What does your mobile phone leak - Unique in the crowd and predictable

Matti Lorenzen
Betreuer: Heiko Niedermayer
Seminar Future Internet SS2014
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: matti.lorenzen@tum.de

ABSTRACT

In this paper, the fact that our mobile phones tell more about us than most people think will be presented. Not only the integrated hard drive but also the archive of the provider or other parties involved with the usage of the cell phone are filled with valuable personal data. This data is highly sensitive and is already being used for personalized marketing and other purposes. After discussing which kind of data is gathered by the cell phone, focus will be laid on the accessability of this data which is often enough to identify the user uniquely in a crowd and even to predict his personality. However, this is not only to be seen as a challenge but also as an opportunity for a better interaction between human beings and machines in the future.

Keywords

Big data - Anonymity - Privacy - Uniqueness - Adaption - Predictability - Accessability - Personalization

1. INTRODUCTION

With almost seven billion global subscriptions [10], cellular services are available to more than 90% of the earth's population. With coverage around the globe, it seems impossible to determine the exact ways in which users are interacting, especially if only the raw data is reviewed. However, studies show, that data leaked by the cell phone is indeed so distinctive that the user is becoming unique in the crowd. In fact, this may be taken even further: Many phone users spend more time with their phones than with any other person; the way we use our cell phones tells a lot about us and makes it possible to predict our personalities with precision of up to 80%. If we are that predictable, will our cell phones adapt to our feelings, emotions or personal traits in the future? What consequences lie ahead if we really are that predictable and do not take precautions in order to protect our personal data? Are we actually in danger? These questions will be answered in the course of this paper.

First, the data gathered by the phone will be presented and it will be discussed who is able to access this information. After presenting the data gathered in a self-study, focus will be laid upon the phone user's personality; how it can be determined and how that information can be used. In order to conclude, the question, whether individuals are appearing uniquely in a crowd, will be addressed and possible solution to reclaiming privacy will be introduced.

2. WHAT DOES MY MOBILE PHONE LEAK?

In the following chapter, the data collected by the cell phone will be described. Furthermore, the question whom is able to access the data obtained will be answered. The amount of people that have access to this information is stunning, however, we often allow our cell phones to leak more than necessary.

2.1 What kind of data does my cell phone gather?

The data collected by the cell phone is immense[5]. In this paper, focus will be laid especially on spatio-temporal data, so location information will be discussed thoroughly. Additionally, other collected information will be discussed although it will not be relevant for the chapters regarding predictability and uniqueness as they already contain personal identifiers.

2.1.1 Location information

The cell phone's location and so, in most cases, the user's location can be detected in different ways. The probably best known possibility is tracking through GPS which is highly accurate with an error of less than five meters.

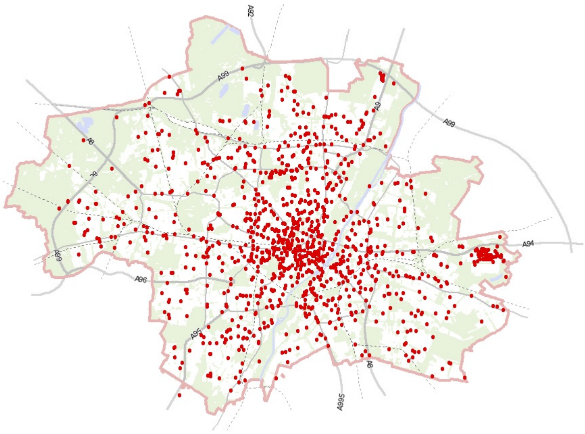

Figure 1: GSM base stations in Munich[23]

However, on most modern cell phones, the GPS signal can be deactivated by the user misleading him to the assumption that his location is untraceable. However, if the cell phone is connected to a wireless network, the location can be resolved

doi: 10.2313/NET-2014-08-1_08

out of the phone's IP address in this network which leads to an accuracy of at least 100 meters.

While the cell phone's wireless connection receiver may also be deactivated, the GSM signal cannot be deactivated without the loss of key functionalities. Normally, at least three GSM base stations are within the cell phones signal range, in cities the amount is increased by a big margin as visualized in Figure 1. There, the GSM base stations of Munich are depicted. The strength of the signal received by the cell phone from the different stations varies and so, the user's location is calculable accordingly. This happens during the stand-by mode. When calls are made, the cell phone ID is recorded at the station closest by which leads to a higher accuracy. Tracking through different types of wireless networks such as UMTS or LTE is working in a similar way.

2.1.2 Phone information

In Europe, more than 50% of the cell phones used are smartphones. The mostly used operating systems, iOS and Android (In this paper, focus will be laid upon the operating systems provided by Apple and Google as they hold a market share of over 90%.), require the user to sign up for an account at Apple or Google, respectively, where he has to specify information including his name, date of birth, email address, credit card information and phone number. Within these accounts, contacts and the calendar are administrated in order to be synchronized with other devices. Hence, the contact information of friends and family are also saved. If the user decides to connect his smartphone with a social network, increased data is added due to the synchronization of the address book or the calendar. Additionally, every telephone has a unique serial number, the so called IMEI which is used in order to identify the cell phone.

2.1.3 Camera and microphone access

The camera and microphone integrated in the cell phone may not only be used by the cell phone's owner. While requirements to access the camera and the microphone of programs like Skype on the phone are understandable, many other applications, the user would not normally have thought of, may access any of these features as well. The images taken and the audio recorded may be saved on the cell phone's internal hard drive or uploaded to online cloud services. Additionally, pictures taken or sound recorded may gather a lot of metadata such as date recorded, location recorded, camera preferences which will automatically be shared with others when we share our pictures.

2.2 Who can access these information?

The data gathered on the mobile phone can be accessed by the cell phone provider, the operating system, the applications installed on the device and other parties that may access this information without permission. The provider monitors the telephone's usage and has access to all the data collected [14] while using the UMTS or GSM network, most importantly the location respective to the time, calls and texts received and made or send, respectively. However, with the personal information the provider already obtained by signing the individual to a phone contract and the data gained by the phone usage, the provider has a deep insight into that client's profile. Profiles may include over 800 attributes including ethnicity, age, income level and frequently visited places. According to media releases [11], aggregated user profiles are likely to be sold by the provider to external enterprises due to the high value of this information regarding marketing aspects. [17] [20]

As the operating system is vital to the phone functioning correctly, complete access to all data gathered on the cell phone is required. Additionally, the operating system's manufacturer reserved its right to access the call and messaging protocol. Hence, Google [15] or Apple, respectively, know with whom their client interacted, when he interacted and how frequently he interacts. This information may be sold as well, as described before. In fact, according to a study held in 2013 [9], each unique user has an average value of about $24 to Google. Those who are not only using the search engine but also own a smartphone operated on Android provide even more data to the company and so, their value is increased.

Upon installation of a new application to his smartphone, the user is usually asked to give permissions to this certain application. The requested permissions often go beyond the features required in order to work correctly. As an example, the Deutsche Bahn's mobile app for Android 4.4 requires the user to reveal his call and messaging history. Although permissions may be revoked, the user should pay attention to the permissions granted and weigh them up to the functionality obtained.

In summer 2013, the documents revealed by former NSA[1] employee Edward Snowden caused a global surveillance scandal. According to his information, the NSA was able to gain information of almost every phone user they intended. Even politicians' phones where among the ones spied upon. Additionally to the call and messaging protocol, also their contents were accessible and the phone's microphone and camera were activated remotely [13] in order to gather intelligence. Only weeks later, it was revealed that the British GCHQ[2] was able to do exactly the same. It is not yet known how much data has been obtained by spying or who has also been able to attack the cell phone despite of all privacy laws.

2.3 Personal data example

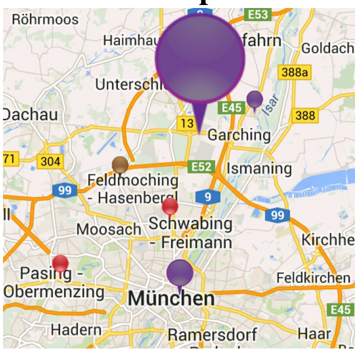

Figure 2: Locations recorded via Track My Life[24]

During the past month, I wanted to find out whether the data gathered by my cellphone is indeed precise enough to

[1] American National Security Agency
[2] British equivalent to the NSA

identify me as the user corresponding to the phone's dataset.

By using the application "Track my Life" [24] created by a student of the Technische Universität München, my location was recorded whenever I spent more than two hours at the same place. The locations most frequently tracked were my apartment, the university buildings, the gym and friends' places. In Figure 2, these top locations are visualized. The size of the points is proportional to the amount of data gathered at that location.

While over 10.000 people are studying at the university campus I am going to, only few of them live in an area of 500 meters to my home. But still, the amount of possible persons corresponding with this dataset is at about 10 people.

By adding more locations into the perspective, like the friends visited or the international group I am attending on a weekly basis, I am soon the only possible match for the mobility trace given.

This already shows that the data needed in order to define mobility traces is not as big as one might initially expect. However, in order to link a person correctly, knowledge of the person is required. This knowledge may be asymmetric as for many persons information is accessible through social networks. This topic will be discussed more thoroughly in chapter five.

Further, I reviewed my call and messaging protocol during the past month. This revealed, that interaction is made on average every three hours[3] without consideration of sleep. The contacts with whom I interacted are spread all across the country, some of them were even outside of Germany while the interaction took place. Factors as the time between interactions and the entropy of contacts can be used in order to predict traits of my personality as will be described more thoroughly in chapter three.

3. PERSONALITY PREDICTION

No matter whether a person is waiting for a train, enjoying his or her lunch break or at work - the mobile phone is always close by. In fact, many people interact more with their cell phones than with other people.

When other people spend a lot of time with us, they can usually identify our personality quite well by the way we are interacting with them. Does our interaction with our mobile phones provide enough data that our personality traits can be predicted only by review of the data gathered?

Smartphones are used for various purposes; among the most frequently used services are messaging, taking photos, accessing social networks and playing games. By analyzing the content of these messages, reviewing their activities in social networks or evaluating the frequency of games played, it would not be too hard to predict the personality quite precisely. In Figure 3, the most frequent usages as determined in a study held in the USA in 2012 are visualized. Especially the evaluation of sites liked on Facebook are accessable to everybody and a very strong indicator in order to predict personality traits. While gender and race were identified in over 90% of the cases, sensitive information like religion, sexual- or political orientation were predicted correctly in most cases as well. However, only the provider or the operator are allowed to gather these information legally and privacy concerns would arise most certainly.

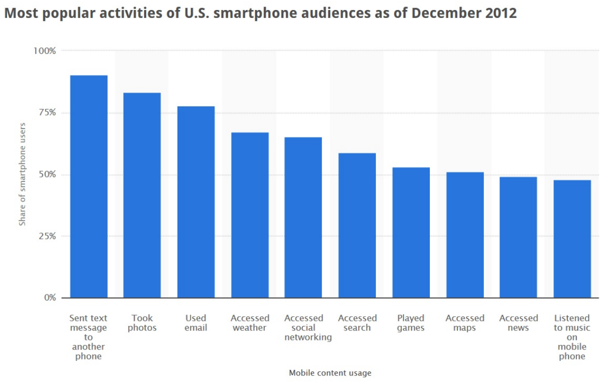

Figure 3: Mobile content usage[22]

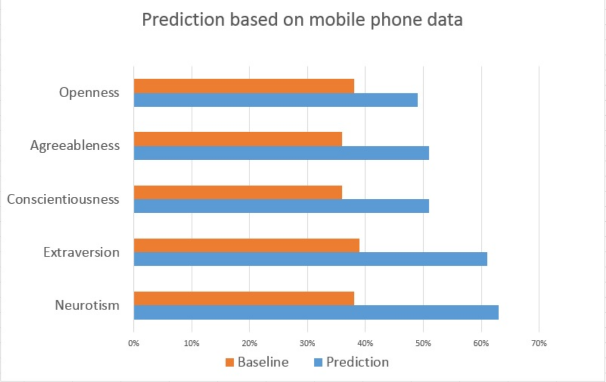

Figure 4: Big five personality traits and the comparision of prediction rates

However, researches have come up with a different approach to predict personality by reviewing information that is easily accessible and less private[19, 2].

Psychologists define five major personality traits [6], also known as the "Big Five." They are openness, agreeableness, conscientousness, extraversion and neurotism. During a study at the Massachusetts Institute of Technology [2], a prediction upon persons' personalities was made only by reviewing data gathered by cell phones. While the conclusion that a person that is frequently interacting with his mobile phone by writing messages to friends or calling them is more likely to be more open than others appears to be obvious, other connections between cell phone usage and psychology are far less trivial.

In this study, a distinction between interacting by calling somebody or by texting somebody was made, as an open, extroverted individual is more likely to use a direct form of communication than one who is not. These interactions have

[3] Calculated based on 227 interactions within the time between 03/22/14 and 02/22/14

been analyzed scientifically by reviewing data regarding the regularity and the diversity of phone usage, the individual's spatio behaviour, active behaviour and basic phone use. As useful indicators, average and variance of inter-event time for calls and/or messages, the entropy of contacts or places and the percentage of initiated texts or calls was defined.

Those indicators have been linked to the personality traits initially presented, giving the researchers the possibility to predict the person's personality. The predictions after review of this data have proven to be on average 42% better than random. This is visualized in Figure 4. When taking into account information like gender or age, the accuracy was improved even further. In order to make these predictions, only basic mobile phone data was reviewed. Hence, predictions can not only be made for persons owning a smartphone but also those who stick to more classical models.

These predictions, however, can be used for personalized marketing as the marketer can target the right kind of customer with the right kind of advertisement in order to trigger a purchase. A person that is highly agreeable is more likely to be effected by a marketing campaign than one who is not. Combined with the other information gathered by the cell phone like location, mobility trace and check-ins in social networks, it offers a great opportunity to advertise their store which is located right on the costumer's usual way in order to get to his work place or to advertise places similar to the ones visited such as ski resorts or amusement parks.

Further, not all persons interact digitally the same way as they would do in "real life". On the one hand, a shy person tends to interact via texting instead of talking to the person directly. On the other hand, a socially active person may not interact a lot via cell phone as he or she does not have the time or the desire to do so. The criteria on which the personality traits are mapped surely correspond with many personality traits of many people but most definitely not with all of them.

Still, the prediction has proven to be accurate in more than two thirds of all cases as a study held in Barcelona [18] revealed in which the data of 600 volunteers was collected during six months. The personality traits predicted were compared to the results of a personality test every participant took in the beginning of the experiment. Future research will have to improve these numbers in order for personality prediction to be seen as a key factor. In order to do so, the criteria reviewed will have to be extended or other sources of information will have to be accessed.

4. PERSONALITY ADAPTION

As seen before, every person interacts differently with his mobile phone. When people interact with each other, they are adapting to other people's roles in society as they will talk differently to a police officer, a famous actor or the nice old neighbor from across the street. Adaption is not only made to the role a person plays in our lives, but also to the emotional state somebody is in. When somebody is sad, we are trying to cheer that person up, when another person is excited, we try to calm him down. In the same way, the other person adapts to us. It is a bidirectional exchange of various signals that defines whether we can or cannot get along with somebody else.

As discussed earlier, interaction with the cell phone is very frequent and still increasing. So, in order to improve the interaction, the cell phone should act like a "real" person and adapt to our needs and habits. Although the following [18] is to be seen as a quick gaze into the future, most of the technology is already available today.

First of all, the phone has to get the opportunity to learn, so it analyzes our personality by evaluation of e.g. inter-event time, entropy of places visited or the amount of contacts interacted with regularly as described in chapter four, it gathers data regarding the location or, the personal information as described in second chapter and it has to get used to our habits such as checking the weather forecast in the morning, checking for the next train in order to get to our workplace or having a look at the current traffic situation in order to not be stuck in traffic jams. After the learning process, the cell phone could do all of this automatically in order to save its owner some time. When leaving the house in the morning, the cell phone could give advice whether to take the train or the subway in order to get to the workplace as all information is accessible for it.

However, it can do much more than just adapting to our habits. Our phone can become much more than just a phone - It may become a partner that guides us comfortably through each day. As devices like Google glass or Galaxy Gear are on the rise, this offers new opportunities for interaction on the base of big data. A watch-like gadget may easily be equipped with a heart rate sensor. If this sensor detects stress, the phone could play the favorite song of its owner in order to calm him down. Blood sugar levels could be tested as well and the person could be notified by the smartphone when anomalies are detected[7] which would be a blessing for people suffering from diabetes.

So, in the future even though we may have the same type of phone as a friend of ours, the phones may behave in a completely different way as they are adapted to personal needs. This development is already set in motion, the technology is ready and future is about to become reality.

5. UNIQUE IN THE CROWD

In this chapter, the central topic of the paper will be dealt with. Are our mobility traces unique? And, if they are, what exactly does that mean for us? Is there anything one can do about it?

5.1 Are we unique?

According to dictionaries, uniqueness describes the state of being the only one of its kind, without an equal or equivalent. [16] Every person is unique but is his phone data unique as well? Is it possible to determine which phone data corresponds with which person despite of anonymization of the data sets?

As described before, each cell phone reveals its location as soon as it is connected to a wireless network, the GSM network or the GPS function is activated. From now on, focus will be laid upon determining the location via tracking through the GSM network which allows an accuracy of up to 100 meters. By combining this information with the current time, spatio-temporal data is created. Together with all other kinds of information gathered, datasets are created. These datasets are simply anonymized - similar to the anonymity, carriers provide when they sell the data aggregated with other users to third parties. Hence, those sets do not contain any personal data such as name, personal address or other distinctive personal identifiers. So, what will be shown is the fact that without any former knowledge about the person, it is possible to gain important information.

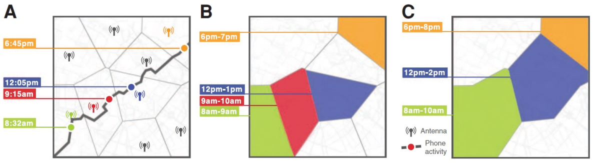

Figure 5: Mobility trace of a single dataset[1]

In Figure 5, the actual mobility trace is depicted in [A]. In [B] the position is depicted by analyzing the signal ranges of the base station that recorded the interaction. In [C] this information aggregated over longer time periods and base station's ranges are grouped.

What can we conclude out of the spatio-temporal data? When the location is tracked at 3am, it is most likely to be the person's home address while a location tracked at 10am is most likely to be that person's workplace. However, usually more than one person is living within a radius of 100 meters, same goes for workplaces. Hence, two points of spatio-temporal data is in most cases not enough in order to determine the phone user corresponding with the data.

So, in terms of mobility traces, this leads to the conclusion that we can only speak of a unique mobility trace when no other trace contains the same locations at the same time. Hence, a location traced at the Marienplatz in Munich at 5am is more likely to make a trace unique than the same place traced in the afternoon. With a population of slightly under 1.4 million, Munich is the third largest city of Germany. In 2013, an amount of 115 million mobile phone contracts were registered [21] in Germany. Assuming that mobile phone contracts are uniformly distributed in the population (and so, there are no variances due to regional aspects) that 1.75% of the contracts nationwide may be registered in Munich which leads to a total number of about 2 million contracts. As shown before in Figure 1, Munich is covered by an immense amount of GSM base stations, so the resolution of the antennas used is yery high. Is it possible to find unique mobility traces in a city as big as Munich?

It is, and it depends on the amount p of the spatio-temporal data extracted as well as on the cardinality of I which is the set that includes all spatio-temporal points. While those points are determined automatically on a regular basis, further interaction due to frequent phone calls or text messaging will increase the amount of points as shown in Figure 6. Hence, increased interaction at the same location will blur the result as the probability of randomly choosing a different location decreases. The higher p, the more increases the probability that the mobility trace becomes unique. If the location at noon and at midnight is extracted, this most likely is not enough to find unique traces. By adding a third location to the set, the cardinality of the subset of traces, that still have the same locations at the same times decreases. It may decrease to a cardinality of 1 and $|S(Ip)| = 1$ means that the trace has become unique as shown in Figure 7A and B.

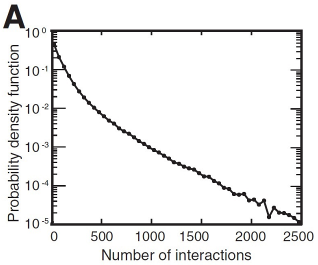

Figure 6: Probability Density with increasing amount of interactions[1]

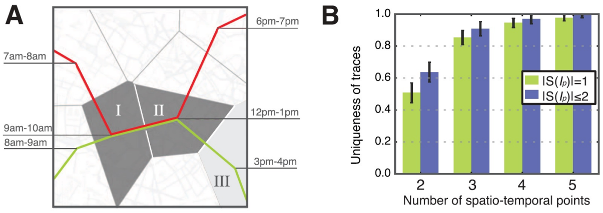

Figure 7: Uniqueness in respect to p[1]

A similar study [1] over 15 months with datasets of 1.5 million people has shown that four randomly chosen spatio-temporal points uniquely identify 95% of the traces while two points still identify more than 50%. By aggregating calls into three hour periods or even six hour periods and by grouping adjacent cell phone ranges, the uniqueness which is characterized by ϵ decreases. The uniqueness of a trace can be calculated by the function $\epsilon = \alpha - (vh)^{\beta}$ in which v is representing the resolution of antennas and h the resolution of hours. Hence, the output data is highly sensible to aggregation and traces at a high resolution are more likely to be unique. Statistically, uniqueness is higher when resolution of either antennas or time is coarse and the other one high. However, by modifying the estimators α and β, the uniqueness ϵ decreases by a constant factor. This can be compensated by increasing the amount p of points reviewed. If p is high enough, the uniqueness ϵ will be high enough despite of the coarse resolution.

So, it is possible to uniquely identify mobile traces. But is it also possible to link one to a specific person and so, to de-anonymize the dataset? As for now, only the location data has been used. Adding the data from social networks, evaluating photos posted on Instagram, check-ins at restaurants and meetings with friends in "real life" will create a social graph which can be evaluated accordingly. A study held in 2012 [3] showed that 80% of the traces could successfully be linked while only 8% of the traces were linked incorrectly

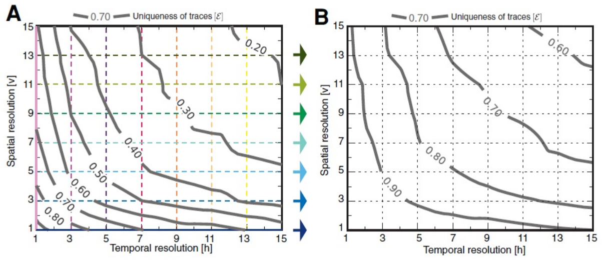

Figure 8: Uniqueness density with $p = 4$ (A) and $p = 10$ (B)[1]

while the remainder of the set could not be identified without a doubt. In this study, a contact graph based on the mobility trace is created. Additionally to that, a social graph consisting out of data that is publicly available at social networks as Facebook or LinkedIn is created. Those graphs are compared through various algorithms such as lowest edit distance[4]. If an accordance between the graphs is found, e.g. when two persons only have one mutual friend in a social network and meet regularly with each other and a third person in ”real life”, those traces would be very likely to be identified. The more vertices are identified, the easier it will be to identify the remainder, especially if the vertices are central and have many outgoing edges.

5.2 How can privacy be reclaimed?

But what does it mean for the individual when his anonymized mobility trace can not only be identified uniquely but also linked back to his personal data? It is a major threat! When the home address has been successfully linked to a mobility trace, it is a good target for thieves as they could find out easily during what hours the home owners are usually at work, school or at the gym. Frequent visits in a hospital could be interpreted as an indicator for bad health. If this information was accessible to an insurance company, monthly fees will either be a lot higher than usual or the person might even be rejected by the insurance company. These are only two of many possible scenarios of what might happen, if de-anonymized mobility traces were publicly available. They already make clear, that this must be prevented from happening. But how can this be prevented?

”Immediately throw away your smartphones!”, some might postulate. This however is most certainly not a good solution as that can only be seen as a hysteric over-reaction. It is necessary though that information awareness is built up. When the user is in control of the data, he knows which information is shared and can administrate it accordingly.

In order to do so, insight about the data provided needs to be gained. Often, it is hard to retrace the information access granted in the telephone's operating system. Thus, programs like TaintDroid[8] were developed in order to visualize the sensitive information shared. This program does not only visualize the data but also determines whether an application is accessing information it is not supposed to. Knowing where data is leaked is only the first step. Actions must be taken in order to stop the leakage.

There are many different models how personal data can be administrated by the phone user so he stays in control. One possibility proposed by the same researcher [4] who also conducted the study ”Unique in the crowd” described before, is to setup personal data stores. Those were to be filled with data collected by the cell phone and given by the phone owner. If an application or different service needs personal information, the owner can grant the right to access information to the respective service. As the data storage is self-administrated, the user may delete personal data at any time and make his personal information inaccessible. This however, is only an idea how to solve this problem and would require a change of laws that prevents companies from saving or selling data. A change is not in sight, yet.

6. CONCLUSION

In this paper, I have described what kind of data is gathered by the usage of the cell phone and to whom it is accessible. With this information being processed for personality prediction and personality adaption, the window of opportunities for the smartphone of the future is wide open. However, every person has to decide for his- or herself, whether he or she wants to keep feeding the phone with valuable personal data. Is the product received valuable enough to weigh up the data provided? However, to isolate oneself from this development is a tilt at windmills. Being a socially connected individual will require you to give up some of your privacy. Being unique in the crowd, however, is a problem that will have to be solved in order to protect the individuals' privacies. The scenarios described must be prevented; so, the user needs to regain control which, however, cannot be achieved without the help of the respective government. It will be a struggle but every way begins with a first step... And if the whole crowd is moving, the persons involved are no longer unique but uniform.

7. REFERENCES

[1] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen and Vincent D. Blondel: *Unique in the Crowd: The privacy bounds of human mobility*, pages 1-5, PDF, Boston, MA, USA, 2012

[2] Yves-Alexandre de Montjoye, Jordi Quoidbach, Florent Robic and Alex Pentland: *Predicting people personality using novel mobile phone-based metrics*, pages 1-3, PDF, Boston, MA, USA, 2013

[3] Mudhakar Srivatsa and Mike Hicks: *Deanonymizing Mobility Traces: Using Social Networks as a Side-Channel*, pages 1-10, PDF, College Park, MD, USA, 2012

[4] Yves-Alexandre de Montjoye, Samuel S. Wang and Alex Pentland: *On the trusted use of Large-Scale Personal Data*, pages 1-4, PDF, Boston, MA, USA, 2012

[5] Atle Arnes and Catharina Nes: *What does your app know about you?*, Datatilsynet, pages 14-16, PDF, Oslo, Norway, 2011

[6] Timothy A. Judge, Chad A. Higgins, Carl J. Thoresen and Murray R. Barrick: *Big five personality traits, General Mental Ability, And Career Success across the life span*, Datatilsynet, pages 623-625, PDF, Iowa City, IA, USA, 1999

[7] Nuria Oliver and Fernando Flores-Mangas: *Health*

[4] Minimal change due to adding or removing vertices

Gear: A Real-Time Wearable System for Monitoring and Analyzing Physiological Signals, Microsoft Research, pages 1-4, PDF, Redmond, WA, USA, 2006

[8] William Enck, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, Peter Gilbert, Byung-Gon Chun and Anmol N. Sheth: *TaintDroid: An Information-Flow Tracking System for Real-Time Privacy Monitoring on Smartphones*, USENIX Symposium, pages 1-15, PDF, University Park, PA, USA, 2010

[9] Chao Li, Daniel Yang Li, Gerome Miklau and Dan Suciu: *A Theory of Pricing Private Data*, University of Massachusetts, pages 1-12, PDF, Amherst, MA, USA, 2013

[10] *Global mobile statistics*, http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers

[11] *Verizon selling personal data*, http://money.cnn.com/2011/11/01/technology/-verizon_att_sprint_tmobile_privacy/

[12] *Every second mobile phone is a smart phone*, http://www.format.at/articles/1314/923/355857/das-handy

[13] *NSA can activate microphone and camera*, http://bgr.com/2013/12/31/nsa-iphone-hack/

[14] *What Does My Cell Phone Carrier Know About Me?*, http://bgr.com/2013/12/31/nsa-iphone-hack/

[15] *What Does Google Know About You?*, http://www.channel4.com/news/what-does-google-know-about-you

[16] *Definition of uniqueness*, http://www.thefreedictionary.com/uniqueness

[17] *How Big Data profits from your personal information*, http://www.theglobeandmail.com/globe-debate/follow-your-data-from-your-phone-to-the-marketplace/article17056305/

[18] *Presentation My Cellphone - My Partner by Nuria Oliver*, https://www.youtube.com/watch?v=kk-eJoK4fug

[19] *Big data and social good*, http://dynamicinsights.telefonica.com/1146/big-data-and-social-good-nuria-oliver

[20] *Telecom firms mine for gold in big data despite privacy concerns*, http://www.reuters.com/article/2014/02/23/us-mobile-world-bigdata-idUSBREA1M09F20140223

[21] *Amount of cell phone contracts in Germany*, http://de.statista.com/statistik/daten/studie/3907/-umfrage/mobilfunkanschluesse-in-deutschland/

[22] *Mobile content usage*, http://www.statista.com/statistics/187128/mobile-content-usage-in-the-us-by-share-of-subscribers/

[23] *GSM base stations in Munich*, http://maps.muenchen.de/rgu/mobilfunkstationen

[24] *Track My Life*, https://tml.me/

[25] *Facebook likes predict personal traits*, http://news.sciencemag.org/2013/03/facebook-preferences-predict-personality-traits