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 with other users.
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 related to sexual and reproductive activities or intimate relationships.
In this work, it is considered why people tracking intimate data in romantic relationships. Further is is investigated how they perceive these data and how this affects the perception in context to the social life.
It can be shown that some highly intimate data are partially collected by the users of self-tracking devices in a unconsidered way and further that these data are processed by third parties with commercial interests.
Thus it can be shown that the collection and tracking of intimate data has taking place in our everyday lives. Nevertheless, it should be considered in what context and for what purpose this intimate data are tracked at all. The role of third parties is also problematic. For example, the use of devices which are not connected to the Internet and transmit the tracked data, could be supported.
Everyone should question themselves for the use of such technologies. The use of such technologies in a romantic relationship also creates an ethical and social trade-off within the topic.

Index Terms—intimate data, quantified relationship, surveillance, self-tracking, self-quantification, data ethics, privacy, love

1 Introduction

In the century of digitalization there are many opportunities offered to perceive the self in everyday life in a different way as before. Tracking and quantifying the self, the body an also other aspects in life is commonly used as showed in [13]. Nowadays many people are engaged in tracking such data like heartbeat, sleeping pattern and other quantifiable data. They are tracking and also sharing this information with others, like friends or like-minded people.

But there are many different types of data which can be tracked. Superficially, such data like heartbeat or sleeping pattern does not seem apprehensive when tracking and sharing these with others, but how about data in intimate relationships and sexual behaviors?

In this work it is investigated how people use techniques for collecting, tracking, storing and sharing of intimate data in romantic relationships. Techniques in this field also called Quantified Relationship techniques. In addition to tracking and sharing, surveillance also plays a key role, which is considered. Therefore, the following questions will be answered by reviewing literature and studies in this scientific field:

RQ1: What data is perceived as intimate? In what circumstances?

RQ2: Why do people track intimate data in relationships?

RQ3: What do they do with, e.g. tracking, storing, sharing and discussing and with whom?

1. Do they over-trust the tracked data?
2. How do they perceive their tracked data?

For answering the questions mentioned above a research of literature and studies on collecting, tracking and sharing intimate data in romantic relationships is carried out. In Addition, some articles and reports by users of tracking and other technologies are also used for finding answers, e.g. the report by Duportail [8] about the data which tinder collect over a period of time.

Intimate data are searched, collected, tracked, stored and shared in every part of relationship, from the beginning until to termination. The different types of intimate data were collected from *Facebook* and *Tinder* and tracked by Quantified Relationship technologies, for example to quantify sexual activities or measuring menstrual cycle. The several types of intimate data are obtained from different sources. At the beginning of a relationship, data are gathered from Facebook, Tinder and other soical networks. At the point the relationship is "established", other technologies become more relevant, e.g. Quantified Relationship technologies, to quantify sexual activities or measuring menstrual cycle of the partner, to gain more details about the mood. If a romantic relationship is broken off, social networks and Quantified Relationship technologies can be abused, e.g. to stalking the ex-partner, or even harm. The usage of all these digital helpers in intimate relationships is always associated with a certain risk. Often, default security precautions are insufficient for specific situations, e.g. as in the dissolution of a relationship. Frequently users are not aware about the type and scope of intimate data which collected and tracked by their own devices (e.g. the smart phone), and which my be accessible by others like the ex-partner or third parties.

In section 2 the term *intimate* is defined by gathering different definitions related Quantified Relationship-technologies and intimate surveillance. In section 3 the so called life course of intimate data is defined including four conditions in which an intimate relationship could be. The following section 4 describes the conditions with regarding to the intimate data that are searched for, tracked, stored and shared in these circumstances. In section 5 the risks related to the use of such technologies in a romantic relationship is investigated. Section 7 includes a summarization of the work with a short view for future steps.

2 Terms of Definition

In this section the term *intimate* is defined. Due to this it is considered which data is perceived as intimate and in which circumstances. Answering the first research question in this work is not as easy as it seems. Therefore, several definitions from different source are collected.

The perceiving of what is intimate depends on several factors. In general it has to be differentiate between the culture, how a human is

- *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*

perceiving the self and which factors are shaping the sociocultural live [3]. It is not possible to consider all well-known cultures in this work, therefore the focus is limited to the scrutiny of the western civilization. In the western civilization or rather in the European Union (EU) pri-

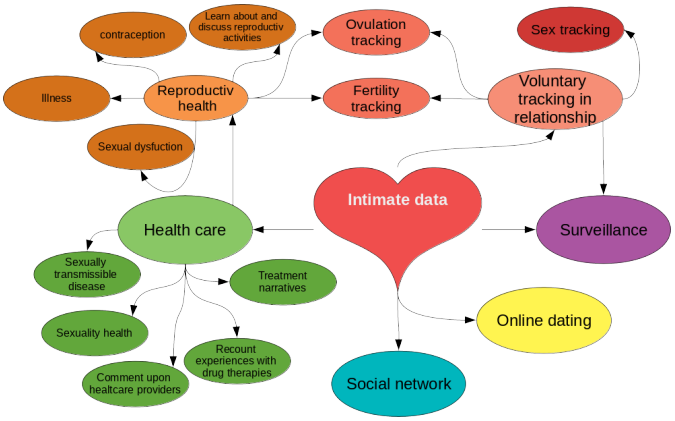

Figure 1. Visualization of possible intimate data, which are arising from using such digital technologies.

vacy and data security takes up more attention, even since the General Data Protection Regulation (GDPR) is applied [1]. However, the state of a person in the society is defining the personal perception of privacy and data security, and the personal view as well. What is perceived as intimate depends on this factors. But these 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 whether data are intimate or not is different. Several works are focused on intimate data in different contexts. Although, which data is intimate or what people perceive as intimate is not clearly defined. Due to this, some descriptions are summarized to give a rough outline.

The focus in Danaher et al. [7] is on intimate interpersonal relationships. In this work no clear definition of the term intimate data is presented. They argued that it does not need a precise definition to get an understanding of intimate relationships. To describing a romantic relationship the authors wrote:

> [...] 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).

If it is possible to define an intimate or romantic relationship about such a way, this concept will also work for the term *intimate*. It can be visualized in a cluster of different types of intimate data, which are assigned to corresponding activities, e.g. fertility tracking. In figure 1 several topics related to the term intimate data are collected 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 monitored. Rather it is an summarization of terms and descriptions which come up in this work.

To give another understanding of what is meant with the term *intimate* it is quoted from the work by Lupton [15], which describes an application for smart 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 [7]).

We can also find intimate data also in other contexts, e.g. as mentioned above in health care. In general it can be said that the perception of what is perceived as intimate depends on the context of prevailing situations. The health of an employee may be an intimate information, e.g. whether an employee is pregnant. The fact that insurance companies offered their customers a discount if they disclosure their Facebook profile shows how relevant such types of data are for different purposes. [1] But the focus in this paper is limited on intimate data in relationships, therefore it is referred to the figure 1 above. This should give a overall understanding for the following sections.

3 Life Course of Intimate Relationships

Levy [14] has defined a so called *life course of intimate relationships*. This course includes four conditions of romantic relationships (see Figure 2). Each condition is colored from colors from figure 1. Here, the connection to the individual topics should be roughly indicated. The transitions in content are sometimes fluid.

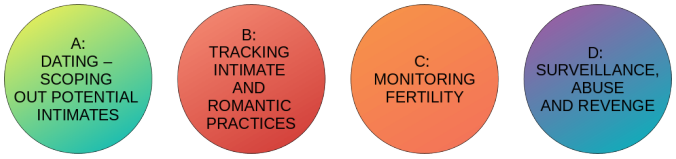

Figure 2. The life course of intimate surveillance.

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, it should be emphasized that this condition includes all sorts of relationships that are understood as such. For a concretely definition what a (romantic) relationship means see Danaher et al. [7] or 2. In this condition the partners know each other better and 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 problems 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 (that refers to the surveillance). This will be discussed later on.

Since relationships are complex and individual, the single conditions are not interconnected [21]. Also this is not the focus of this work. The descriptions above only should give an idea of what the conditions mean for the following section 4, in which all conditions will be discussed in detail.

[1] https://www.heise.de/newsticker/meldung/Versicherung-wollte-Hoehe-der-Kfz-Versicherung-aus-Facebook-Posts-errechnen-3454410.html

4 CONSIDERATION OF EACH CONDITION IN LIFE COURSE OF INTIMATE RELATIONSHIPS

In this sections it is how the single conditions are each condition is investigated for the type of data that can be searched, collected, tracked and shared by the user or others in this condition. Therefore each condition is is treated in a separate section. The individual sections summarize which intimate data is collected, tracked and so on, how it is perceived by the user and how it affects the users perception.

4.1 Condition A: Dating - Scoping out potential intimates

At the beginning of a potential relationship one want to know more about the person person of our interest. Due to this, one collect data about this person.

4.1.1 Searching for information

A good way the get relevant information is using a standard social network like Facebook [2] or using Google search. Monitoring a person on Facebook is known as Facebook stalking [14]. To stalk another person on Facebook undiscovered, much articles has been written about [23]. With the Website stalkscan.com [3] 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 stalk 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 engine [18]. Also for this topic there are many article how to *google someone*. For instance, the search on images is of high interest [4].

4.1.2 Creating and providing information

The topic in this condition A is not only searching for data about someone, but also create such data. Levy [14] 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 friend 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 [5]. 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 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 her 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 [25]. 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. [24]. 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. [17] 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 impacts of disclosure the personal and also intimate data. For this purpose, Nandwani et al. [17] 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.

4.2 Condition B: Tracking intimate and romantic practices

The potential of creating, collecting and tracking intimate data rises if the romantic relationship between two individual deepens. A romantic relationship in which intimate data were tracked is named a Quantified Relationship (QR). Danaher et al. [7] describing in their work three categories of intimate data which can be tracked in a QR. In table 2 the three categories are summarized with a descriptions and examples.

In the following the categories intimate tracking and intimate gamification are considered in more detail. The third category intimate surveillance will be discussed in section 4.4.

4.2.1 Intimate tracking

For the tracking of intimate data, there are a variety of apps that can be used for it. The apps usually track the following data about sex life [7]:

- number of partners
- number of "sessions" per partner
- sexual positions used during theses sessions
- number of thrusts per session
- duration of these sessions
- number of calories burned per session

This list only mentions the most common. There are many more variants of intimate data that can be tracked. As Kelly [13] mentions, nearly everything is tracked that is possible. That may not cover the big crowd, but that's also practiced.

The data are voluntarily or automatically tracked using such technologies [7]. That means, the data is either actively provided by users or automatically recorded, e.g. by running the app in the background and recording audio. This type of tracking or communication is also

[2] www.facebook.com

[3] https://stalkscan.com

[4] https://www.lifewire.com/google-people-search-3482686

[5] https://tinder.com

Table 1. Interrelated types of data in Quantified Relationship, source from [7]

Type	Description	Examples
Intimate tracking	Collection of all (measurable) data that can arise through intimate behaviors (in a relationship), e.g. number of partners, number of sexual encounters, duration of sexual encounter, or romantic behaviors (gifts, help in the household, attention)	SexTracker SexKeeper Nipple Lovely kGoal
Intimate gamification	Use of gamelike incentives to change or improve the behavior in a romantic relationship; Playful learning to lead a successful relationship	-
Intimate surveillance	Use of technologies to monitor intimate partners	-

referred to as *participatory surveillance*. As Lupton [15] writes, this includes looking at oneself, but for one's own purpose. Self-tracking is often associated with self-reflection, but it has less to do with it [16]. Rather, it is a visualization and reflection of the collected numbers. But the reflection of the self in this context involves much more than the visualization of the numerical data. This is more of a strict focus on the pure numbers. These numbers are only objectively perceived, and no longer associated with the subjective activity or context to which they once belonged. Often, these apps also contain elements for the gamification of the mission or goals.

4.2.2 Intimate gamification

Another observation is the gamification in this area of tracking. Users are encouraged to quantify their sex lives in order to measure their performance and compare themselves with other users [15]. This type of quantification mainly focuses on the male user.

One consequence of using such technologies may be the reinforcement of gender stereotypes [15]. The algorithm defines the goals that users use to orient and measure themselves against. The individuality is lost.

In addition, this type of feedback does not necessarily have to be of good quality or have a lasting effect on relationship life. [7]. After all, a good relationship is not measured by how much sex one have or how long it lasts. As explained in the section 2 above, there are many more components that make a good relationship.

4.2.3 Objections

The automatic recording of such data in an app can be very questionable, because the danger is great that the user is not aware of it. Most users do not read the the fine print of the terms and conditions of these services before using them [14].

Also, the sole quantification of a relationship does not necessarily lead to an improvement of the relationship skills. Rather, these types of behavioral change supports gender stereotypical reinforcement. That would be a very retrograde development compared to the current perception of our conception of love and sexuality. In addition, as already mentioned above, the users perceive the data objectively only by quantifying the activities, similar to a sport activity like running. The reflection of the real activity is lost.

Users share this data with like-minded users, or keep it for themselves and do not share it, or share it with their intimate partner. The mere possibility of sharing this data brings with it a significantly larger audience [15]. This also influences the willingness to disclose intimate data to strangers. Users also share the data for the purpose of comparison with other users. The gamification which is often used in such apps also supports this in addition.

4.3 Condition C: Monitoring Fertility

This section will focus on tracking the cycle and fertility of female users. These types of data are therefore very intimate. So far, they have been collected only in conjunction with a medical treatment and evaluated with the doctor.

4.3.1 Overview of technologies for monitoring fertility

The cycle and thus the connected fertility of the woman has been "monitored" for a long time. The exact beginning is unknown, it has been writing about it since the 1920s in scientific medical [20]. With Josef Roetzer the symptothermal method became well known [19]. With this method the cycle could be monitored and the fertile days could be determined exactly with a few differences.

In the age of digitalization, there are of course digital technologies that support the female user to monitor the data.

The following table lists some (known) app, which can be found in Google App Store or Apple App Store.

Table 2. App for tracking the cycle

term	operating system	Description
myNFP	iOS Android	myNFP evaluates the cycle according to the symptothermal method (NFP). All important parameters for the evaluation are entered by the user herself.
Kindara Fertility & Ovulation	iOS Android	is based on the Fertility Awareness Method; supports the Sympto-Thermal method and can be used for Natural Family Planning (NFP)
Lily	iOS	It is evaluated according to the rules or according to the symptothermal method or based on average values of other users; If one want to use the app in full functionality, a contribution will be charged; therefore, the manufacturer guarantees that the data will not be evaluated by third parties, the personal information will not be stored, and no backup of personal data will be stored on any server; [6]
Glow	iOS Android	

According to the manufacturer of the myNFP app, the sensitive data is not processed by third parties. Furthermore, as few as possible data is recorded. The data are anonymous and does not indicate the person. The manufacturer justifies this with the argument that the app charges a monthly fee of 2.50 € [7].

For Kindara app can also be found information on privacy, but these look different than in the previous app. An excerpt from the privacy policy provides more information [8]:

> Kindara collects and uses the information you provide to us when you use the Kindara Service. Information that Kin-

[7] https://www.mynfp.de/datenschutz
[8] https://www.kindara.com/privacy-policy

dara may collect includes: name, date of birth, e-mail address, fertility-related data and other family planning and health-related information you provide. You may consider some of this information to be sensitive so you should choose carefully regarding whether and if you will use the Service.

Since the app is offered for free, it is reasonable to assume that the data will be processed further. The commercial interest of the manufacturer should be noted and analyzed in more detail before using this app. An additional device is offered for the app, which can be used to measure the wake-up temperature. The device will automatically connecet with the app when the temperature is being measured. The data will be sent to the app via bluethoot [9].

4.3.2 The Glow Application

I would like to comment on the Glow app separately, because a lot of papers are writing about it [7], [14] and [15]. Launched by Pay-

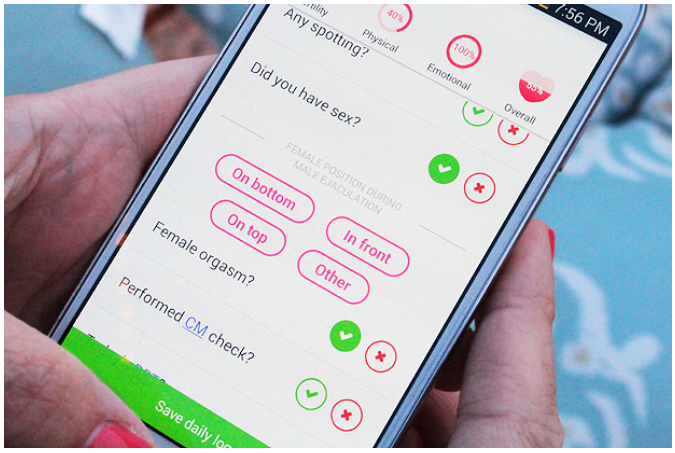

Figure 3. The Glow app collects a variety of intimate data (Potograph source: [2])

Pal founder Max Levchin in 2013, the app offers great concurrence with many other fertility and natural prevention apps. The Glow app tracks a huge amount of intimate data, among others the menstruation, position and firmness of a womens's cervix, sexual intercourse (with the women's position during ejaculation), whether they had an orgasm [and] whether they experienced emotional or physical discomfort during sex" [15]. In addition, the mood of the user can be tracked. The difference to other apps is that the Glow app makes the collection of intimate data a family affair. The users' partners are invited to download a mirror app and provide additional data [14] The app also sends messages to the partner about the current status of the partner's period, reminding of attention such as flowers or a nice message. The data of the users are evaluated collectively in order to be able to specify better forecasts for the individual user from the large collection.

Danaher et al. [7] argue under the point *Gender Relationship Objection*, that these types of technologies are making women an object of surveillance and quantification. These technologies give the impression that the cycle of a woman is unsupervised chaotic and can only be "rebuilt" with strict control. In addition, this app would promote the development and enhancement of gender stereotypes, as also augmented in [15].

The giving or disclosure of such intimate data is sometimes very questionable if the user disregards how the data is further evaluated. Certainly, these technologies can be helpful in the evaluation of the collected data, and remind of the daily measurement. Unfortunately, these very sensitive data are also used for commercial purposes.

[9] https://www.kindara.com/wink

4.4 Condition D: Surveillance, abuse and revenge

The condition D is about surveillance in relationships. The other three conditions are also about surveillance, but in a different way. The differences are briefly described and illustrate in the following.

The conditions described above deal with the different situations in which intimate data can be created and used, e.g. for surveillance purposes. The section 4.1 covered the collecting of data via social networks and online dating services. In section 4.2 the generation and collection of intimate data in a relationship was described. In Section 4.3 it was discussed about the monitoring of woman or rather their menstrual cycle and fertility. A summary of the previous conditions can be seen in figure 4. As described above, users voluntarily or unconsciously disclose this data to benefit from data science (see Glow App, which calculates the course of the menstrual cycle among other analytics from the data set of other users, making a relatively reliable prediction of ovulation possible without the user providing daily tracked information). In all these states one can speak of an voluntarily participatory surveillance. The supervisor is usually the provider of the smart phone application or the wearable devices, which is commercial interested in the data. This possible form of surveillance is discussed critical in more detail in section 5.

In this section the mutual surveillance of the partners in existing or also terminated relationships is considered in more detail. The type of surveillance in a relationship can be voluntary or involuntary. The threat of providing such kind of intimate data in the context of an intimate relationship should not be disregarded.

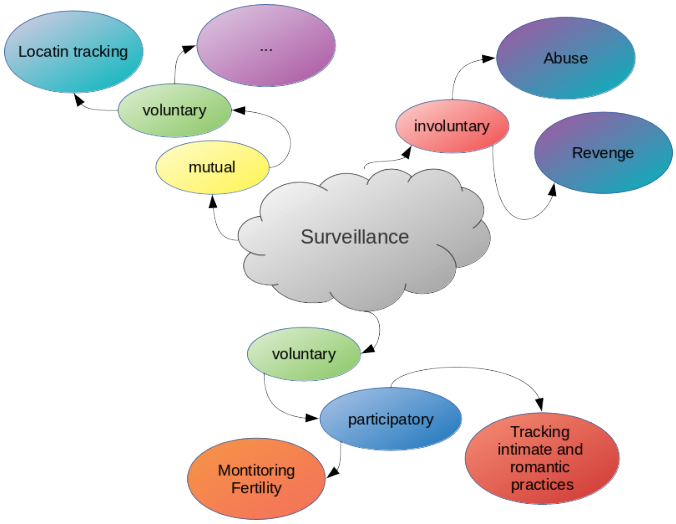

Figure 4. Summarizing of conditions A, B and C, based on the visualization of [5]

4.4.1 Mutual voluntary surveillance provides mutual trust?

For mutual voluntary surveillance in an existing relationship, Danaher et al. [7] have given an interesting but also something questionable approach.

The authors consider if mutual voluntary surveillance in an existing intimate relationship could be useful to provide mutual trust. First they define the concerns related to the use of such QR-technology for supporting partner's mutual trust in a well-functioning relationship. They found out, that such a tracking technology could corrode the mutual trust, which a romantic relationship is usually based on.

Levy argue in [14], that mutual trust in a relationship has played a fundamental role so far and promotes pro-social behavior in the relationship. If digital technologies take on this role now, by tracking the partners in the relationship, and if the partner does control themselves and build their trust on it, it does not rely on loyalty to the partner anymore, but only to the tracking software.

Due to this fact, it is questionable, where the using of such tracking technologies in relationships leads. Danaher et al. argue that "even if mutual trust is an ideal, it is an ideal that many fall short of in reality." [7]. The authors suggest that partners, to some part in the relationship, voluntarily observe themselves to appease the other's doubts. But they also add some considerations to privacy and security risks. Such use of tracking technology requires extreme caution and respect. It requires the explicitly agreement of the partner. Furthermore, the technology itself should involve a hard-but-reversible lock-in, to bring the surveillance under control and interrupt this if any of the partner would not tracked further from the other. They suggest that an example could be an smart phone application that allow mutual surveillance, e.g. for a period of time. It would be interesting to survey if partners would use such an tracking technology, in which circumstances and conditions and, especially, if they would find such an approach desirable and helpful in a relationship.

Some couples are using tracking technology already in there relationship. There are a few possibilities to do this via the smart phone. The Google Play Store and also the App Store form Apple offers some applications to locate a person, e.g. friends, a family member or the own children. To give an example, with the application called *Find my Friend* it is possible to locate another person which is also using the same application or (if the other person doesn't use a smart phone) with the agreement via a simple text message [10]. After agreement, the users can communicate and locate each other. One further option to track people who matter most is given via the operating system of the smart phone itself. Apple offers the service called Family Sharing [11]. With this service, the user can share the actual location with members in the family group, after the function called *location sharing* is turned on. Within the *Find my Friend* application the user can see all members in the family group, if they share there location too.

Another possibility to share a user's location with friends is the *Live Location feature* of WhatsApp[12]. With this function a user can share the location with friends for a period of time.

These three examples should only give an overview what today is in use. It is on no case completely. It only shows that technologies for location tracking are already available and in use.

4.4.2 With whom do people track their location?

In [4] Consolvo et al. investigated the willing disclosure of information from location-enhanced technology users to specific other people. In this study, 16 participants have given a social network consisting of people from their social networks. This network also includes the participants partner, in that work called *spouse/significant other*. They found out that for the willing disclosure for the user it is most important "[..] who was requesting, why the requester wanted the participants location, and what level of detail would be most useful to the requester.". The results also shows that "[...] who the requester was had the strongest influence on participants willings to disclosure.". If the partner, called *spouses/significant others* was requesting, the participants "[...] were willing to disclosure something for 93% of the 670 requests.". It can be concluded, that people use this technologies and are willing to disclosure informations about theirs location, activities and accompaniment. Further they give more details of information if the have an special relation to the requester.

4.4.3 Why do people track their location with others?

In the opinion by Ikrath [10] we are living in a change of values. THe present generation is non-solidarity and self-centered. Individual values are preferred over community values. As a result it could be possibly difficult, to have a relationship based on trust and other mutual values, how Danaher et al. already argue in [7].

Also the urge for control could also be a possible reason why people are tracking each other.

4.4.4 Does location tracking corrode the love?

It is questionable, if location tracking is helpful in a relationship. Engl et al. [12] actually working on an application with an concomitantly website for parters. The application should encourage the user to regularly invest time in successful discussions and to improve the communication in the relationship. In addition, the application gives specified tasks and configurable exercises for reflection and interaction, as well as for assessing the quality of the relationship. But the application will be implemented without an location tracking function.

Location traction in a relationship with digital techniques provides some risks regarding to privacy. In the following, the possible dangers are considered in more detail.

4.4.5 Abuse and revenge

Unfortunately, such technologies as discussed above can also be misused for other purposes. Freed et al. [9] conducted a study with 89 participants to show how abusers in intimate partner violence context exploit technologies to intimidate, threaten, monitor, impersonate, or harass their victims. They grouped the different types of attacks by abusers in four categories. A summary of these categories with examples is shown in figure 5.

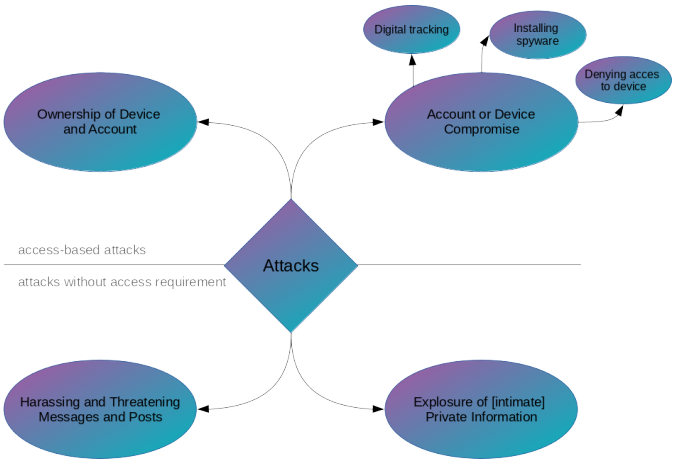

Figure 5. Summary of different types of attacks by abusers in intimate partner violence context [Visualization based on content from [9]].

In the following these four categories grouped by Freed et al. [9] are explained in more detail, focusing on intimate data, which the abuser accessed. Freed et al. found also other attacks (e.g. messages, posts in social networks and phone calls) to harm the victim, but that goes beyond the focus in this work.

Ownership of Device and Account Abuser and victim have or had an intimate relationship. This often includes a cohabitation or marital togetherness. In such a relationship with shared possession one of the partners commonly is taking responsibility for the couple finances. This fact leads to devices and accounts belonging to the abuser in these circumstances. The study showed that many participants (n=20) stated that their device (e.g. smart phone) was " [...] bought and paid [...]" by the abuser. With the ownership the abuser gained control about the different functions a provider offers to its customers. The abuser was able to control the victims digital accounts, e.g. received the phone bills and therefore knew detail facts about the usage behavior by the victim (including call history, text messages and voice mails), or "[...] exploit the data back-up services [...]" and get information or data, e.g. pictures saved on the victims smart phone. The abuser was also able to use the "[...] location-based services to track victims devices, including anti-theft services (e.g., 'Find My Phone'), parental tracking, and other safety-based services (e.g., Find My Friends') [...]".

[10]Find my Friends application: https://play.google.com/store/apps/details?id=com.fsp.android.friendlocator

[11]Apples Family Sharing: https://support.apple.com/en-us/HT201087

[12]Live Location feature of WhatsApp: https://faq.whatsapp.com/de/android/26000049/?lang=en

Account or Device Compromise If the abuser was not able to get access through the ownership of devices and accounts, there were also other ways to gain access. The study sowed that "[...] abusers are able to compromise victims' devices or accounts against their will and/or without their knowledge. Such compromises predominantly occurred via two routes: compelled password disclosure and remote compromise of accounts by guessing of victim passwords or the answers to password reset security questions.". If the abuser had access to the device and/or the account, it was no longer difficult to install software for spying the victim. The study also showed that the "[...] abuser were able to "hack" into victim accounts.". With the access gained by guess the password or compel password disclosure the "[...] abusers used their access to monitor, control, impersonate, or otherwise hurt their victims." [9].

Harassing and Threatening Messages and Posts Abuser used social networks to harm their victims. The victims were harass with messages or calls on the smart phone device. In addition, the networks were use to damage the victims' reputation. Therefore abuser contacted friends and family of the victims in order to negatively influence the friendship or to pursue their jealousy.

Exposure of Private Information Digital technologies offer abusers a way to harm their victims by disclosure private information to third parties or friends and social contacts. Freed et al. found that "The most common exposure-based threat [...] was exposure of intimate images (photos or videos) of victims, commonly known as non-consensual pornography or *"revenge porn"*[...].

Levy also wrote about the *revenge porn* as an possible risk in condition D in the life course of intimate relationships.

Tong surveyed in [26] "[...] how [...] individuals use Facebook as a from of surveillance." The survey showed that there were three dimensions for general social activity monitoring. The first was "[...] referred to looking at the ex's profile, photos, and status updates to see what the ex is doing." Second it was important to "[...] detecting an ex-partner's new romantic interests [...]", e. g. by checking the realtionship status of the ex-partner. The third dimension included "[...] direct statements made to, or by the ex-partner [...]. Compared to the results in the study from Freed et al. [9] mentioned above these three dimensions seems harmless and quite safely. However these activities are also kinds of surveillance the user which is monitored can not controlled. It is similarly to the research results in condition A 4.1.

In summary, partners in intimate relationships are increasingly discovering digital technology to harm their partner. Freed et al. [9] found that the attacks were technologically unsophisticated and often carried out by a *UI-bound adversary*.

5 Risks

Lupton wrote in [15] "[...] that mobile digital technologies that can be used for surveillance are part of everyday social life." Since the technologies discussed in 4 are in daily use, they pose some risks to the users privacy, the perception of themselves and also of their relationships. In this section some of these risks are summarized to give an overview. The overview is divided into three categories that are described in the following.

5.1 Quantification: Perception and rating of the self and the relationship

Due to the various ways in which intimate data can be tracked, there is a risk of losing the actual reference to the data [15] and [16].

In Condition B in 4.2 it was mentioned that by tracking of sexual activities the act itself is only perceived by numbers at a later time, thus the act is quantified. The quality and perception of scenes felt by the user can be lost. Or in other words, the user can be lost in a jumble of numbers [13]. When using these technologies, the user should be aware of why he or she is using them and what these data are actually collected for [7]. Often it is the case that many users are interested in tracking at the beginning, but after a while they gave up using the tracking device and are no long interested in [22].

In Condition C in 4.3 the tracking of the cycle and fertility of female users is described. Especially for the symptothermal method by Roetzer a digital device to support the measurement and evaluation of the measured values could be helpful. However, it is claimed that the analog measurement leads to better results. Regardless of this, there is also the possibility of losing in the tracked data and not paying attention to one's own body feeling.

The risk of being lost in data also applies to data obtained through mutual (location) tracking in relationships described in Condition D in 4.4. This kind of tracking also includes the risk that the focus is solely on the data and the trust on which relationships normally build up is lost. The fact that one knows the exactly location of the partner at every time can lead to wanting constant knowledge about the partners location. What is if the location data is not available once a time? This should be examined in future work. This also applies to applications in which advice and tips for the relationship are given in the form of notifications, e.g. by the Glow application mentioned in 4.3.2 It is questionable whether this type of support for the relationship is sustainable or whether it is influencing the self-questioning of the actual relationship status.

5.2 Trust: unknowingly and knowingly tracking by intimate partner; over-trust in data only

The surveillance of the partner without his consent is on the topic of QR-Technologien out of the discussion, as Danaher et al. in [7] argue. This is clearly the abuse of the data. This includes also the use of such apps as Flexispy [13].

However, the approach that partners voluntarily monitor each other as described in D could also create problems related to the use of such an app or tracking device. This includes for instance the abuse by a dominant partner that might force the use of such software in the relationship. That would not be mutual agreement.

> Many survivors were unaware that their location could be tracked using these services and asked us to teach them how to turn off location services on their phone. Professionals also described how survivors' lack of awareness regarding location tracking may result in potentially dangerous physical stalking [...]. [9].

> However, our research shows that technology-related abuse is already extremely prevalent in IPV. Therefore, we believe it is critically important to bring the details of these attacks to the attention of the computer security and privacy community.[9].

5.3 Privacy: Risks related to QR technologies

In Danaher et al. [6] the risks associated with the use of QR-technologies are summarized. The authors argued that the concerns " [...] of the privacy-invading elephant lurking in the room [...]" are not alone a problem of a single person, but also involves one or more persons, e.g. a person with which one is sharing knowledge about intimate facts like such in a relationship. In this case it is a exclusively private and an interpersonal matter. The decision whether and with what device QR technologies are used in a relationship depends on the person itself. As further concerns, they stated that users use applications on devices that are also used for other purposes, e.g. such devices as smart phones, and that these devices are connected to the Internet. They conclude their argument that it is not a single process of tracking the data, which leads to problems. Rather, the problem lies in the fact that third parties collect the data on the devices that track the data, and so they get the data within existing network connection.

A solution for this concern could be applications on devices which does not communicate with third parties servers via a network connection. This could be devices that only track the data the user want to quantify, without network connection, which lead to use an device in addition to the smart phone. Or, go a step backwards, the user can track that data completely whiteout digital technologies, e.g. as mentioned above with the symptothermal method model by Roetzer. Remedy would create devices that only track without transmitting the data.

[13] https://www.flexispy.com/en/

It used to be tracked without digital helpers, see **??** the symptothermal method model from Roetzer.

"We found that the typical vectors of remote account compromises are technical mundane. Frequently, abusers are able to use their knowledge of the victim's personal details to infer passwords or correctly answer their security questions and reset their password [...]" [9]

6 Discussion

- Privacy concerns: Tracking without digital devices? Das ist sehr schwer umzusetzten, wer schafft das schon? Digitale Helfer machen sinn
- Wann werden intime Daten intim? Wechel der Wahrnehmung und Umgebung
- user should be aware of why he or she is using them
- not enough awareness for data protection and data security. possible risks related to disclosure of intimate data
- over-trust in systems and quantification
- changed values $\mapsto$ monitoring as a standard in relationships?

7 Conclusion and future work

In this work, different conditions in a relationship were considered in which intimate data can be searched, collected tracked and shared. Further, an attempt was made to formulate a definition for the term *intimate data*. It also summarized how people perceive this data and how the data affects their perception.

The problem lies in the change in the conditions in everyday life. In a romantic relationship a lot of information is shared over time, even those that are very intimate. This is important for the well-being of the relationship, because the trust is based on such shared facts. But at the same time providing such important intimate information provides a point of attack and gives power to the partner. Nevertheless, this does not means that it is better to hide such intimate information in a romantic relationship and build up relationships based on superficial communication. Nevertheless it is sowed in several works, that abusing such intimate data and information is commonly used and possible. Due to this fact, more awareness for the own intimate data is needed, as well as the knowledge how to protect these data for abusing and disclosure, and how to protect oneself form being monitored by the partner or third parties.

Condition 4.4 includes considerations towards mutual voluntary surveillance in a romantic relationship. One fact by tracking the location of the partner constantly should be noticed in future works: It is questionable if the quantification of trust in romantic relationships is influencing the perception of the partners in the relationship, and in which way. Are location-based tracking device helpful for building trust in a relationship? How helpful are these informations for the partners.

References

[1] Jan Philipp Albrecht. "How the GDPR will change the world". In: *Eur. Data Prot. L. Rev.* 2 (2016), p. 287.

[2] S. Andrews. *The Glow App: Track your period, fertility and much more*. 2015. URL: https://weheartthis.com/wp-content/uploads/2015/06/Glow-App-review-screenshot-1.jpg.

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

[4] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. "Location Disclosure to Social Relations: Why, when, & What People Want to Share". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '05. Portland, Oregon, USA: ACM, 2005, pp. 81–90. ISBN: 1-58113-998-5. DOI: 10.1145/1054972.1054985. URL: http://doi.acm.org/10.1145/1054972.1054985.

[5] J. Danaher. *The Ethics of Intimate Surveillance (1)*. URL: https://algocracy.wordpress.com/2016/07/05/the-ethics-of-intimate-surveillance-1/.

[6] J. Danaher, S. Nyholm, and B. D. Earp. "The Benefits and Risks of Quantified Relationship Technologies: Response to Open Peer Commentaries on "The Quantified Relationship"". In: *The American Journal of Bioethics* 18.2 (2018). PMID: 29393778, W3–W6. DOI: 10.1080/15265161.2017.1422294. eprint: https://www.tandfonline.com/doi/pdf/10.1080/15265161.2017.1422294. URL: https://www.tandfonline.com/doi/abs/10.1080/15265161.2017.1422294.

[7] 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.

[8] Judith Duportail. "I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets". In: *The Guardian* (Sept. 2017). URL: https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold.

[9] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. ""A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology". In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. CHI '18. ACM. 2018. DOI: 10.1145/3173574.3174241.

[10] P. Ikrath. "Generation Ego". In: *Paediatr Paedolog Austria* 53.1 (), pp. 28 –31. ISSN: 0030-9338. DOI: 10.1007/s00608-017-0520-y.

[11] Bundesamt für Sicherheit in der Informationstechnik (BSI). *IT-Grundschutz - 4.3 Risiken bewerten*. German. visited on 25.05.2018. Bundesamt für 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.

[12] F. Thurmaier J. Engl. *Paaradiese - damit die Liebe bleibt - Partnerschafts-APP mit korrespondierender Website*. [2016]. URL: https://www.institutkom.de/forschung/forschung-app.html.

[13] Kevin Kelly. *The inevitable: understanding the 12 technological forces that will shape our future*. Penguin, 2017.

[14] 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.

[15] 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.

[16] Deborah Lupton. *The quantified self*. John Wiley & Sons, 2016.

[17] 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.

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

[19] Josef Roetzer. "Erweiterte Basaltemperaturmessung und Empfängnisregelung [Supplemented basal body temperature and regulation of conception]". In: *Archiv für Gynäkologie* 206.2 (1968), pp. 195–214.

[20] Josef Rötzer. "Zur Geschichte der Natürlichen Empfängnisregelung". In: *Referat gehalten am International Congress on Certainties and Doubts in Natural Family Planning Today, Mailand*. 1988, pp. 9–11.

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

[22] Mimmi Sjöklint, Ioanna D Constantiou, and Matthias Trier. "The complexities of self-tracking-An inquiry into user reactions and goal attainment". In: *Twenty-Third European Conference on Information Systems (ECIS)*. Münster: ECIS, 2015, p. 15. URL: https://balsa.man.poznan.pl/indico/event/44/contribution/36.

[23] 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.

[24] 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.

[25] 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.

[26] Stephanie Tong. "Facebook Use During Relationship Termination: Uncertainty Reduction and Surveillance". In: *Cyberpsychology, behavior and social networking* 16.11 (2013), 788–793. ISSN: 2152-2715. DOI: 10.1089/cyber.2012.0549.