly phone expense. None of the previous studies seemed to have offered a calibration point (even though in some studies the maximum possible bid was capped).
- Finally, the number of possible data recipients was geographically circumscribed, namely as businesses the participants walk by. In many prior studies, the number of possible recipients was unlimited.

Overall, these results hold promise for *consensual* footfall analytics: while a large proportion of our study participants was opposed to the transfer of all their customer data by their mobile phone providers to retail stores they walk by (even in aggregated or anonymized form), 85% of them were willing to agree to such a transfer if they received a discount on their monthly phone bill. For most of those who were open to such a deal, the expected discount seems modest (resulting in low single-digit Euro amounts per month). Even when prevailing privacy legislation would allow non-consensual footfall analytics with aggregated or anonymized data, providers who want to enter this line of business might prefer using a compensation scheme to avoid a repeat of the privacy uproars from the recent past [7, 8].

4.3 Limitations of this Study

The number of participants in our exploratory interview study was relatively small. While this is quite common in this type of research, caution must be exercised in drawing overly broad conclusions from the findings. Moreover, since our study was conducted in Germany, its results cannot be immediately applied to other countries. In a Eurobarometer survey [40], 30% of German respondents agreed with the statement "disclosing personal information is not a big issue", while the agreement in the other EU member states ranged from 23% to 51%. For the statement "you don't mind disclosing personal information in return for free services online", Germans ranked median with a 26% agreement rate in a 15%-56% pan-European range. It seems prudent to take the relative differences in those agreement rates into account when generalizing the results to other European countries.

Our study also asked participants about footfall analytics through their mobile phone provider only (who would use cell-tower based and thus relatively coarse positioning), and not about finer-grained WiFi-based footfall analytics or combinations of both technologies. None of our participants addressed the precision of locational positioning though, and hence it may not make a big difference to them. This precision also has no implications on what data get communicated to a business, but only on the amount of false negatives and positives when determining whether a passer-by is within the required range to a retail store.

Moreover, our study only asked participants about the disclosure of demographic data legitimately held by their mobile phone providers in the regular course of business. At least one U.S. wireless carrier meanwhile also links location data of customers with third-party data obtained, e.g., from credit reporting agency Experian [41]. This carrier also sells aggregates of subscribers' movement patterns and not only of their locations [42]. It is unclear whether the linkage of such data can still be performed anonymously, to avoid the purview of European data protection regulation.

As [43] points out, "estimations of the monetary value of personal data are highly context dependent", and the above comparisons with bids from study participants in prior studies should therefore be looked at with caution, even when they are about the same types of personal data. Likewise, if the purpose of the personal data transfer to retailers gets changed or widened (e.g., to displaying ads in shop windows that are highly tailored to the transmitted personal data of each passer-by), then a new study should be conducted to gauge consumers' attitudes within this new or wider context.

Finally, our study polled participants' stated willingness to agree with data disclosure, and not their actual behavior. [44] and others found that participants' actual amount of personal data disclosure significantly exceeded what they had intended to disclose when they were surveyed on the same items several weeks earlier. Those and similar findings are however also disputed, and dismissed as an experimental artifact [45]. The methodological solution for the time being is to poll both stated privacy-related attitudes and intentions, as well as actual behavior [46].

5. Conclusion

We conducted the first study of mobile phone users' attitudes towards footfall analytics that involves the transfer of personal data from their mobile phone providers to retail stores that users walk by. This is likely also to be the first privacy study that compared user attitudes towards two different methods of de-identification for shared personal data: aggregation and anonymization. We found that only very few users were willing to give out all their data in anonymized individual form, and only a minority in aggregated form. The difference in respondents' average agreement with disclosure between the two forms of de-identification was statistically significant. Agreement with disclosure also varied strongly by type of personal data.

We also found however that a large majority of users would consent to footfall analytics with data transfer by the mobile phone provider (in aggregated or anonymized individual form), provided that they receive a financial compensation. The amounts requested correlated somewhat with their levels of agreement to data disclosure in aggregate form. The expected compensation is noticeably lower than the amounts that

have been reported in prior research. This may be due to the de-identified data transfer in our study, the use of an anchor point when requesting bids (namely a percentage of participants' monthly phone bill), and the narrow geographical circumscription of the set of recipients ("retail stores you walk by").

The results of our study have policy and business implications. With rare exceptions, current privacy laws do not regulate the transfer of personal data to third parties when it is carried out in aggregate or anonymized individual form. The only reason for businesses to refrain from it would be damages to their reputation, as has happened in the past. Giving data subjects their "fair share in profits", as some of our study participants put it, might be a viable way to reconcile consumer demands for wider privacy protections and business interests in leveraging and monetizing valuable but privacy-invasive technical innovations.

Acknowledgments. This study has been carried out while the author was a visiting researcher at Telekom Innovation Laboratories, Ben-Gurion University, Israel.

References

1. Nandakumar, R., Rallapalli, S., Chintalapudi, K., Padmanabhan, V.N., Qiu, L., Ganesan, A., Guha, S., Aggarwal, D., Goenka, A.: Physical Analytics: A New Frontier for (Indoor) Location Research. MSR-TR-2013-107, Microsoft Research, Banglore, India (2013).
2. Experian: People Counting Cameras, http://www.footfall.com/people-counting (2014).
3. Telefonica: Smart Steps, http://dynamicinsights.telefonica.com/smart-steps (2013).
4. Euclid: Euclid Analytics, http://euclidanalytics.com/ (2014).
5. Ruckus: Location Services, http://www.ruckussecurity.com/Location-Services.asp (2014).
6. Little, J., O'Brien, B.: A Technical Review of Cisco's Wi-Fi-Based Location Analytics, http://www.cisco.com/c/en/us/products/collateral/wireless/mobility-services-engine/white_paper_c11-728970.pdf, (2013).
7. Biermann, K.: Überwachung: Telefonica will Handy-Bewegungsdaten an Werber verkaufen, www.zeit.de/digital/datenschutz/2012-10/telefonica-smart-steps-vorratsdaten, (2012).
8. David Roman: Telefónica Goes a Little Bit "Big Brother," http://on.wsj.com/WJh6jb, 2012.
9. EU: 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 etc. (1995).
10. White House: Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy. Washington, D.C. (2012).
11. BDSB: German Federal Commissioner for Data Protection and Freedom of Information - Wiki, http://www.bfdi.bund.de/bfdi_wiki/.
12. Mascetti, S., Monreale, A., Ricci, A., Gerino, A.: Anonymity: A Comparison Between the Legal and Computer Science Perspectives. In: Gutwirth, S., Leenes, R., Hert, P. de, Poullet, Y. (eds.) European Data Protection: Coming of Age. pp. 85–115. Springer (2013).
13. ICO: Anonymisation: managing data protection risk code of practice. Information Commissioner's Office, Wilmslow, Cheshire, U.K. (2012).
14. EU: Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data etc. (2012).
15. Hall, R., Fienberg, S.E.: Privacy-Preserving Record Linkage. In: Domingo-Ferrer, J. and Magkos, E. (eds.) Privacy in Statistical Databases. pp. 269–283. Springer Berlin (2011).
16. Verykios, V.S., Christen, P.: Privacy-preserving record linkage. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 3, 321–332 (2013).

17. BBC: Telefonica hopes “big data” arm will revive fortunes, http://www.bbc.co.uk/news/technology-19882647.
18. DE-FDPA: German Federal Data Protection Act, as of 1 September 2009. (1990).
19. DE-TCA: German Telecommunications Act, as of 7 Aug. 2013. (2004).
20. Mantz, R.: Verwertung von Standortdaten und Bewegungsprofilen durch Telekommunikationsdiensteanbieter: Der Fall Telefónica/O2. Kommunikation und Recht. 7, 7–11 (2013).
21. Stage, C.W., Mattson, M.: Ethnographic interviewing as contextualized conversation. In: Clair, R.P. (ed.) Expressions of ethnography, pp. 97–105. SUNY Press, Albany, NY (2003).
22. Glaser, B.G.: Doing grounded theory : issues and discussions. Sociology Press (1998).
23. Kumaraguru, P., Cranor, L.F.: Privacy Indexes: A Survey of Westin’s Studies. Institute for Software Res. Intern'l, School of Comp. Sci, Carnegie Mellon Univ., Pittsburgh, PA (2005).
24. Westin, A.F.: Privacy and Freedom. Atheneum, New York, NY (1967).
25. Posner, R.A.: The Right of Privacy. Georgia Law Review 12, 393–422 (1977).
26. Rule, J., Hunter, L.: Towards Property Rights in Personal Data. Grant, R.A. and Bennett, C.J. (eds.) Visions of Privacy: Policy Choices for the Digital Age. Univ Toronto Pr. (1999).
27. Laudon, K.C.: Markets and privacy. Communications of the ACM. 39, 92–104 (1996).
28. Schwartz, P.M.: Property, Privacy, and Personal Data. Harv. L. Rev. 117, 2056 (2003).
29. Tsai, J.Y., Egelman, S., Cranor, L., Acquisti, A.: The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Info. Sys. Research. 22, 254–268 (2011).
30. Jentzsch, N., Preibusch, S., Harasser, A.: Study on monetising privacy. An economic model for pricing personal information. Deliverable 2012-02-27, ENISA (2012).
31. Preibusch, S., Kübler, D., Beresford, A.R.: Price versus privacy: an experiment into the competitive advantage of collecting less personal information. Electron Com Res. 13, 423–455 (2013).
32. Beresford, A.R., Kübler, D., Preibusch, S.: Unwillingness to pay for privacy: A field experiment. Economics Letters. 117, 25–27 (2012).
33. Danezis, G., Lewis, S., Anderson, R.: How Much is Location Privacy Worth? Fourth Workshop on the Economics of Information Security, Cambridge, MA (2005).
34. Cvrcek, D., Kumpost, M., Matyas, V., Danezis, G.: A study on the value of location privacy. Proc. ACM WPES, pp. 109–118. ACM, Alexandria, Virginia, USA (2006).
35. Matyas, V., Kumpost, M.: Location Privacy Pricing and Motivation. 2007 International Conference on Mobile Data Management. pp. 263 –267, Mannheim, Germany (2007).
36. Hann, I.-H., Hui, K.-L., Lee, T.S., Png, I.P.L.: Online Information Privacy: Measuring the Cost-Benefit Tradeoff. Proc. ICIS, pp. 1–10, Barcelona, Spain (2002).
37. Huberman, B.A., Adar, E., Fine, L.A.: Valuating privacy. IEEE Sec & Priv 3, 22–25, 2005.
38. Rose, J., Rehse, O., Röber, B.: The Value of our Digital Identity. Boston Cons. Gr. (2012).
39. Tversky, A., Kahneman, D.: Judgment under Uncertainty: Heuristics and Biases. Science. 185, 1124–1131 (1974).
40. EC: Attitudes on Data Protection and Electronic Identity in the European Union. Special Eurobarometer 359, European Commission, Brussels, Belgium (2011).
41. Pepitone, J.: What your wireless carrier knows about you - and what they’re selling, http://money.cnn.com/2013/12/16/technology/mobile/wireless-carrier-sell-data/, (2013).
42. Troianovski, A.: Phone Firms Sell Data on Customers. WSJ.com, http://online.wsj.com/news/articles/SB10001424127887323463704578497153556847658, (2013).
43. OECD: Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value. Report 220, OECD, Paris (2013).
44. Norberg, P.A., Horne, D.R., Horne, D.A.: The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs. 41, 100–126 (2007).
45. Rivenbark, D.: Experimentally Elicited Beliefs Explain Privacy Behavior. Univ. of Central Florida, Dept Economics, http://EconPapers.repec.org/RePEc:cfl:wpaper:2010-09 (2011).
46. Preibusch, S.: Guide to measuring privacy concern: Review of survey and observational instruments. International Journal of Human-Computer Studies. 71, 1133–1143 (2013).