Intimate data in relationships: Tracking, sharing, surveillance - personal boundaries?

Diana Irmscher

Abstract— Self-tracking has become commonplace in the century of digitalization. People are tracking themselves or rather personal information. Moreover, they are storing and sharing this data.
The Quantifying Self movement has inspired this trend. Today it is possible to track quantifiable data like heartbeat or sleeping pattern, but also "'not measurable"' data like moods, feelings and behaviors, which have a high intrinsic value. Such tracked data can be highly intimate, e.g. data of sexual and reproductive activities or intimate relationship.
In this work, it is considered why people tracking themselves, and storing and also sharing such intimate data.

Index Terms—self-tracking, self-quantification, personal informatics, intimate data, data ethics, privacy

1 INTRODUCTION

In the century of digitalization there are many opportunities offered to perceive the self and own life in a different way as before. Tracking and quantifying is commonly used. Nowadays many people are engaged in tracking their data. They are tracking and also sharing this information with other people, like friends or like-minded people.

But there are many different types of data, which can be tracked. Such data like heartbeat or sleeping pattern does not seem to be too intimate when tracking and sharing, but how about data in intimate relationships and sexual behaviors?

In this work, the collecting, tracking, storing and sharing of data in intimate relationships is investigated. Therefore, the following questions will be answered by searching for literature and studies in this scientific field:

1. What data is perceived as intimate? In what circumstances?

2. Why do people track intimate data?

3. What do they do with, e.g. tracking, storing, sharing and discussing and with whom?

   (a) Do they over-trust the tracked data?

   (b) How do they perceive their tracked data?

For answering of the mentioned above questions a research of literature and studies on collecting and tracking data in intimate relationships is carried out. The answering of the first question is not as easy as it seems. Therefore, several definitions from different source are collected.

2 TERMS OF DEFINITION

In this section the term *intimate* is defined. Due to this it is considered what data is perceived as intimate and in what circumstances.

The question can not be answered easily. The perceiving what is intimate depends on several factors. In general it has to be differentiated in the culture, how a human is perceiving the self and what is shaping the sociocultural live [1]. It is not possible to consider all well-known cultures in this work, therefore the focus is limited on the scrutiny of the western civilization. In the western civilization privacy takes up a lot of space. Nevertheless, the state of a person in the society is defining the personal perceiving of privacy and intimate data. And

- *Diana Irmscher is studying Media Informatics at the University of Munich, Germany, E-mail: d.irmscher@campus.lmu.de*
- *This research paper was written for the Media Informatics Advanced Seminar 'Advanced Seminar in Media Informatics', 2018*
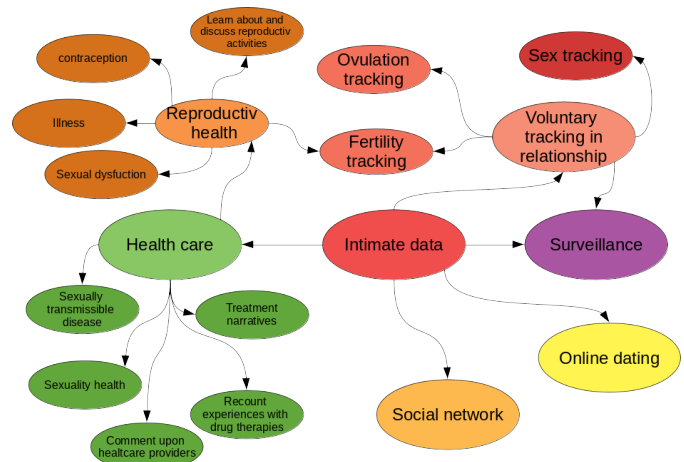
Figure 1. Visualization of possible intimate data, which are arising from using such digital technologies.

the personal view, as well. These things can not be defined in a few sentences, the topic is to complex and not measurable. Furthermore, it is subjective. For the individual, the perception of intimate data is different.

Due to this, the definition of what is perceived as intimate for people living in the western civilization, will be shown by the following examples. Several work are focused on intimate date in in different contexts. Although, a clear definition of what data is intimate or is what people perceive as intimate is not found. In the following some descriptions are summarized to give a rough outline.

The focus in Danaher et al. [2] is on intimate interpersonal relationships. In this work there is no clear definition to be found. They think a definition for such term is not needed. However, to describing a romantic relationship the authors in this work are writing the following:

> [...] we trust that most readers' intuitive sense of those terms [..] will be adequate for our arguments to make sense". That said, romantic relationship might usefully be thought of as a cluster concept, with paradigmatic examples in the middle, and less paradigmatic examples clustered around it, each one different along various dimensions (e.g., the degree to which sexual interaction is central to the relationship).

So, if it possible to define an intimate or romantic relationship about such a way, this concept will also fit for the term intimate. We can

build a cluster categories of intimate data, which are assigned to corresponding activities, e.g. fertility tracking.

In figure 1 several topic related to the term intimate data are collected and and brought in relation to each other. At this point it must be emphasized that this does not cover the complete field, in which intimate data would be collected, tracked, shared and so on. Rather it is an summarizing of terms and descriptions from Levy [4], Danaher et al. [2], Lupton [5] and more.

The idea to use an cluster concept can be thought of one step further. The sensitivity or level of intimate data could be arranged in some sort of data hierarchy. Form IT-Security Management it is known to evaluate risks by assigning a probability and to classify accordingly (see documentation of Federal Office for Information Security (BSI) [3]). In this table I want to classify the data summarized above based on their sensibility.

To give give another understanding of what is meant with *intimate* in this paper I want to quote a paragraph form Lupton [5], which describes an Application for mobile phones:

> The Glow app brings male partners into the equation by sending them a digital message when their partner is in her fertile period and reminding them to bring her flowers [...]. This app also tracks menstrual and ovulation indicators, as well as asking women to enter details of their sexual encounters, including sexual positions used, whether or not they had an orgasm and whether they experienced emotional or physical discomfort during sex. It employs the aggregated data from other users to refine predictions of ovulation and fertility for the individual user. [...]

This paragraph describes a sort of tracking which also called *intimate tracking* (defined by [2]).

At this point I will close with definitions of what is perceived as intimate by people. We can also find intimate data in other contexts, e.g. as mentioned above in health care. But the focus in this paper is on intimate data in relationships, therefore I refer to the Figure above. This should give a general understanding of the context.

3 LIFE COURSE OF INTIMATE RELATIONSHIPS

Levy [4] has defined a so called *life course of intimate relationships*. This course includes four conditions of romantic relationships (see Figure 2).

Figure 2. The life course of intimate surveillance

In each of these conditions (potential) partners can use technologies for different purposes.

Condition **A** stands for the beginning of a potential relationship. The partners know each other or would like to know each other. At this point, there is an interest from one or both sides. The aim is to learn more about the other person, to check their identity and social life.

In condition **B** the partners are already in a relationship or something appropriate. At this point I will notice that this condition will include all relationships that are understandable as this. For a concretely definition what a (romantic) relationship means see Danaher et al. [2] or 2. The partners know each other better, have an increased (mutual) interest. There were other forms of contact, possibly sexual contact.

In condition **C** there is usually an established relationship (but that does not have to be the case, there maybe exceptions). The couple exercises sexual activities, deals with contraceptive measures (together) or plans to start a family.

Condition **D** contains the surveillance of the partner, also abuse (of data) and revenge. Describing this condition is complicate. It can be a relationship that has already ended. The partners therefore have a relationship to each other based on their previous history. This can be different (as in the other states). More generally, this condition maybe arise from problem in the relationship, due to interpersonal conflicts oder something else. But it may also be a state or point in the relationship which is fine for both partner (at this point I mean surveillance). This will be discussed later on.

The different conditions are not connected to each other because this is not possible to give sense at any time. Relationships are complex and individual [8]. Also this is not the focus of this work. The descriptions above only should give an idea what the conditions mean for the following section 4.

4 CONSIDERATION OF EACH CONDITION IN LIFE COURSE

TODO: For each state, the results from the individual papers are collected. Further individual distinctions can be derived from this (for instance in B it is is to be distinguished between intimate tracking and intimate gamification). The types of possible data collection, tracking and also sharing is to be reported for each condition in life course.

4.1 Condition A: Dating: Scoping out potential intimates

At the beginning of a potential relationship we want to know more about the person of our interest. Due to this, we so called collect data about this person. A good way the get relevant information is using a standard social network like Facebook [1] or using Google search. Monitoring a person on Facebook is known as Facebook stalking [4]. To stalk another person on Facebook undiscovered, much articles has been written about [9]. With the Website stalkscan.com [2] it is possible to get all public entries from a persons Facebook profile site which is public by only one mouse click. Surley, it can only shows what is already set public, still it make it more easily to talk another person very quickly. Within this website as tool is also avoided to give an involuntary like by clicking through the photographs, for instance. The Google search mentioned at first is known as *google someone*. With this method is it possible to get information from every source which is findable for the search machine [7]. Also for this topic there are many article how to *google someone*. For instance, the search on images is of high interest [3].

The topic in this condition A is not only searching data about someone, but also create such data. Levy [4] mentioned the application Lulu as a tool to create data for use in prospective relationships. The focus of this application is on campus life. The app Lulu gives young women the opportunity to review male students and friends, with which they are connected on Facebook. The review contains information in relation to humor, manners, look and style, sex and kissing. The review giving by the female users is anonymously. In the first version, each male fiend on Facebook could be reviewed in this app. But after concerns related to privacy of reviewed male Facebook users, a review can only be committed for such male user which have explicitly allowed to this.

Furthermore, such services that combine online dating with user's geographical location are well known. Tinder is a widespread location-based dating service. The app shows potential people with different interests (e.g. romantic relationship) near to the user's location or next holiday destination [4]. By showing the user several profiles he/she can deside to swip right for a like. If the other person does also a right swip, it is a match. Now the user can exchange messages, for instance to get a date. The princip sound easy, but isn't at all. By using these app, a huge among of intimate data is collected. First of all, the tinder app is connected to Facebook and Instagram, a photo-sharing social networking service, owned by Facebook itself. In order

---

[1] www.facebook.com
[2] https://stalkscan.com
[3] https://www.lifewire.com/google-people-search-3482686
[4] https://tinder.com

to this there is a huge commercial interest to assume. Judith Duportail demanded access to here personal data under European data protection law after four year using the tinder app. The respons was an over 800 site report containing diffrent types of data like Facebook likes, information about education, age-rank of men she was interested in, number of Facebook friends, when and were every online conversation with her matches happened, also interests and jobs, pictures, sexual preferences. The list contains a huge amount of intimate data. In the article Duportail writes, she was amazed by how much information she was voluntarily disclosing. This was also called secondary implicit disclosed information. Firms have an increasing interest in gathering personal data from user's activities [11]. This results in a trade-off for the user - use the system and accept privacy concerns due to the commercial interest from the provider, or abstain the service. Nevertheless all concerns, users reveal their data very quickly, as shown in Tait et al. [10]. Users who tend to gain confidence quickly, therefore, also more quickly reveal more information. In addition, this study showed that higher profile activity increases the amount of information desired. That means, users who maintain an active profile and present activity also receive more and higher information from other user's rather than users of profiles that provide barely information. The disclosure of information is determined in part by the personality of the user and the context in general. This affects how users surround their data online and with strangers. They found out that in only 6 - 10 minutes a user can extract the full name and date of birth from a conversation. Within these information it is easy to get further data about the person via Google search and Facebook, for instance.

In Nandwani et al. [6] it was examined how quickly users reported their data to strangers and, above all, which data. For the study, an automatism was developed to contact 100 Tinder users. The study was a single blind study, so users did not know at the moment that they were writing with a Chat-bot. The evaluation of the data yielded the following results: Most of the published data was personal data, for instance: full name, date of birth, phone numbers, work details, email-addresses, complete address and other data that will not be listed here.

Why are this data disclosed to strangers in online platforms and apps? As mentioned above, the user trusts in the authenticity of the other within an active profile account. Also they do not reflect the inpacts of disclosure there personal and also intimate data. For this purpose, Nandwani et al. [6] suggest an virtual assistant in such applications like Tinder, which study the relationship between the users by parameters and inform the user which information should be reveal in the conversation.

A *Data collection at the beginning of a relationship, Facebook stalking, potential partner googling, Tinder. In the following: why is this used or why are these data collected, recorded etc. Subsequently, how do people perceive this, influence of data on perception*

B *Categorization in intimate tracking and intimate gamification from Quantified Relationship: example of these apps and tracking devices. What added value do they have in the relationship? What's in it? How do people perceive that (Quantifying, over-trust in numbers).*

C *Drafting the role of women at this stage of a relationship: many apps and devices for tracking women (cycle, fertility, etc.).*

D *Category intimate surveillance from Quantified Relationship: main emphasis: Tracking the partners in a relationship: acceptable or not by mutual agreement? Does that affect the relationship, or the mutual trust? There is no investigation until now (continue at the end (conclusion, further work)).*

5 RISKS

1. *Quantification (perception and rating of the self and the relationship)*

2. *Trust (unknowingly tracking by intimate partner, over-trust in data only)*

3. *Privacy (risks, current news, data gaps, etc.)*

6 CONCLUSION AND FUTURE WORK

7 ACHIEVEMENTS

REFERENCES

[1] Michael Carrithers, Steven Collins, and Steven Lukes. *The category of the person: Anthropology, philosophy, history*. Cambridge University Press, 1985.

[2] J. Danaher, S. Nyholm, and B. D. Earp. "The Quantified Relationship". In: *The American Journal of Bioethics* 18.2 (2018). PMID: 29393796, pp. 3–19. DOI: 10.1080/15265161.2017.1409823. eprint: https://www.tandfonline.com/doi/pdf/10.1080/15265161.2017.1409823. URL: https://www.tandfonline.com/doi/abs/10.1080/15265161.2017.1409823.

[3] Bundesamt fr Sicherheit in der Informationstechnik (BSI). *IT-Grundschutz - 4.3 Risiken bewerten*. German. visited on 25.05.2018. Bundesamt fr Sicherheit in der Informationstechnik. [2018]. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/ITGrundschutzSchulung/Webkurs1004/4_RisikenAnalysieren/2_Risiken%20bewerten/RisikenBewerten_node.html.

[4] K. Levy. "Intimate surveillance". In: *Idaho Law Review* 51 (2014). [visited am 23.05.2018], pp. 679 –693. URL: https://heinonline.org/HOL/P?h=hein.journals/idlr51&i=709.

[5] Deborah Lupton. "Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps". In: *Culture, Health & Sexuality* 17.4 (2015). PMID: 24917459, pp. 440–453. DOI: 10.1080/13691058.2014.920528. eprint: https://doi.org/10.1080/13691058.2014.920528. URL: https://doi.org/10.1080/13691058.2014.920528.

[6] M. Nandwani and R. Kaushal. "Evaluating User Vulnerability to Privacy Disclosures over Online Dating Platforms". In: *Innovative Mobile and Internet Services in Ubiquitous Computing*. Ed. by Leonard Barolli and Tomoya Enokido. Cham: Springer International Publishing, 2018, pp. 342–353. ISBN: 978-3-319-61542-4.

[7] Jason Nolan and Michelle Levesque. "Hacking human: data-archaeology and surveillance in social networks". In: *ACM SIGGROUP Bulletin* 25.2 (2005), pp. 33–37.

[8] S. Sassler. "Partnering across the life course: Sex, relationships, and mate selection". In: *Journal of Marriage and Family* 72.3 (2010), pp. 557–575.

[9] M. Strathmann. *Diese Webseite macht Facebook-Stalking unheimlich einfach*. 2017. URL: http://www.sueddeutsche.de/digital/privatsphaere-in-sozialen-netzwerken-diese-webseite-macht-facebook-stalking-unheimlich-einfach-1.3380921.

[10] S. Tait and D. Jeske. "Hello stranger! Trust and self-disclosure effects on online information sharing". In: *International Journal of Cyber Behavior, Psychology and Learning* 5.1 (2015), pp. 42–55.

[11] David G Taylor, Donna F Davis, and Ravi Jillapalli. "Privacy concern and online personalization: The moderating effects of information control and compensation". In: *Electronic Commerce Research* 9.3 (2009), pp. 203–223.