The value of personal data
Trust and reputation within a chaotic network

Benjamin Heurich

DFG-Research Training Group 1681 'Privatheit (Privacy)' – University of Passau

Abstract. With so much information being processed and so many possibilities for surveillance, how can people expect privacy anymore? How do they want to see their privacy being protected? The question is not so much about how people want to have absolute control over their personal data, it is a question of whether something is recognized as personal and, more importantly, by whom. Privacy protection in Germany derives from Article 2 of the Basic Law: "Every person shall have the right to free development of his personality." To understand this correlation between privacy and identity it is necessary to have a close look at how people exercise this right in a digital society.

Keywords: Privacy, Personal Value, Communication, Privacy Paradox, Metadata, Identity Management, Non-Linear System, Systems Theory

1 Introduction

The analysis of privacy concerns goes back a long way. Dr. Alan Westin conducted over 30 privacy-related surveys between 1978 and 2004. He wanted to outline different areas and levels of concern about privacy. He conducted a *Privacy Index* to summarize trends in privacy concerns of today's society. He has surveyed the general level of privacy concern of the public and has also studied the attitudes about specific privacy-related topics such as confidence in organizations that handle personal information, acceptance of a national identification system, and use of medical records for research [1]. In one of his latest surveys, conducted in 2003, Westin came to the conclusion that "most people are 'Privacy Pragmatists' who, while concerned about privacy, will sometimes trade it off for other benefits"[3]. Although the term Pragmatists already gives a clear insight of what the main characteristics of this group consists of, I want to highlight the exact definition of this category[1]:

[1] Westin examined responses to several privacy-related questions, starting in 1990. He related general concern levels and privacy concern levels and divided the respondents into three different categories: the privacy *Fundamentalists*, the *Pragmatics* and the *Unconcerned*. [3]

> **The Pragmatic:** They weigh the benefits to them of various consumer opportunities and services, protections of public safety or enforcement of personal morality against the degree of intrusiveness of personal information sought and the increase in government power involved. They look to see what practical procedures for accuracy, challenge and correction of errors the business organization or government agency follows when consumer or citizen evaluations are involved. They believe that business organizations or government should "earn" the public's trust rather than assume automatically that they have it. And, where consumer matters are involved, they want the opportunity to decide whether to opt out of even non-evaluative uses of their personal information as in compilations of mailing lists. [3]

This definition describes a pragmatic behavior of a single person when it comes to the opportunity to opt out of a possible surveillance situation [22]. Similar to today's discourse, Westin also refers to privacy as something that is under a constant threat and something that has a social value [2], [24]. He only differentiates between different courses of action to deal with this rather negative position an individual finds itself in. This general and individualistic view does not accommodate the norms and structures of today's fast-paced and strongly interconnected digital society. On this note, privacy is a multidimensional construct that is simultaneously forming and adapting to multiple contexts [5]. It is highly flexible and keeps changing, depending on which perspective one chooses. Both individuals and institutions opt for trust and reputation at one another within this disperse and spaciously environment. Furthermore, privacy is regarded as a relational concept that is produced within the patterns of intersubjective social interaction [7], [14]. What makes it even more complicated to identify privacy concerns is the fact that individuals choose the identity on which they want to encounter digital communication [8].

Manifestations and variations of privacy are essential for modern societies and are deeply rooted in cultural structures and of vast importance in the way we are developing our identity in the social sphere. Notions of responsibility, autonomy, surveillance, authority, governmentality, self-determination and freedom cannot be fully analyzed without taking privacy into account [9], [24]. Right now, the concept of privacy faces radical transformations because technological progress shakes up its structure, hereby reconstructing all the aforementioned principles, as well. This paper focuses on information and data privacy. Concerns, in that matter, address the collection, usage and deletion of personally identifiably information. In this context, one of the few constants scientific approaches can work with is the increasing desire for convenient and advantageous technological features as a comprehensive support in today's social life [24]. The dilemma between competing demands to use information technologies and the need for security against potential threats to personal data is referred to as the *Privacy Paradox*: "Why do people share their personal information in such an improvident way while having ever-expanding security demands at the same time?" A clear distinction is inherent in this question which is of significant importance for the following argumentation: when this paper refers to data as *personal* it focuses on information that has been actively created and released by the individual. However, this does not mean that the individual consented to an objective

disclosure nor was it in any state of self-awareness of all the information necessary to make an informed decision. This definition excludes surveillance techniques and passive recordings (e.g. camera surveillance, GPS-tracking and audio beacon recordings). In this sense I want to follow Beate Rössler when she states that personal data has to be "connected to the intentions and self-chosen activities of the person concerned" [10]. It has to be clear, however, that I will not distinguish between a personal, social or common value of privacy that might be created as a result of a personal cost-benefit analysis [24].

In the following I will outline personal value arises from digital interaction. Chapter 3 addresses the characteristics and properties of interaction within social networking services as the main platform [6] for the type of this interaction. Before I come to my conclusion I will focus on the effectiveness of the internet's review system and its interconnected evaluation procedure.

2 Common perception and value of privacy

2.1 Protecting privacy in digital liberal societies

Although most people value privacy to some degree [24], the concept is still captured in a narrow way. Individuals do not recognize nor understand privacy harms to their fullest extend when they occur [22]; even more when it comes to the dimension of data control [4]. Thus, what can be done with personal data once it has been collected by a commercial or governmental institution lies far beyond any influence on personal behavior or future constructions of an individual's identity. This leads to the wrong impression that people do not care enough about the extent of their activities or interactions online. Instead, it should raise the question of what actually concerns individuals when they interact with each other in a digital social infrastructure [3].

Lawmakers are torn between new challenges regarding the protection of individuals using internet services and losing more and more control over their data on the one hand and economic demands for the creation of data markets and for a more flexible approach to data protection on the other hand. What makes it even more difficult is the fact that people are not able to articulate their expectations of what they want to see protected. Neither can each individual specify the exact value of personal information as a part of digital interaction [10].

Article 2 of the Basic Law in Germany, where privacy protection derives from, is titled: Personal Freedom. By law, the state has to guarantee the necessary autonomy and freedom an individual needs to shape and test personal identities and social roles [2], [17]. It classifies privacy protection in the course of self-determination as a human right. Brandeis described a right to privacy as "the most comprehensive of rights and the right most valued by civilized men" [23]. This task is highly complex and raises a lot of difficulties for the executive power in liberal societies [4], represented in Germany, for example. If nothing else it is because of the complex matter illustrated in the Privacy Paradox. It is a question of where the law has to exactly be put to work to ensure an adequate and intended amount of observations in a social context

without undermining the free and autonomous identity management of each member of society [4], [8], [10].

2.2 Digital Communication and identity management.

To understand, or even solve this dilemma, one has to look at the addressed issues from a certain perspective. This paper clearly focuses on the individual as a producer of data as a self-determined digital citizen whose willingness to share information online involves evaluating the outcome of online communication. Communication has to be understood as a constant and accessible feedback within an autopoietic system [12]. It is important to note that this does not presuppose that the individual is capable of understanding each output from a certain operation as information nor is it prepared to operate on what feedback might be given. It is only aware of what to expect from the observation by others since it is communicating in a well-known trans-subjective categories [5] using a carefully crafted identity.

While the need for protection and the attempt to act in accordance with social norms is a highly subjective act, the evaluation of communication and disclosed information only occurs within a social and public negotiation process [8], [14]. The existence of a designated recipient or data-controller is mandatory to adequately value processed information.

By all means, individual privacy protection is to be considered imperative, yet the emergence and omnipresence of the internet have made it even more necessary to focus on personal data as a social good produced by the digital day-to-day interaction. The proper use and the protection of this good is going to shape future societies since the internet has numerous and extensive benefits for each individual, group or institution; and they expand every day both in quantity and quality. It is a matter of interest in activities, opinions and interactions between individuals testing out digital social roles. Acquiring a vast variety of identities is what motivates the individual to spend their time on the internet chatting with friends or buying new clothes [8]. Moreover, it is a place where you can find a certain kind of *trust* from people you have never met and know nothing about.

2.3 Cost and benefit of digital social interaction

Internet users must determine the degree to which they want to participate in a digitalized social system and what they want in return. A classic framework used to understand this decision making, primarily from an economic perspective, is the *utility maximization theory*. It has been applied to consumer privacy in previous research to examine the market for privacy [1]. It is argued that utility maximization is difficult to apply to social actions and communication because there is no actual value in social exchange [16]. Another issue addresses the lack of a clear distinction between the values of one social exchange from another. I argue, however, that digitalized communication makes this evaluation possible. Namely, to the extent that a person can combine the used information and the time and energy spent on a certain act of communication to a form of investment or cost. The confronted benefit would be the ex-

pected result of this social act based on the opportunities and contingencies this act produces for a certain social system [11], [14]. As explained later on, this benefit evaluation has a lot to do with the quantity and quality of the observations of this social act. Moreover, it depends on the availability of an interconnected review system within a non-linear network. The internet has changed reality extensively in the recent past. It has produced a range of new means of communication, information and online services, which heavily influence our actions and thoughts, and thereby the life of the individual and society as a whole. The internet thus becomes a subject matter of the law and for the fundamental rights, which are expressed in the self-determination of the individual [23]. Whereas the benefits of the internet are widely recognized, its potential harm and danger for the individual are often overlooked. Big Data is used to profile a country, a region or a group of citizens. That means, in theory, each personal information is in itself as important as any other within that target area [25].

Everything mentioned has led to a point where personal data and the actual time spent on the internet has become more and more valuable; not only to businesses and institutions but most of all to the individual. Instead of asking "how should I spend my money in order to maximize utility" individuals are evaluating a certain *return on engagement* in the digitalized social sphere. Therefore, utility today is much more than spending money. It is the process of decision making and evaluating the personal information necessary before an individual clicks on a link or a button as a form of agreement. Also, benefit is derived through the degree of personalization received and cost is a function of consumer privacy concerns, previous privacy invasion experience, time-performance ratio, and hedonistic effects [1], [16]. Arguing that individual decision making in a digitalized social sphere follows an efficient cost-benefit equation [22], one still has to ask: What exactly does the individual take into account? To find an answer to this, it is necessary to have a close look at the regulations and rules of the platform on which personal data is generated and exchanged. Most of the theoretical conclusions of the following argumentation will derive from abstract concept of the Systems Theory of Niklas Luhmann [11], [12], [15].

3 Web 3.0 – input and output of personal data

Web 3.0 enables a more disperse and interactive Internet communication since modern technology allows a wide number of individuals to participate on multiple social platforms simultaneously (e.g. YouTube, Facebook, Twitter and fast-growing communities like Reddit). This kind of network communication breaks down geographical borders and negates any requirements for access and participation [7]. To express an opinion about a certain topic, people can simply watch a video and click on a button [25]. Although a click on a like- or share-button contributes to or even initializes a political operation, it is rarely recognized as a democratic act; nor is it motivated by just social responsibilities or intrinsic motivation where it might get nothing in return

except for a certain kind of relief.[2] In fact, it is opportunism, so called *e-fame* and an aspired edge in knowledge that all play a huge part in each individual's cost-benefit equation of social interaction [9]. Being present on social networking sites in pursuit of popularity or for the purpose of blogging about current topics does not mean an individual knows what to expect from each social interaction, but it is clearly aware of the observations since it is acting in a certain social role [14]. A networked social interaction helps individuals to co-produce their subjectivity with others [8]. This co-construction is closely linked to both identity and reputation of an individual. These people reflect and evaluate certain performances and start a feedback loop which contains information that can either be integrated or rejected by the type of identity they have chosen to portray themselves [2], [8], [17].

3.1 Communicating within the intended system

Many authors stretch out the necessity to focus on social interaction when it comes to a clear view on peoples need for privacy protection [5], [7] [8], [17]. It is quite clear that privacy has to be addressed in a social context rather than an intrinsic need or desire. Although it is always an individual at first who chooses to disclose personal information, privacy can only be adequately protected when the recipient of this information can be identified. How else would someone know that a communication process is compromised by someone or something that is not, in fact, the recipient or at least a part of its network? However, for this identification to be possible the information has to have left the state of intention to communicate itself. The sheer act of disclosure is completed and the authority over the information flow is out of reach for the individual [7]. I will go further and argue that it has gone forever. Not only is this personal information stored indefinitely, but it also can be a part of any metadata evaluation process in between two points in time from this moment on. These two specifications take the range of possible outcomes of this communicative act close to infinity [25]. So where is the connection to a personal value of this data for the individual and, to identify the need for protection, for any observer? The value for possible observers is easily identified, since it lies directly within the definition of metadata and its infinite use for future operations. Metadata is not information in itself. It is an atomic accumulation of bits containing a great number of data about data in a binary structure [25]. It can be compared and combined in any different order to fulfill a certain – not yet any – need for information about a person or a group of individuals.

It might have been this simple access to a value-paradigm of privacy that has led to so many theoretical approaches that are focused on privacy as something that needs to be protected from others; especially commercial usage and governmental surveillance. It is, of course, common sense that an individual does not want to live and be recognized as a transparent human being. It is always very concerned with keeping personal information as safe as possible. However, by not re-evaluating social norms and values in a digital context many approaches came to the false conclusion that the

[2] New institutional economics and current political events prevent me from drawing a more altruistic picture of a modern digital society.

excessive sharing of personal information is a form of uninformed consent or frivolous behavior. But to arrange a social model of privacy and to analyze the social value of personal data it is more important to know which information and – more importantly – under what circumstances it is considered to be personal. Not only does this view combine different micro-perspectives on privacy as a value in general, it also takes into account that protection is not so much a rigid concept as it is a flexible condition.

3.2 Identity management by matching expectations

It is crucial to understand how individuals evaluate their own personal data. The tendency in contemporary society to share private details online can be described as an obligation and eventually a merit because it represents an essential requirement to be considered an active part of the digital community. The continuous and time-consuming interaction with others on the internet and within a semantic, non-linear network symbolizes the creation and accentuation of numerous personal online images. These projections are very important for the success of future interactions [8]. Each digital act can be related to – at least one – of these images and is also always intended to do so. The sheer amount of personal data and the expenditure of time alone, however, does not state whether this perception is in line with reality or not. Social norms might help to create various identities, but they are not imperative when it comes to digital communication. Individuals interactively create and/or modify social norms; they unite in order to approach a nuisance or they coincide behavioral patterns to improve the chances of achieving a certain goal.

The latter can be observed when individuals want to enhance their chances to fill a valuable job. People spend a lot of time shaping their working-self by informing observing systems about its past career choices, personal strengths and weaknesses and work expectations. It has become a social norm to disclose this kind of personal information to the economic system online in order to enhance the possibility of a successful career and to sell one's labor to the highest bidder. Images, diction and conduct, all serve the purpose of making communication more possible by matching the expectations – or maxims – of the system the individual wants to communicate with, namely: honesty, accuracy and completeness. Although these expectations may vary from system to system, all of them have one expectation in common: transparency.

Subsystems of society observe communication in order to ensure their existence in the future [12]. It is obvious that the probability of existence increases with the amount of information it gathers, since contingency leads to additional ways to ensure future operations [13], [15]. Transparency enables more and more communication processes to be of use for a certain system just because it is able to observe it. It depends on the internal, autopoietic structure, however, how communication is processed. To pick up the example above: If a boss of a large company wants his or her organization, as a social system, to work properly he or she has to employ new workforce. The decision of which individual ensures continuing operations, however, is based on the information that very system receives from the environment [13], e.g. via a profile on a business-themed social networking service. This information is pro-

cessed by the internal structure of this company. It might search for several different variables, but in order to find the best employee it must be able to identify the most suitable working-self. It is a matter of self- and other-reference in which a system has to decide what enables future operations [11]. There is no single way to always make the best decision, but transparency makes this objective more likely to be successful, since it offers opportunity in form of contingency.

The semantic web combined with the global connectivity of today's internet meet this need for a transparent flow of information like never before. I would argue that the systemic structures of most of the subsystems have reached a point where it is useful to adapt to all sorts of communication processes just to obtain as many data as possible. You can already observe such comprehensive operational behavior in the political and economic system. The commodification of personal data is complete [9] and it will be even more valuable for companies in the future, since the cost of digital storage decreases and the value of personal data increases at the same time [25].

Apart from personal data being traded and moved from data controller to data controller in a rather horizontal way, the political system, however, provides a significant example of how vertical processes are also being restructured on the basis of the newly-created transparency.

3.3 Weakening established power structures

The operational process of the political system can be described as legitimized decision making [11], [13]. It is interested in public opinions and it needs a clear understanding of what people want in order to reduce complexity and channel social decision making for the members of society. The functional differentiation of the political systems uses the code *power/powerlessness* to identify information that makes future operations possible and effective [13]. The protection of privacy in that context is especially valuable since it maintains the integrity and legitimacy of a *democratic* political system [24]. A traditional way to reduce complexity was to focus on politics *behind closed doors*. Members of political parties were elected and statistics were created to substantiate certain decision making without any nameable involvement of the public. Today, this pattern of legitimization slowly decays, because, as mentioned above, the demand for transparency is apparent and society knows how to create it through the internet – mostly to their benefit.

The Web 3.0 offers numerous ways to exploit false information and untenable decision making processes by the political system. Several websites and communities made it their business to fact-check[3] critical information and to make them available to the public. The range of these observant control mechanisms varies from smaller websites like *factcheck.org*, which wants to "reduce the level of deception and confusion in U.S. politics[4], up to large non-profit organizations like *WikiLeaks* which aim

[3] The term fact-checking describes the ante- or post-hoc analysis of a non-fictional text for its factual correctness. The American Journalist Review mentions a "fact-check explosion" in 2004. (http://ajrarchive.org/Article.asp?id=4980 – accessed June 30th 2016)

[4] Statement on the website http://www.factcheck.org/about/our-mission

to promulgate large sets of political data sets and classified materials in order to encounter political structures on a macro level. I want to clarify, that it is not the purpose of this paper to make any statement about the work of these websites and communities. But it is important to note that their actions transformed traditional social norms and power structures by expanding the political discourse about legitimized legislative power to a much greater audience. Not only do they harm and weaken institutions or political personae, but they also strengthen each individuals standing in the decision making process – by adding them to the binary coded communication process based on the success media *power* [11], [13].

Individuals lose more and more trust in existing systemic processes with every *untrue fact*[5] they discover. In contrast, who is really able to reduce complexity for the individual, is the community. It helps to identify a more suitable *polity*-self within political actors which is able to ensure the desirable legitimized decision making process. Being part of a community that evaluates the processes of the political system means to review, like and share what the members of this social system do. Furthermore, each member works as a detector for privacy intrusions which leads to more safety within that group [7]. The connection to other people itself encourages individuals to be online and to share information with each other.

However, there are many other aspects that motivate individuals to communicate in the Web 3.0, apart from being an active member of a community to achieve a certain goal or to reach a superior position over established power structures. Below I will outline some of the main technical features and characteristics of today's online-communication to give a closer look on how mechanical procedures meet and trigger intrinsic impulses.

4 The social networking review system

4.1 Investment in a non-linear connection

Continuous operations in a social networking system are inconsistent, massive in number and sporadic. Due to immanent internet features, e.g. share, retweet and hashtags, one can no longer comprehend cause and effect within a chain of communication. The output of any information is disproportional to the input. Only a non-linear network like this can lead to a rather destructible force of opinions and solidarity called *shitstorm*. These waves of resentment originate, amongst other things, from the emergence of the above mentioned *untrue facts*. Such phenomena are well received by the individual as superiority over institutions, persons of public interests or other social systems in general. People have recognized the potency of these systematic features and gather actively in order to weaken traditional power structures such as in-transparency, asymmetrical information and market or price fixing.

---

[5] An *untrue fact* respectively stands for any information that is not able to ensure future operations in a social system. Thus, it was no information in the first place since it could not be observed [12].

However, shaming companies or other people's behavior is not the nearly comprehensive enough to explain the extensive and time-consuming use of online interaction on social networking services. E-commerce, social reputation and the review market in general are much more valuable when one has to evaluate an investment of personal data and time. Also, referring to Westin's definition above, it is a place where an individual finds itself in a very pragmatic context [4]. Past behavior and interactions are stored and evaluated by others. In asking and answering questions, writing detailed reviews and comments or participating in discursive topics, the personal reputation of an individual rises with every single social action. People tend to only participate in the kind of online communication that is appraisable, meaning it is connected to an internet feature that offers a cross-linked *reviewability*. If people like what they see, they have to (and also want to) express their affection within a short period of time before it disappears in a massive stream of continuous communication; especially if they want to still be a part of it in the near future. It epitomizes the pursuit of popularity and the need for a comprehensive online-image. Personal information is not only stored for marketing purposes or surveillance but also for the individuals own identity management [8]. The more an individual participates in an online discussion or a rating of any kind, the more it becomes a part of a larger group of interest and a more effective force of intelligence.

The review system of the internet is based on the aggregation of social activities and personal opinions. Likes, star-reviews or simply clicks in general, as a source of agreement, build up to a reputation for a single source of opinion and/or information which is highly accessible for algorithms and news-feeds. They refer to each other over an unlimited amount of time and benefit from each newly established network effect [12]. The review system intensifies the need for attention, because it works with symbols and words which have an objectively good connotation and is visible to others [9]. Only few of these systems work with negative feedback which is actually visible for internet users. One example is the *down-vote* feature on community websites like *Reddit*. These are not seen as actual votes, they only diminish already proceeded *up-votes* within that very same subsystem. There is, of course, the possibility for a comment or thread to be in negative voting-numbers, but these communication cycles cease to exist before they begin to produce value for a significant group of people.

Another example is the one-sided social communication structure of Facebook. This social networking service does not feature a dislike-button, and probably never will, since negative feedbacks work against any operational system that produces recommendations and suggestions. The newsfeed on a Facebook-user‘s timeline is a string of suggestions based on own past behavior, behavior and activities of friends and already disclosed information. Although a dislike-button would serve the same purpose as the share and hashtag feature on other social networking websites, it does not ensure Facebook's continuity. This button would only tell the Facebook algorithm to do nothing, since the act of not-liking something is already known by the system as ignoring it. From a systemic perspective, it is no information at all [11]. Therefore, *one-sided* means, that Facebook mainly works with people's confirmations. Saying *yes* to something in the digital sphere clearly states a wish or desire, whereas saying

no only excludes or postpones something. Facebook rather benefits from not giving an individual the chance of wasting a click on a fact that does very little for the definition of the personality; and defining digital personalities is the product of Facebook.

Personal data creates a value for the user of social networking services as well as for the service itself. However, these two evaluations cannot be more unlike. It became clear that individuals invest their time and data to achieve draw attention on their digital activities and to achieve some kind of superiority over other subsystems, whereas political or economic institutions just want to create a clear picture of a person's (or other institution's) decision making process to predict future behavior or to estimate potential resistance against instructions [9]. Individuals recognize surveillance mainly if their autonomy and freedom to charge their multiple identities with popularity, acknowledgment and attention is not fully provided and comprehensively ensured [5], [7]. Only within an already commenced communicative act can the individual raise a concern about an unwanted intrusion or defective information [14].

In addition to this rather active value in the act of communication itself, another dimension has to be taken into account, which is more directly connected to reality. The masses of the internet do not only interconnect in order to position themselves in a more advantageous way, they also work as a reputation system that has a huge influence on, not only online decisions, but also on social and economic activities in real life that cannot be underestimated in their reach and impact.

4.2 Weak ties in social media

A social action in real life can lead to an inter-systemic chain of communication through digitalization; yet detached from any expertise or even intention. Once a communicative act is performed, it can lead to an infinite number of *truths* in the future, since its information can always be understood differently [11], [14], [15]. For instance, because of his or her millions of followers on Twitter, a single celebrity in the entertainment business can have an immense inter-systemic impact on the economic system by tweeting about the purchase of a certain good or even a company share. In 2011, the rapper 50 Cent tweeted, that H & H Imports had "one of the 15 products this year. If you get in technically I work for you." In the following two days 9.24 million shares were traded, causing not only the share value to rise but it also generated a huge boost for a company was operating at a loss at this point[6]. Another example of the interconnectivity was a message from Mark Zuckerberg on New Year's Eve. He posted his 10 favorite books he is going to read this year. Within hours, these books were out of stock on amazon.com.

However, thinking of celebrities as a testimonial does not quite accommodate the magnitude of the effect of this interconnectivity on today's society. This functional integration [12] and the intersubjective extend of an individual's interaction in a social networking system, e.g. Twitter, YouTube, Reddit, are far more valuable than the imitation or impersonation of testimonials. It combines weak ties where communica-

[6] http://www.telegraph.co.uk/technology/twitter/8254618/Rapper-50-Cent-makes-10m-after-plugging-stock-on-Twitter.html (accessed July 2nd 2016)

tion is interconnected momentarily and without any reasonable understanding of other people's identities [18]. Hashtags, in that matter, symbolize a wave of opinions and statements assembled in one single voice. A Twitter user with millions of followers acts as a weak tie for each of these followers with a large degree[7]. This tie represents a bridge and is of so much significance, since its removal would cost the individual a vast amount of time to reach all the other followers. Interpersonal ties are defined as information-carrying connections between people [18]. However, the so called *sociological strains* are less crucial in weak ties, which means, that individuals spend less time and effort thinking about what other people related to someone you are communicating with think about a certain action [19]. Agreement and disagreement both stand behind the need for affirmation, the willingness to be a part of something big or the opportunity to save any sorts of expenditure. To find what they are looking for, individuals do not hesitate to use any personal tie they have access to, because they have developed a certain degree of trust in the interconnected and social communication. Mostly because communicative actions related to these connections have been successful in the past [13], [14]. It is not only a degree of trust but also a level of effort individuals had to put in to reach a certain goal. To spend more energy on something often means that you have done something wrong – or at least differently than before. This can be related to the fact that people are less and less willing to pay money for products of journalism or television.

An individual's online identity develops more and more access points for further communication [8], [17]. Furthermore, the time spent on the internet and the countless cost-benefit calculations which led to a certain action create a reputation in several different areas of social interaction [20]. Followers, links and likes increase the degree of trust by others. Analyzing an online profile related to a certain social action is one of the few ways to efficiently evaluate the quality of information within a non-linear and fast paced chain of communication. Being part of large communities and spending much time on supplying quality information and authentic interaction directly lead to a valuable social reputation throughout a huge group of people worldwide. The creation of followers and the gathering of all the different forms of agreements tend to result in transforming weak ties into strong ties with even more benefits for an individual's identity management [1]. A study conducted by the University of Chicago in 2010 showed that patterns of influence were much more likely to be demonstrated among close friends and network contacts, suggesting that strong ties in cyberspace are more likely than weak ties to influence behavior [1], [17].

---

[7] Granovetter defines a tie "as a local bridge of degree 'n', where n represents the shortest path between two points" [18]. Therefore, the larger the degree, the more significance the tie represents. For example, a weak tie between A and B with degree 7 means that, if this tie ceases to exist, A has to use a connection over 7 other ties to reach B again.

5 Conclusion – The problem with traditional operations

The internet is a chaotic network. Since the output is not directly proportional to the input you cannot foresee future operations by analyzing the actual state. The most important issue is the distribution of power and political deliberation. Most other systems, like the economic, education or policy system, however, work in a linear way. Internal operations are used to predict future operations and events by referring to statistical evaluation. Solove reflects on one of the main problem of today's privacy protection laws when he says "law does not deal with what is wrong today, it is focusing on shaping the future so things will not happen again" [21].

The internet is not a digital society within an already existing society. It is a new form of communication and interaction with a huge effect on traditional social norms and personal standards of that existing society [7]. The decisions and social actions, however, still originate from the same emotional and sensual human being. I argue, that the amount of participants and the immense interconnectivity of today's web-based communication assemble a framework of a global (digital) society. What makes it so difficult for other systems to find a link to this society is the representation and creation of different social norms and systematic momenta based on intercultural values and a new form of power. To adequately address a social system, observers have to fully understand what kind of feedback they can expect and under which circumstances an initiated act of communication is not perceived as disturbance or even harm. Long-term prognostics do not work in a non-linear system because of the chaotic interconnections. There is no link between input and output after an information has accessed the network. However, if the political system develops empathy it enables the possibility to react in time. Meaning, it could lead to an understanding of what determines social norms and maybe even the creation of these norms. To develop empathy means that political operations have to quietly observe, ensure freedom and autonomy and don't interrupt [9]. Nissenbaum speaks of the right to privacy as "a right to live in a world in which our expectations about the flow of personal information are, for the most part, met" [5]. Lawmakers tried their best to identify these expectations, but, like many other social subsystems, if not all, the political system has to admit that it has suffered a significant loss of power, before it can start to approach the digital society. Their role in today's digitalized society has to be restructured or even reinvented. These systems operate within a linear institutionalized power structure that tries to achieve a goal by analyzing a current state and then applying statistics, norms and regulations to that state. This competence is of no use anymore; it is now (more than ever) an interaction between self-reinforcing and non-linear systems [11], [12].

The economic system for example has struggled with many different situations in the past, because it refused to see individuals as personalities with different fluctuating identities. A customer is only a customer when he chooses to be one. The individual is not accessible for commercial communication if it is currently acting as a friend, relative or scholar. It did not take long until companies decided to take a step back and stopped chasing a significant Return on Investment for social media marketing, for instance. Instead, closer and more personal interaction and subliminal infor-

mation seemed to be the key. Although this was not a sufficient solution to the problem, this advancement did no harm to its own system; and society for that matter. But, the success of applications and workarounds like *adblocks* and *proxy servers* speaks for itself when it comes to the popularity of these forms of communication. Where there is resistance there is no acceptance; and therefore no systematic interconnection which would allow a valuable insight into people's behavior [6]. This paper will not come to the conclusion that there is a single way to connect each and every operation within the social system, so that (sub-)systems could develop a futile symbiosis and individuals would not have to worry about the misuse of their information. However, I want to close my argument by pointing out what it means to adequately address a digital society by using the right attitude to communicate.

In the beginning I pointed out that individuals allegedly are not able to identify and articulate their privacy concerns. It is important to note that the protection of privacy is most important when autonomy and freedom enables the kind social interaction I tried to accentuate above [2]. Not till then will an individual actively recognize harm to its privacy [5], [7], [14]. The success of communication depends on the ability to understand information correctly and to receive it in the right context [5], [12]. People need varying degrees of privacy protection based on their emotional and psychological development [20]. To truly understand how to adequately address these different, diversified and omnipresent concerns, other systems have to closely examine personal behavior and interactions and develop *empathy*. Individuals determine their own (digital) future, because they are closest to the social norms they trust and work with when they create, shape and test their vast amount of identities [8]. Basic operations of the economic or political system [12], i.e. statistics or investment appraisal, do not have access to personal motivation of the internet user at that exact moment a like-, share- or confirm-button is clicked. Moreover, even if statistics might be able to accurately predict the accumulation of likes or the probability of a purchase, the act itself has a different intention. The sharing of a newspaper article on Facebook is not supposed to work as a democratic act nor is a retweet of a brands picture considered to be a buying desire. It is a snapshot of the pluralistic character of human subjectivity [7] and a fragile composition of interest, emotion and desire [15], [17]. Most of all, it is a need for attention and an attempt to shape and accentuate digital identities. Privacy related concerns only exist if individuals realize that their information has been received by someone who was not intended to have it or if the debate is compromised with institutional or commercial intent [6]. Although this behavior might be characterized as *pragmatic*, I disagree with Westin when he says that individuals "weigh the benefits to them of various consumer opportunities and services" [2], [3]. They are just not able to outline the exact amount and quality of each opportunity, although they are clearly aware of their existence. Westin's and other statements, e.g. Privacy Paradox, testify for a discomfort when social systems have to deal with self-reinforced dynamics, because they are hard to explain and even harder, if not impossible, to foresee. The two allegedly opposed dimensions mentioned in the Privacy Paradox, disclosure of personal information and the demand for security, actually one and the same; it is just a form of misunderstood communication. Individuals mean to say "let my information go" and institutions watch them go.

6 References

1. Kumaraguru, P., Cranor, L.F.: Privacy Indexes: A Survey of Westin's Studies. Tech. rep. CMU-ISRI-5-138, Institute for Software Research International (ISRI), Carnegie Mellon University (2005)
2. Steeves, V.: Reclaiming the Social Value of Privacy. In: Kerr, I., Steeves, V., Lucock, C. (eds) Lessons from the Identity Trail. pp. 191-208. Oxford University Press, Oxford (2008)
3. Westin, A.F.: Social and Political Dimensions of Privacy. In: Bettencourt A. (ed) J. Soc. Issues 59(2), pp. 431-453. (2003)
4. Westin, A.F.: Privacy and Freedom. Anatheum Press, New York, (1967)
5. Nissenbaum, H.: Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, Stanford (2009)
6. Nissenbaum, H.: Respect for Context as a Benchmark for Privacy Online: What It Is and Isn't. In: Roessler, B., Mokrosinska, D. (eds) Social Dimensions of Privacy, pp. 278-302. Cambridge University Press, Cambridge (2015)
7. Parsons, C., Bennett, C., Molnar, A.: Privacy, Surveillance, and the Democratic Potential of the Social Web. In: Roessler, B., Mokrosinska, D. (eds) Social Dimensions of Privacy, pp. 202-222. Cambridge University Press, Cambridge (2015)
8. Steeves, V.: Privacy, Sociality and the Failure of Regulation: Lessons learned from Young Canadians' Online Experiences. In: Roessler, B., Mokrosinska, D. (eds) Social Dimensions of Privacy, pp. 244-260. Cambridge University Press, Cambridge (2015)
9. Roessler, B.: The Value of Privacy. Cambridge University Press, Cambridge (2005)
10. Rössler, B.: Should Personal Data Be a Tradable Good? On the Moral Limits of Markets in Privacy. In: Roessler, B., Mokrosinska, D. (eds) Social Dimensions of Privacy, pp. 141-161. Cambridge University Press, Cambridge (2015)
11. Luhmann, N.: Introduction to Systems Theory. Polity, Cambridge (2013)
12. Luhmann, N.: Soziale Systeme: Grundriß einer allgemeinen Theorie. Suhrkamp, Frankfurt am Main (1984); Engl. transl: Social Systems. Stanford University Press, Stanford (1995)
13. Luhmann, N.: Beobachtungen der Moderne. Westdeutscher Verlag, Opladen (1991)
14. Habermas, J.: Theory of Communicative Action 1: Reason and the Rationalization of Society. McCarthy, T.A. (transl.) Beacon Press, Boston (1984) [1981]
15. Habermas, J.: Theory of Communicative Action 2: Lifeworld and System: A Critique of Functionalist Reason. McCarthy, T.A. (transl.) Beacon Press, Boston (1987) [1981]
16. Blau, P.M.: Exchange and Power in Social Life. Transaction Publishers. New Brunswick (1986)
17. Mead, G.H.: Mind, Self & Society. University of Chicago Press, Chicago (1935)
18. Granovetter, M.: The Strength of Weak Ties: A Network Theory Revisited. In: Abbott, A. (ed) Am. J Sociol. 78(6), 1360-1380. University of Chicago Press, Chicago (1973)

19. Heider, F.: The Psychology of Interpersonal Relations. Wiley, New York (1958)
20. Kasper, D.: Privacy as a Social Good. In: Legerski, E.M. (ed) Social Though & Research 28, 165-188. (2007) http://dx.doi.org/10.17161/STR.1808.5227
21. Solove, D.J.: The Meaning and Value of Privacy. In: Roessler, B., Mokrosinska, D. (eds) Social Dimensions of Privacy, pp. 71-81. Cambridge University Press, Cambridge (2015)
22. Solove, D. J.: Conceptualizing privacy. California Law Review 90(4), 1087–1156. (2002)
23. Warren, S., Brandeis, L.: The Right to Privacy. Harvard Law Review 4(5), (1890)
24. Regan, P.M.: Privacy and the Common Good: Revisited. In: Roessler, B., Mokrosinska, D. (eds) Social Dimensions of Privacy, pp. 50-70. Cambridge University Press, Cambridge (2015)
25. Mayer-Schönberger, V., Coukier, K.: Big Data: A Revolution that Will Transform how We Live, Work, and Think. Houghton-Mifflin-Harcourt, New York (2013)