CORPORATE RESPONSIBILITY IN THE TELECOM SECTOR

Privacy Matters

Privacy Matters

Why Digital Telecommunication Companies Should Protect their Customer's Privacy

Ute Wiemer and Katharina Elkhanova

Keywords

Privacy Protection, Unique Value Proposition, Autonomy, Digital Telecommunication Sector, Threema, ZenMate

This paper provides an ethical as well as a strategic foundation for the protection of privacy as a unique value in the telecommunication sector. We provide a detailed definition of the term privacy, also taking into account its origins. Based on a specified definition of privacy for the digital telecommunication sector, relevant sources of conflicts and trade-offs are pointed out. Next, we focus on the ethical legitimation of privacy and show that it is a necessary condition for the autonomy of individuals. By analysing different concepts of autonomy, we highlight why autonomy and, therefore privacy are worth protecting. From this, we derive normative implications for the telecommunication sector. After proving that there is a moral obligation for companies to protect their customers' privacy, we will show that it is also economically and strategically recommendable for companies to do so. We identify several explicit strategic implications for companies to implement privacy in the existing framework. Lastly, we examine two practical examples of communication companies that successfully use privacy as a unique value proposition and evaluate them.

ute.wiemer@biomail.de
s3kaelkh@stmail.uni-bayreuth.de

1. Introduction

Imagine that the mailman who delivers mail to your home would open every single letter addressed to you, scan, evaluate, and store it, and then possibly sell the information it includes before he closes it again and delivers it to your door without you noticing the process. What appears to be a crime when it comes to paper-based mail delivered by the post office is daily business when it comes to electronic mail sent via email providers. Modern cyber technology makes it possible to collect, save and evaluate enormous amounts of information. Companies use this possibility to learn more about their (potential) customers and by doing so aim to increase their profits. However, data collecting has reached a dimension that users of digital communication products start to recognise as a threat and an intrusion to their privacy. More than 55% of German Internet users are convinced that their personal data is unsafe or very unsafe on the Internet, while 43% feel threatened by potential misuse and surveillance of their personal data (cf. BITKOM: 22, 28). According to research from ComRes, 79% of the 10,354 people interviewed from nine different countries (Brazil, United Kingdom, Germany, France, Spain, India, Japan, South Korea and Australia) expressed concerns about their privacy on the Internet (cf. ZenMate internal documents).

Arguments against violations of privacy usually conclude that for moral reasons, companies should accept a loss in revenue and an increase in costs in order not to violate their customers' privacy. We will, however, show that privacy protection is a highly underestimated market gap. Based on this thesis, we develop strategies to implement privacy as a unique value proposition (UVP) that companies in the digital telecommunication sector can use as a strategic competitive advantage. One of the very few existing definitions of digital communication is as "any electronic transmission of information that has been encoded digitally and is stored and processed by computers" (The free dictionary 2014: 1). Since this definition is far too broad for our purposes, we focus on digital telecommunication. The main difference between digital and analogue communication is that digital communication, unlike analogue, uses digital media like PCs or smartphones as a communication channel (Grimm 2005: 1). We concentrate especially on communication via e-mail, SMS, chat and similar communication types via digital devices such as smartphones or PCs. We will focus on with the business-to-customer relation, and exclude external actors, such as governments.

First, we develop a detailed definition of the term privacy, also taking into account its origins. Based on a specified definition of privacy for the sector, relevant sources of conflicts and trade-offs

are pointed out. Next, we focus on the ethical legitimation of privacy and show that it is a necessary condition for the autonomy of individuals. By analysing different concepts of autonomy, we highlight why autonomy and, therefore privacy, have a unique value that should be protected. From this, we derive normative implications for the telecommunication sector. After proving that there is a moral obligation for companies to protect their customers' privacy, we will show that it is also economically and strategically recommendable for companies to do so and therefore translate the ethical value of privacy into a value proposition that can be measured with economic means. We provide several explicit strategic implications for companies to implement privacy in the existing framework. Lastly, we examine two practical examples of communication companies that successfully use privacy as a UVP.

2. How to Define Privacy

2.1 Concept of Privacy

In this chapter, we will approach the concept of privacy, point out its complex dimensions and work out a definition of informational privacy according to the Restricted Access/Limited Control Theory for the scope of this paper. We point out the specific dimensions of privacy in the field of digital telecommunication and identify three main sources of conflict caused by trade-off effects between customers' informational privacy and other claims and values leading towards companies' primary goal of profit maximisation.

What does it mean for something to be private? As Young humorously pointed out, "privacy, like an elephant, is (…) more readily recognized than described" (Young 1987: 2). Defining privacy is challenging: The concept is interpreted differently in various contexts and cultures[1], and it has been changing rapidly, especially since the Internet has added new dimensions to it. One of the earliest definitions of privacy was made by Warren and Brandeis in the 19th century. According to the authors, the right to privacy is defined as "the right to be let alone" (Brandeis/Warren 1890: 1) in the sense of being physically alone. However, this definition does not seem to adequately address today's dimensions of privacy. When browsing the Internet, your privacy can be violated

1 As an analysis about the specific cultural and contextual differences regarding privacy would go beyond the scope of the paper, we will look at privacy from a Western perspective. For further reading, we recommend Moor (1997: 215-227).

even though you are physically alone; for example, your privacy is invaded if the Internet provider saves your browsing history or if your emails are collected and evaluated by a non-recipient. The same is true for speaking on the phone: You can be physically alone, but not experience privacy, for example when you are being spied on or if someone calls who you did not share your phone number with. Since privacy is often given up voluntarily to some degree, it is particularly hard to identify its exact scope. Sharing personal information on Facebook does not necessarily violate your privacy. If, however, someone shares personal data about someone else on Facebook against her will, that second person's privacy is most likely violated.

Privacy is a complex concept that describes things, places and situations, but also decisions and actions. Rössler distinguishes between three types of privacy, each based on a different aspect of the concept: Informational privacy, decisional privacy and spatial privacy. Informational privacy is about restricting other people's access to an individual's personal data that she does not want to share. Decisional privacy is concerned with a person's decisions and actions that she does not want to be influenced in. Spatial privacy means the literal local restriction of access by others, for example to a person's private rooms (cf. Rössler 2001: 25).

Various approaches to defining those different dimensions of privacy have been made since Warren and Brandeis first offered their conception of (spatial) privacy as a matter of physical aloneness. Almost all of them have been accused of being either too wide or too narrow or both,[2] which is why no commonly agreed upon definition of privacy exists. Some approaches are based on the aspect of control and define privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Rössler 2001: 22). Others define privacy as a matter of access: There are public areas of an individual's life and private ones, such as the body, the home or the thoughts and opinions. The individual decides which parties gain access to the private areas of her life. Other approaches contrast privacy versus the public and define everything that belongs to the sphere of the home and the house as private (cf. Rössler 2001: 20 et seq.). Since questions of privacy that arise when dealing with digital telecommunication are usually about people's personal information, the focus of this paper lies on informational privacy.

2 For an overview of different approaches to privacy and criticism towards it, see Rössler (2001: 20-23).

2.2 Restricted Access/Limited Control – an Approach to Informational Privacy

Among the variety of conceptions of informational privacy, we picked the one that we think suits our aim of analysing privacy in the digital telecommunication sector best: the Restricted Access/Limited Control (RALC) definition as introduced by Moor and Tavani in 2001. It combines aspects of a control-based and an access-based approach to privacy. It "distinguishes between the concept of privacy, which it defines in terms of restricted access, and the management of privacy, which is achieved via a system of limited controls for individuals" (Himma/Tavani 2008: 144). This recognises the fact that an individual should be able to protect her privacy actively in some situations (Limited Control) and be passively protected from violations towards her privacy by others (Restricted Access). The notion of limited control involves "choice, consent, and correction" (Himma/Tavani 2008: 145). For example, a person can choose whether or not it is acceptable for her to share pictures of herself in a bikini in a social network. Revealing information voluntarily therefore does not mean a violation of privacy in the RALC framework. This can be done using the consent process, which is supposed to ensure that the act of revealing is actually done voluntarily. Moreover, the correction process is important, because "it enables individuals to access their information with an ability to amend it if necessary" (Himma/Tavani 2008: 145). For example, in order to be capable of managing her privacy, a person should be able to retract pictures that she shared in a social network if she wishes to. "So, in the RALC scheme, individuals can manage their privacy via these kinds of limited controls and thus do not need to have absolute or total control over all of their information" (Himma/Tavani 2008: 145) in order to be private.

According to the RALC definition, a person has privacy in a specific situation with regard to other people if in that situation, she "is protected from intrusion, interference, and information access by others" (Moor 1997: 30). The notion of restricted access implies that there are certain situations in which an individual should be normatively protected from intrusions to her privacy. If a doctor looks at her patient's medical records, that patient's privacy is not violated, because the situation is "naturally private" (Himma/Tavani 2008: 144). If, however, the patient's email provider collects and evaluates an email from her doctor including her medical records, her privacy has been violated. According to RALC, the second situation is "normatively private" (Himma/Tavani 2008: 144) and requires protection in order to guarantee informational privacy.

2.3 Informational Privacy in the Digital Telecommunication Sector

The rise of technological innovation has provided fertile ground for new communication devices. Smartphones and tablet PCs are only a small part of the communication equipment regularly used by a large number of consumers. Most modern communication devices are constantly connected to the Internet. Through data which consumers disclose during communication and transaction processes, new profit-creating opportunities for firms arise through the possibility of massive data analysis, which will be analysed in chapter four. At the same time, studies like the ones mentioned in the introduction show that customers are concerned about their privacy and have an interest in protecting it.

As data security leads directly to privacy protection when it comes to digital telecommunication, it seems that competing interests and trade-off effects exist between privacy and other claims and values leading towards profit maximisation. "Consumer privacy can be viewed in the context of any interaction, profit or non-profit, between marketer and consumer" (Goodwin 1991: 150); examples of this include surveillance, transactions, marketer-initiated surveys and the collection and evaluation of customers' data. When deciding whether to disclose personal information, consumers usually differentiate between sensitive and insensitive data. Sensitive data includes among others financial data, e.g. credit card information, as well as communication content such as emails or conversations. Demographic and certain kinds of lifestyle data are rather insensitive and therefore cause fewer privacy concerns (cf. Phelps et al. 2000: 33). With regard to digital telecommunication, a customer can see a threat in the misuse of her personal data by communication companies in the following areas: control over how her data is used, what length of time her data is stored and used, where the data is stored, how her data is transferred, who uses the data, and why the data is being used (cf. Bodorik/Jutla 2003: 470). Different technologies used in these areas, such as data mining, surveillance technologies, data collection and evaluation technologies, provide a potential threat to the privacy of users of digital telecommunication products. We have identified three main sources of conflicts resulting from trade-off effects that communication companies and, in many situations their customers as well, have to consider between privacy and other claims and values.

1. Privacy vs. usability and quality: Companies collect data in order to enhance their products' usability and quality and develop new devices and services in order to be able to compete with other providers. On the one hand, customers' informational privacy is often violated

when companies collect and evaluate sensitive data. On the other hand, customers profit from product improvement and would often rather accept violations of their privacy than not be able to use certain products.

2. Privacy vs. cost efficiency: By collecting relevant information, companies try to cut costs, for example in the fields of marketing, advertising, customer relation management or R&D. Often they do this in a way that threatens customers' privacy.
3. Privacy vs. revenue increase: The better a company knows its (potential) customers, the more easily it can increase its revenue by gaining new customers or by increasing after-sales service and customer loyalty. The information required is often sensitive, and the collection and evaluation processes provide a threat to informational privacy.

3. Ethical Valuation of Privacy

3.1 Concepts of Autonomy

In this chapter, we look at informational privacy from an ethical point of view, show how it is valuable and why there is a moral obligation to protect it. Most arguments for privacy in recent political debates follow the liberal tradition of connecting it with autonomy. In order to understand the complex relation between autonomy and privacy, we will first give a brief overview of the meaning of autonomy and then show how it gives privacy its instrumental value.

The use of the term autonomy in philosophical arguments "is generally understood to refer to the capacity to be one's own person, to live one's life according to reasons and motives that are taken as one's own and not the product of manipulative or distorting external forces" (Christman 2003: 1). Berlin's distinction between negative and positive freedom is useful to point out the specific characteristics of autonomy. While negative freedom merely describes the absence of constraints or barriers that could prevent an individual from doing or becoming something, positive freedom or autonomy includes much more. An individual is autonomous if she is self-governing and able to live her life according to her own wishes and independent decisions (cf. Berlin 1990: 131 et seq.). But which conditions have to be fulfilled in order to ensure that an individual is self-governing? Various, often conflicting answers to this question have been given in philosophical discourse since Enlightenment humanism, a movement in the 17th century focusing on reason rather than

tradition, first put moral weight on the individual's capability to govern herself regardless of her social role or status. A basic distinction among those answers and interpretations can be made between moral autonomy and personal autonomy. Moral autonomy refers to an individual's capacity to apply the objective moral law to her and to act rationally and independently according to it. According to Kant who based his moral theory on the concept of autonomy, it is a capacity all rational agents, i.e. all humans, have. In the framework of Kant's moral philosophy, it is autonomy that enables humans to act morally (cf. Kant 1785: 74 et seq.). The focus of this paper, however, lies on personal autonomy, as it provides the ground for the instrumental justification of privacy discussed later. Personal autonomy focuses on moral obligations, but also defines autonomy as a quality that individuals can show in every aspect of their lives (cf. Christman 2003: 2). It goes back to Mill who emphasises the importance of personal autonomy as "one of the elements of well-being" (Mill 1859: 182), because it supports the development of an individual's character and enables her to pursue her preferences and her individual concept of the good life. Consequently, it leads to an overall maximisation of utility (cf. Mill 1859: 132 et seq.). As Berlin points out, Mill's central arguments are founded on "his passionate belief that men are made human by their capacity for choice" (Berlin 1991: 34) and their ability to decide autonomously. This also includes the ability for self-improvement through acting incorrectly and making mistakes. To be autonomous in the sense of personal autonomy means to be self-governing (cf. Buss 2013: 1). This stresses the value of self-integration: "We don't want to be alien to, or at war with, ourselves; and it seems that when our intentions are not under our own control, we suffer from self-alienation" (Buss 2013: 1). In order to govern herself, an individual must be guaranteed external factors such as a sphere of privacy in which she can act without interference and the satisfaction of basic needs. Additionally, she needs to fulfil competency conditions such as rational thought or self-control as well as authenticity conditions (cf. Christman 2003: 4). The latter ones are central to recent interpretations of autonomy, which have added psychological concepts to the debate in order to explain what makes a person self-governing. These interpretations emphasise the individual's ability for self-reflection and claim that "autonomy requires second-order identification with first-order desires" (Christman 2003: 4). A person in this sense is authentic and therefore able to act autonomously if she is able to identify with and reflect her wishes and desires. Her actions then derive from her essential character. Christman points out that the developing process of wishes and intentions is relevant for autonomous action and "focuses on the personal history of the agent as an element of her autonomy" (Christman 2003: 5). Rössler combines different elements of these concept and

develops three necessary and sufficient conditions for autonomy. According to her, an individual acts autono¬mously if (1) she acts authentically, (2) her decisions have a plausible history that rules out manipulation and self-betrayal and (3) the person is capable of developing and stating individual intentions and goals (cf. Rössler 2001: 109 et seq.).

There is no commonly agreed-upon definition of personal autonomy. However, it has become clear that autonomy has some kind of basic value that is worth protecting. There is reason why most modern Western legal systems impose prison sentences and therefore a loss of autonomy on convicts as the most serious punishment: Autonomy has a central meaning in an individual's life and is usually not given up voluntarily.

3.2 Privacy as a Condition for Personal Autonomy

As Solove points out, "privacy is an issue of power; it affects how people behave, their choices, and their actions" (Solove 2002: 1143). But where exactly does its value lie? According to some philosophers, privacy has an intrinsic value that is found in "a form of respect that must be provided to all rational beings" (Solove 2002: 1145). However, for the purpose of this paper, it seems insufficient to assign intrinsic value to a concept that is as hard to grasp as the concept of privacy and that has no agreed upon definition. Therefore, it makes sense to understand privacy as instrumentally valuable and connected to an end. While there have been many different approaches to define that end,[3] it is an idea from the tradition of liberal philosophy that can most frequently be found in current debates about privacy in media and politics: the idea that the value of privacy lies in its connection with autonomy. It goes back to Mill who, in his essay On Liberty, explains why individuals need to have a sphere of privacy in order to act autonomously. In this sphere, the individual is able to make decisions without the interference of society or the public. Mill states that this sphere "is the appropriate region of human liberty". (Mill 1859: 142). Autonomy here provides the ends for and the normative element of privacy.

Kupfer provides a psychological approach to the connection between privacy and autonomy, which is especially relevant for this paper as studies about consumers' behaviour will be analysed later in order to understand how and to what degree privacy is valued by individuals (cf. Kupfer 1987: 80 et seq.). He agrees with Mill's basic idea of privacy as a necessary condition for autonomy

3 For an overview of different approaches to privacy and criticism towards it, we recommend: (Rössler 2001: 20 et seq.).

and argues that "autonomy requires a conception of self for which privacy is indispensable" (Kupfer 1987: 81). Even though autonomy seems to depend on a number of factors such as intelligence or the satisfaction of basic needs, privacy seems to be a central condition for autonomy. According to Kupfer, this is because autonomy is connected to the notion of the individual's autonomous self-concept, which means that she conceives of herself as a responsible, self-governing agent that acts autonomously. So how do we develop this autonomous self-concept? First of all, we need to be sure of the social boundaries of the self. We must have control over our movements, over who interacts with us, who is involved in intimate relationships with us and who gets information about us. Privacy provides individuals with control over their social boundaries and therefore contributes to the development of their autonomous self-concept. Growing up, children learn to control information about themselves, for example by keeping secrets, finding places to be alone or even by lying, and therefore develop an understanding of their autonomous self. In contrast, if privacy is systematically taken from individuals, for example in institutions such as prisons or nursing homes, their autonomous self-concept is violated and their autonomy is diminished. This can lead to unnatural and destructive behaviour such as enuresis. But privacy is not only necessary to develop an autonomous self-concept in the first place; it also enables self-examination, self-reflection and self-criticism and therefore a sort of control over the self-concept. Privacy protects individuals from "others both as intrusion and distraction" (Kupfer 1987: 84) and gives them a sphere where they can try out their thinking and acting, make mistakes and take risks without facing public humiliation and judgment through others. Privacy, therefore, also enables an individual to think of herself as trustworthy: "By providing opportunities for failure or wrong-doing, society indicates confidence in the individual's exercise of autonomy" (Kupfer 1987: 84). In contrast, monitoring, observing and data collection question the trustworthiness of individuals and therefore violate their self-worth (cf. Kupfer 1987: 85).

But to what degree does violating a person's informational privacy mean explicitly violating their autonomy? Rössler argues that privacy violations such as data collection, surveillance and observation change a person's behaviour in a way that makes her less autonomous, because her impression of being observed constantly has an impact on how she acts (cf. Rössler 2001: 206 et seq.). Therefore, violating a person's informational privacy prevents her from fulfilling Rössler's second condition for autonomy, which states that a person's decision must have a genesis that rules out manipulation (cf. Rössler 2001: 125, 153). Similar to Mill's idea, informational privacy in this sense is a necessary condition for autonomy and is therefore valuable. It is worth protecting because

the information others obtain about a person can violate her ability to pursue her individual conception of a good life and can prevent her from making autonomous decisions. One could criticise Rössler's argument by saying that not every case of violating informational privacy directly violates autonomy in a way that is relevant. Collecting and evaluating people's private emails, for example, is usually only used by the email provider to match advertising or certain features of the email service provided exactly to a person's individual needs and tastes which does not necessarily violate her autonomy. But even though it may be impossible to draw the line between those violations of informational privacy that violate autonomy in a relevant way and those that only have a tolerable impact on autonomy, studies as the one presented in chapter one show that many people using digital telecommunication products feel seriously violated in their privacy. Individuals are often not protected from access by others in situations that are normatively private, and they frequently lose control over their private information in the sense of the RALC theory as they are not able to manage their informational privacy. The constant and systematic violation of informational privacy that individuals face in today's society eventually leads to modified acting and thinking and this to a certain extent deprives individuals of their personal autonomy. Data collecting, surveillance and monitoring activities of communication companies have reached a dimension that leads to a violation of individuals' private spheres of action as described by Mill. As Cohen points out, informational privacy should be valued and protected, because it "is an essential building block for the kind of individuality, and the kind of society, that we say we value" (Cohen 2000: 1435).

3.3 Normative Implications for the Digital Telecommunication Sector

From an ethical perspective, companies in the telecommunication sector are morally obliged to protect their customers' privacy in order not to violate their autonomy. The RALC framework offers useful suggestions on how to implement this. Every telecommunication company should protect customers' informational privacy in normatively private situations (restricted access) as well as enable them to manage their privacy (limited control). When it comes to deciding which elements of informational privacy are relevant for their customers' autonomy, it makes sense to use the choice, consent and correction process as suggested by the RALC theory and let customers themselves decide what kind of information they are willing to share in which situation and at what time. This rules out secretly selling information about customers, collecting, saving or evaluating data without customer approval or secretly tracking customers' behaviour.

Many companies argue that their customers explicitly agree to their activities by signing the terms and conditions and that their actions of violating informational privacy are therefore legally and ethically justified. This is, however, questionable, because customers are often not aware of the real content of the terms and conditions due to transparency issues, lack of background knowledge, or lack of time. In addition, they often lack relevant alternatives: Either they agree to the terms and conditions, or they cannot use certain channels of communication at all. How can companies be sure that they are acting in an ethically correct manner when it comes to dealing with customers' informational privacy? We suggest two strategies companies can use in order to ensure their customers' privacy.

For the first suggestion, we transfer the concept of informed consent, which originates from medical ethics, to the discussion about privacy. In medical ethics, informed consent describes a process of doctor-patient interaction in which the patient gives her permission for a certain healthcare intervention such as a specific procedure. During this process, the patient needs to be informed thoroughly and must gain a clear understanding of the circumstances, alternatives and consequences of her decision. She must also have the capacity to decide adequately and know about all relevant facts at the time she gives her consent (cf. Faden 1986: 36 et seq.). The result is an individual who is an autonomous decision maker. Communication companies should aim for the same kind of process when they ask for their customers' consent to use their private information. This means that the customer must have a thorough knowledge of how her informational privacy is influenced by the company's activities, of the alternatives and consequences of her consent and of all relevant facts. She should then be able to choose in which situations she gives her informed consent to disclose personal information. This fulfils two criteria for informational privacy suggested by the RALC framework: choice and consent. It is the company's responsibility to provide her with this knowledge and to make sure that she is capable of making autonomous choices. This might not be the case if the customer is underage or if there are simply no relevant alternatives she might choose from, because the customer has to give her consent in order to use a specific form of communication at all. In this case, the often-used justification argument that customers agree to the terms and conditions would not be a sufficient indicator for consent.

The second approach for companies that want to act ethically correct when it comes to their customers' privacy focuses on the ownership of customers' personal data. "Opponents of strengthened privacy protection think of collections of personally-identified data as 'their' property; as evidence, they point to their investment in compiling the databases and developing algorithms to 'mine'

them for various purposes" (Cohen 2000: 1378). A company that respects its customers' autonomy and therefore aims to secure their informational privacy should, however, grant their customers the right of ownership of their personal information. As it is her property, a customer should be able to know how her data is used at all times and to have access to it and object to its use. As the RALC theory suggests, a company should give customers control over their data by allowing them to correct what kind of information they disclose and delete or remove data if they wish to. Respecting customers' ownership of their personal data means securing their informational privacy and therefore respecting their autonomy.

4. Economic Justification of Privacy

4.1 Resolving the Sources of Conflict with the Privacy Calculus

In this chapter, we look at informational privacy from an economic point of view and show that the three sources of conflict areas can be solved using so-called privacy calculus. The idea of using privacy as a UVP will be introduced. In order to show how privacy can be used to increase quality and revenues as well as cut costs, we analyse the relevant target group and divide it into subgroups according to customers' preferences regarding privacy. From this, we derive strategic implications for companies in the digital telecommunication sector and show how privacy can be used as a competitive advantage in practice. As shown in section 2.3, companies in the digital telecommunication sector and their customers face three sources of conflict that cause a trade-off between profit maximisation and privacy: (1) privacy vs. usability and quality, (2) privacy vs. cost reduction, and (3) privacy vs. increase of revenue. The idea that companies need to make use of customers' personal data to remain competitive seems to be common knowledge in the digital telecommunication industry and is rarely questioned. Consequently, we now take a closer look at the specific factors that cause companies to violate their (potential) customers' informational privacy by collecting data in order to understand what kind of value this behaviour creates.

1. The customer makes her purchase decision depending on the usefulness of the product and thus determines whether or not the company's product is sold. A company thus needs to find out what suits its (potential) customers' needs best. A company that provides communication

services can improve its service by tracking customers' behaviour. By analysing how and how frequently certain features of the product are used, a company can improve its products constantly. A messenger service could introduce a group chat function, for example. The company could decide to violate their customers' privacy and analyse their customers' data to find out whether or not it has attracted new target groups by the introduction of this feature. If so, the company might concentrate on further improvements to this group chat function and thereby also improve its product. In this case, the company would have violated its customers' privacy by analysing the data, but as a consequence could have identified new customers who would buy the messenger service because of its new feature. Data like time, location and content of a communication process are often useful for specific analysis and easy to generate since communication devices like smartphones can easily transfer such data to their providers. For example, a company could decide to implement a location-sending feature after analysing the content of communication processes and finding out that information regarding whereabouts is sent frequently. The users' personal information is often also used directly to increase usability. For example, many apps track the user's location in order to suggest other users nearby with whom the person can communicate with. An app, which uses private information in order to increase quality, is the dating app "tinder" (Der Westen 2014: 1). It is designed to connect users with potential partners. For that purpose, it uses location data to find possible partners nearby. It also evaluates users' Facebook profiles in order to find similar interests and shared Facebook "friends". This aims to increase usability by providing better matches and therefore enhances the quality of the service the app provides. The same holds true for the following example: a newspaper app might remember the articles a user has read to conveniently recommend similar ones to her. Saving the users' preferences and creating e.g. political attitude profiles, which could also be stored, may be an issue for a potential future employer.

2. The costs of a company that can be lowered by strategically using customers' personal information include, among others, customer acquisition costs, R&D costs (as described in [1], product improvement processes are more efficient if users' data is evaluated), as well as customer relation management. Customers are acquired most efficiently if the advertising of a company focuses on an adequate target group and therefore increases the chances of a successful transaction. The analysis of a target group becomes more efficient when the personal information about the customer can be evaluated and advertising can be personalised. The same is true for activities regarding customer relation management. It is conceivable that e.g.

WhatsApp identifies that the need to communicate is particularly prevalent in young people by analysing their customers' profiles. As a result, the company would invest in advertising space frequently visited by young people. The location-sending feature mentioned in the last paragraph could also save R&D costs as by just analysing the data of their customers, the company could find out the need to state locations instead of having to use expensive market research. The same is true for sending contact information by one click of a button. If by analysing text content a messenger company can recognize the frequent sending of contact information, it can implement a contact-sending feature and therefore reduce R&D costs.

3. Better-tailored advertising not only cuts the costs because irrelevant groups are not addressed, but it also increases effectiveness because targeted advertisement is matched to the interests of a potential customer and therefore increases the conversion from a potential buyer into an actual customer. Communication companies like email providers often use their customers' data not only to sell more of their own products, but also to provide advertising services to external actors like retailers. They produce valuable detailed customer profiles based on the evaluation of customers' communication processes such as messages. The e-mails of Google-mail users are screened for their content, for example. If one is eager to tell all friends about the upcoming holidays, Googlemail might offer the advertising space on the email website to vacation trip providers. The more accurately Google determines the target group for the vacation provider through analysing the data of its users, the higher the conversation rates that the trip provider can expect will be. The willingness to pay for the advertising space is greater if more new customers are expected. Therefore, Google can demand higher prices and thereby increase profits.

All in all, information about (potential) customers, their preferences, needs and behaviour can mean a crucial competitive advantage, which provides an incentive for companies to violate their customers' informational privacy. On the other hand, privacy, just like usability and low prices, is also valued by customers. Many studies, such as the one by Phelps, Nowak and Ferrell, found that many consumers are concerned about the ways companies use personal information about them (cf. Phelps et al.: 29). We have, however, seen that for usability and customer acquisition purposes, companies need to collect personal information.

Although most consumers are concerned about the ways companies use personal information, (cf. Phelps et al. 2000: 29) consumers are willing to disclose certain personal information if they

get "something valuable in return" (Kobsa 2001: 4). Thus, based on the findings from Jutla and Bodorik, we see that privacy is much more applicable as a value model than as a selling proposition (cf. Jutla/Bodorik 2003: 469). Value in this sense is not limited to monetary profits, but also takes value-adding factors such as reputation into account (cf. Barnes et al 2009: 28). "Strategy is based on a differentiated customer value proposition. Satisfying customers is the source of sustainable value creation" (Kaplan 2004: 10). By measuring economic success in terms of value instead of monetary profits, we can show that privacy has economic as well as ethical value.

Losing control over the use of personal information is one of the greatest consumer fears (cf. Phelps et al: 33). Research has even highlighted that customers are not only concerned about the storage of their personal information but already act proactively (cf. Kobsa 2001: 4). In western countries like Germany or Great Britain, more than a third of the customers have refrained from buying a product or bought less due to privacy concerns (cf. Kobsa 2001: 4). Privacy intrusion leads to risks such as customer loss through lack of reputation and trust, as well as the failure to use the value of privacy economically as a UVP and a strategic competitive advantage. So how can this assumed conflict between privacy and value maximisation be resolved from an economic perspective?

The resolution of all of the conflict areas depends on one crucial factor: the customer. If more customers decide to buy a product or service for a given price, sales figures can be increased. If a greater percentage of customers is persuaded by well-tailored advertising, customer acquisition costs can be reduced. As a consequence, the key question for companies is: How do customers weigh the risks of information disclosure against the benefits they can get from a transaction?

The first researchers who came up with an idea of how to evaluate the benefits of information disclosure and privacy concerns were Laufer and Wolfe in 1977. They assumed that

> "individuals should be willing to disclose personal information in exchange for some economic or social benefit subject to an assessment that their personal information will subsequently be used fairly and they will not suffer negative consequences in the future" and called the evaluative process the privacy calculus." (Laufer/Wolfe 1977: 35)

Therefore, people are going to reveal personal information if they believe they will profit from the benefits of a relationship with a company. The benefits of the revelation are weighed against the risks

of doing so. Individuals will exchange information as long as they feel that the benefits outweigh the risks of disclosure. The calculus hence creates an incentive for the company to mitigate privacy violations and increase privacy protection, because it takes the value of privacy into the equation.

4.2 Privacy as a Unique Value Proposition

The protection of privacy does not necessarily have to cause profit reduction. Quite the contrary is true once companies realise that privacy protection is more than an instrument to minimise the risk of scandals but in fact a highly underestimated market niche. As a result, the three areas of conflict we originally identified in chapter 2.3 do not necessarily cause trade-off effects, but, as matter of fact, synergy effects if they are approached with privacy calculus in mind. Protecting customers' privacy can contribute to an increase in the quality of a digital telecommunication service by adding privacy as a value to the product, as well as cutting costs and increasing revenues. Using privacy as a UVP can therefore lead to the retention of existing customers, the acquisition of new customers who are not yet using similar products, and the enticement of customers from the competitors. These three processes contribute to transforming the originally identified areas of conflict into areas of synergy and making use of the privacy market niche.

We found that the UVP of privacy is especially influenced through (1) trust and (2) security. Increased trust and security in the company, which administers the personal information, lead to higher satisfaction with the company than if the consumer does not trust the company (cf. Kobsa/Knijnenburg: 15). Higher satisfaction leads to a higher level of reputation capital and thereby attracts a higher number of customers or retains them. Thus, because customers value trust and security, it is important for the company to enhance both of them.

1. Whenever a company convinces its customers that they can trust the company and its use of their personal information, the company increases its reputation capital. Based on the findings of Culnan and Bies, treating the consumer's personal information in a consumer transaction fairly is "essential to building trust in a customer relationship" (Bies/Culnan 2003: 327). To sustain trust, the organisation's practices as perceived by the consumer must be consistent with the policies it discloses. If the company does not act in accordance with its privacy guidelines, trust is lost and the chance of disclosing personal information in the future decreases. (Bies/Culnan 2003: 327 et seq.) It may as well raise "concerns about the integrity of

the organization's information practices" (Bies/Culnan 2003: 327 et seq.). A significant factor in showing that privacy is able to become a UVP is to reveal the customer's willingness to pay for it. The study of Savage and Waldman 2013 indicates that customers are ready to pay for privacy-friendly communication technology which they can trust. The latest study of Savage and Waldman was conducted in the US and concentrates on the app market which is part of the communication sector. Their results suggest that a representative customer is willing to make a one-time payment for an app she can trust. Such trust components are deleting of browser history ($2.28), the concealment of the list of contacts ($4.05), of location ($1.19), of the phone's identification number ($1.75) and concealing text message contents ($3.58). There is also a willingness to pay for the removal of advertising ($2.12) (cf. Savage/Waldmann 2013: 1). The market potential is therefore enormous, and customers can be attracted by using privacy as a UVP if especially the different concealment options are made available. Furthermore, through cumulative positive experiences of the information practices of a company, trust is enhanced over time (cf. Bies/Culnan: 327). Thus, whenever a company enjoys a high level of trust and reputation, it becomes more costly for the customer to switch. She has to put some effort to change firms to get a service or product which she can trust in the same way as the original company. As a result, it is much more likely that the benefits of the trusted company outweigh the costs for a company change

2. Customers will also change the company or decide to buy a privacy-friendlier product if the perceived risks of using privacy violating products become too high. The risks can be lowered and therefore customers attracted if the perceived security in the privacy-friendly company is higher. The perceived security is "the subjective probability with which consumers believe that their personal information will not be viewed, stored, or manipulated during transit or storage by inappropriate parties, in a manner consistent with their confident expectations" (Chevlappa/Pavlou 2002: 359). Chevlap¬pa and Pavlou empirically verified the highly positive relation between this perceived security and control mechanisms. The better the control mechanisms, the higher the security the customer perceives. Among others, they list encryption, authentication (e.g. through digital certificates/third parties) and protection (e.g. through presence of privacy policy statements) as positively affecting consumers' perceived security (cf. Chevlappa/Pavlou 2002: 358, 364). We will discover later how exactly a company can implement privacy as a UVP.

4.3 Segmentation of Consumers Based on Their Privacy Attitudes

Security and trust are the main variables of the unique privacy value. However, not all people value their informational privacy to the same extent. Throughout the population, one can differentiate among three groups regarding their privacy valuation according to Westin: (1) privacy fundamentalists, (2) privacy pragmatists and (3) privacy unconcerned. Westin paved the way for modern privacy research in the late seventies by his aforementioned typology of privacy attitudes which he edited in 2001 (cf. Westin 2001) and 2003 (cf. Westin 2003: 445). In his more recent studies, he recognised a shift in privacy attitudes moving from a minor focus topic for just a few people to an "issue of high intensity" (Hann et al 2002: 2). The download numbers of one of our practical examples, "Zenmate", exploded when privacy scandals became an issue in their respective target markets. Thus, we expect that the number of privacy fundamentalists has increased since 2003, and the number of privacy unconcerned has decreased since privacy violations have caused widely recognised scandals and discussions in media and politics since then.

1. The privacy fundamentalists are deeply concerned about privacy. Therefore, they are likely to reject the social or economic benefit a company offers in exchange for information disclosure. Fundamentalists also have a rather strong tendency to demand legal regulation and control of the business' use of personal information. In 2003, 25% of the US population were found to be privacy fundamentalists.
2. Privacy pragmatists made up the majority of the US population (55%) in 2003. Before making the decision whether to disclose information or not, they use a sophisticated privacy calculus process. First of all, they want to know the social or economic benefit they will get from information disclosure and how their personal information is collected and used. Further, they are interested in the risks they are exposed to if information is gathered. Thirdly, privacy pragmatists look to see whether and which safety measures a company adopts to mitigate privacy risks. Finally, they ask themselves whether they can trust the company. If they want a benefit but are concerned about risks and do not trust the company, they too demand an appropriate legal framework to hedge against privacy risks.
3. The privacy unconcerned hold the opposing position to the privacy fundamentalists and do not care much about personal information dissemination or privacy. In 2003, approximately a fifth of the population were assigned to this group (cf. Westin 2003: 445). As Westin characterises

them, "(…) for 5 cents off, they will give you any information you want about their family, their lifestyle, their travel plans, and so forth" (Westin 2001: 23).

4.4 Strategic Implications for the Digital Telecommunication Sector

As we have identified different types of privacy attitudes, we also recommend strategically differentiated approaches to restoring or implementing trust and security as a competitive advantage by using privacy as a UVP. First and foremost, our proposals are aimed at privacy pragmatists who form the majority of the population. Yet we also think that the concerns of privacy fundamentalists can be calmed although they might not be fully convinced of secure informational privacy by the strategies we suggest. The strategic implications for this group rather aim at the future when more positive experiences with privacy-friendly companies will be gained. As privacy unconcerned do not care about the dissemination of information, the privacy mechanisms we propose do not have to be applied to this group of the population from an economic point of view.

We suggest four main strategies for implementing privacy as a UVP that contribute to fulfilling the conditions for informational privacy as suggested by the RALC theory: (1) encryption, (2) authentication, (3) protection and (4) privacy-friendly data collection.

1. The first essential pillar of the concept is encryption. Encryption is defined as "the process of translating information from its original form into an encoded, incomprehensible form" (Chevlappa/Pavlou 2002: 361). Encryption techniques should always aim for end-to-end encryption. It is currently considered a very popular and safe method to transfer personal information from the sender to the recipient. Once a message is sent, it can only be decoded by the sender or the recipient's terminal equipment. It thereby becomes very difficult to skim information during the transfer. End-to-end encryption can be realised, for example, through "web servers and browsers that are built with a technology referred to as secure socket layer (SSL)" (Chevlappa/Pavlou 2002: 361). While surfing, it can be noticed through an added 's' to the traditional 'http' protocol in the address of a website. Messaging apps, for example, should only use the safe protocol to transfer data in order to minimise privacy risk caused by spying through external actors.
2. The second strategy is authentication. Authentication is defined as the process through which a company "can be established through a trusted third party" (Chevlappa/Pavlou 2002: 361)

which guarantees the correct identity of the company (Chevlappa/Pavlou 2002: 361). This could most efficiently be realized through a privacy seal or digital certificates (cf. Chevlappa/ Pavlou 2002: 361). A privacy seal guarantees that firms reveal their privacy approach and act according to it (Bies/ Culnan 2003: 333) and makes the UVP privacy visible to the customer. According to a study of BITKOM, 55% of Internet users reported a wish for a government label for data security (cf. BITKOM: 23).

3. Thirdly, fair information practices should be implemented. They protect informational privacy as suggested by the RALC theory. We found notice, choice and access to be fair informational practices of first priority. Notice means that individuals should know whether and how information about them is collected as well as how it is going to be used. Choice can be applied when customers object to information use in cases when the information was collected for one consented purpose but is used for another. Access includes the possibility for customers to see their information and correct mistakes (cf. Federal Trade Commission 2000: 3).
4. While our focus lies on the value of privacy, we also acknowledge the need for companies for a minimum of personal information collection due to the trade-offs mentioned in 2.3 and 4.1. In order to increase trust without having to work without essential customer information, we suggest the process of privacy-friendly data collection. A company seeking to implement a privacy-friendly data collection has to consider a number of points. Privacy-friendly data is insensitive data as explained in 2.3. In general, sensitive data should be treated more carefully than insensitive data, i.e. asking for sensitive data should be avoided. In a poll conducted by Kobsa 2001, 73% of the customers found it helpful and convenient if, for example, a website remembered basic personal information about them (cf. Kobsa 2001: 3). Nevertheless, the customer also has to have the feeling that the requested information is needed for a transaction and not collected arbitrarily (cf. Li et al 2010: 25). If the address of a customer is requested for product delivery, the customer is probably willing to disclose it. However, in other situations, asking for address data might fuel distrust.

Each of the recommended strategies goes one step further to a privacy-friendly company. The provided strategies complement each other and promote the conditions of the RALC theory. To encrypt, authenticate and protect her information could turn out to be very time-consuming for the customer if, for example, she has to check the privacy guidelines of every website before beginning to use it. A company can take this burden on itself and use so-called privacy-enhancing

technologies as, for example, proposed by Ackerman and Cronor (1999). They help to implement the strategies we proposed. The first strategy, encryption, should be realised through a secure connection while surfing the Internet or texting. End-to-end encryption is the most promising approach. Privacy-enhancing technology could authenticate a website as being on a warning list on well-known associations as e.g. BBBOnline or on the contrary confirm a privacy-friendly site through the recognition of a privacy seal with which privacy-friendly companies could be labelled by an independent third party. Most time would be consumed if the consumer had to read through all the privacy guidelines of every website. With technology that can check whether or not the privacy guidelines of a company match the privacy preferences of the customer, this would not have to be done. Once privacy settings are set, the privacy-enhancing technology either verifies whether the consumer's setting match or do not match a website or app. Thus, the decision whether to continue the interaction with the website/app or not is left to the consumer. With platforms, such as P3P, this is already possible. P3P is a standard sponsored by the World Wide Web Consortium (W3C). Web sites encode their privacy policies in a machine-readable format, allowing web browsers and other P3P agents to find them automatically.

Regardless of whether companies choose to implement privacy as a UVP through privacy-enhancing technologies, guidelines authenticated through certifications or seals, or other implementation strategies, the need and demand for privacy protection is increasing, and so are the opportunities to use privacy as a UVP.

5. Practical Examples of Privacy as a UVP

5.1 Threema as an Example of Privacy Protection as a Competitive Advantage

In the following section, two case studies will support our hypothesis that the value of privacy can be translated into economic figures by using it as a UVP. The first case study analyses Threema, a secure mobile messaging service, and the second one is about ZenMate, a company providing privacy-enhancing technology. Both companies focus on business-to-customer relations and show a strong focus on the issue of privacy protection in the general sense. We chose Threema as an example as it is the only messenger service rated 'noncritical' by Stiftung Warentest, a German

consumer protection organisation (cf. Haak 2014: 1). The exclusive criterion for the ranking was data security.

Threema's main competitor WhatsApp dominates the market with a German market share of 84% in 2014 (cf. Horn 2014: 1). Both companies offer a mobile messaging app which can be installed on a customer's smartphone through download. Both allow real time communication with the user's personal network via online chatting. In contrary to mere SMS delivery, both providers offer the sending of messages at no charge. Threema provides end-to-end SSL encryption (Threema Homepage 2014), which ensures that only the sender and the recipient of the message can read it, and therefore provides strong protection for user's informational privacy. WhatsApp does not offer any service in this area. Installing Threema costs €1.79 (for Apple devices) or €1.60 for Android. WhatsApp is free for the first year and then requests a yearly charge of €0.89.

For a long time, Threema's download figures were very low compared to WhatsApp. However, when Facebook took over WhatsApp on 20 February 2014, Threema's users doubled in just 24 hours. Since the takeover in February 2014 till early May of that year, an additional 2.6 million users joined Threema – an increase of 700% in four months (cf. Weigert 2014: 1). Eighty per cent of Threema's users are German residents. Nevertheless, Threema is not a German phenomenon. In many other European countries as well as the United States, Threema ranked among the top 5 paid apps after the WhatsApp takeover. The expansion of Threema after the takeover of WhatsApp could be caused by three factors: (1) usability, (2) price, and (3) privacy concerns.

1. Threema entails all functions WhatApp has. It is possible to send text messages, emoticons, voicemails, and locations or interact in group discussions. The main difference is that Threema, in contrast to WhatsApp, does not lay claims to the copyright of the pictures, texts and videos of its users. It also does not analyse the text messages of its customers. In particular, Threema increases protection against data skimming because it has integrated end-to-end encryption. Since there is no functional advantage in using Threema rather than WhatsApp, we reject usability as a factor for Threema's expansion.
2. The price could also be a distinguishing criterion. Nevertheless, we think that in absolute terms, the difference between the two apps is negligible. After the third year of usage, Threema, with its one-time payment, becomes even cheaper than the WhatsApp subscription.
3. As usability and price levels are so similar, the reason for the rapid increase of Threema users must be a different one: Threema uses privacy as a UVP and therefore creates a competitive

advantage for itself. Customers who used WhatsApp before its takeover might have transferred the privacy concerns they had to WhatsApp since Facebook's privacy reputation is very poor. We have seen that Threema does not stand out from its competitors for reasons of functionality. Instead, they advertise their product using the slogan 'Seriously secure mobile messaging'. The slogan clearly focuses on security – one of the two proposed values created by privacy. It is the offered security through privacy protection which gives the product its uniqueness. Threema fulfils two of our suggested strategies: protection through fair information practices and encryption. Through the SSL encryption, data is transmitted safely. End-to-end encryption ensures that only the sender and recipient of the message can read its content. Fair information practices are described in the privacy guidelines of Threema. The customer can read whether data is collected, for how long and for which purposes it is used. The company stores information only for the time which is required to transfer texts or images. Afterwards, the data is deleted. The user is free to link her Threema ID with an email address or telephone numbers of his address list. If she made the choice to link the contacts, she can always undo and thereby correct her actions. Unauthorised access to third parties is also prohibited. Therefore, both restricted access and limited control conditions as proposed by the RALC definition are fulfilled (cf. Threema Homepage 2014).

5.2 ZenMate as an Example for Privacy-Enhancing Technology

ZenMate offers privacy-enhancing technology which protects users' informational privacy by restricting external actors' access to users' data. At the same time, it enables users to manage their privacy by giving them the opportunity to switch ZenMate on and off according to their preferences when to disclose information. It is a browser add-on, which is currently downloadable for free and offers encrypted, anonymised and thereby secure data traffic in the Internet. Of the strategies proposed in chapter four, ZenMate fulfils encryption and protection. No matter which network is used, ZenMate manages to encrypt and secure every connection through a "cloud-network of highly secured servers" (ZenMate). By doing so, it hides the personal IP address of the electronic device used and replaces it by a generic ZenMate IP. Not even the geographical location is localisable. The person surfing with ZenMate turned on is now "untraceable, unidentifiable and secure" (ZenMate Homepage 2014). In contrast to other clients, ZenMate's usability is very high, and users do not need much technical education for its implementation. Simon Specka, the founder of ZenMate,

describes the vision of his company as "to provide security and privacy through encryption in a simple easy way that anyone can implement, regardless if you are a tech guru or a 92 year old granny." (ZenMate Blog 1). Four million ZenMate users show that there is an increasing demand for the protection of informational privacy as provided by ZenMate's privacy-enhancing technology. Every minute, thirty new signups are registered. ZenMate got all of their clients without one single euro of marketing budget (cf. ZenMate internal documents) and yet acts in nearly every country. The download numbers in specific situations indicate how important the protection of privacy through anonymisation really is: whenever the freedom of speech is oppressed in a country and governments try to restrict access to, for example, social networks, ZenMate's download numbers increase significantly in that country. Although the following examples refer to governments, we think the company case is similar: if governments restrict freedom of speech and hence violate informational privacy, the citizens' demand for privacy-enhancing technology increases. Likewise, if companies impede undisturbed communication and violate informational privacy, customers will switch to a privacy-friendlier communication provider.

During the local government elections in Turkey, access to Twitter was blocked. As a result, ZenMates' download rates increased by 2300%. Out of the 10 million Turkish Twitter users, 180,000 installed ZenMate to continue to use that social network anonymously. Similar processes could be seen when the Venezuelan government censored social networks during anti-government protests (cf. ZenMate Blog 2). In the U.S., ZenMate is also successful. Mainly schools, universities and employees at the workplace want to protect their privacy. Public awareness grew especially with the NSA/Snowden affair (cf. ZenMate internal documents).

Every person using privacy enhancing technology shows that privacy is increasingly becoming "an issue of high intensity" (Hann et al 2002: 2) and according to Simon Specka, the founder of ZenMate, this proves that ZenMate 'got it right' (cf. ZenMate internal documents). This becomes even more significant if we consider the rising demand for privacy after every 'privacy crisis' like the NSA affair. Although ZenMate is currently available for free, it declared its intention to provide a paid version in the future as well. In the emerging freemium model (combination of free and premium), implementing privacy as a UVP will also create monetary value. Other companies that want to offer privacy protection for their customers should also be interested in ZenMate's paid version being released in the future. All in all, the constantly increasing user numbers of ZenMate indicate a demand for privacy protection.

6. Conclusion

In this paper, we have shown what is meant by the term "informational privacy" and why it is valuable from an ethical perspective. Privacy protects autonomy that has a basic value that people do not want to give up. Data mining and monitoring make a person less autonomous because the feeling of surveillance alters her behaviour. Therefore, privacy is valuable, especially in the context of digital telecommunication. At first sight, it appears difficult for companies to protect their customers' privacy, because it seems to restrict their range of action and seemingly causes economic damage. We have shown that this is not the case. On the contrary: there is an increasing demand for privacy, which is why privacy can even constitute a competitive advantage when used strategically as a UVP that creates trust and enhances perceived security. If companies are not ready to comply with the wishes of their customers, they might face customer migration to more privacy-friendly companies such as Threema in the communication sector or ZenMate as a protector of Internet privacy. During our investigations, we came across several studies about the demand for privacy in very specific situations or industries. Further research in the digital telecommunication sector could shed light on the specific willingness to pay for privacy and the details of informational privacy that are especially valued by customers. Our example, Threema, indicates that at least for certain communication services, customers already pay a premium. We await ZenMate's extended freemium model and other privacy-friendly companies to show the potential privacy has – because privacy matters not only from an ethical perspective, but also from a strategic one.

References

Barnes, C. / Blake, H. / Pindler, D. (2009): Creating & Delivering Your Value Proposition: Managing Customer Experience for Profit, London: Kogan Page Publishers.

Bies, R.J. / Culnan, M.J. (2003): Consumer Privacy: Balancing Economic and Justice Considerations, in: Journal of Social Issues, Vol. 59 / No. 2, 323–342.

BITKOM (2011): Datenschutz im Internet. Eine repräsentative Untersuchung zum Thema Daten im Internet aus Nutzersicht, URL: http://www. bitkom.org/files/documents/BITKOM_Publikation_Datenschutz_im_Internet.pdf (accessed: 30/07/2014).

Bodorik, P. / Jutla, D. (2003): A Client-Side Business Model for Electronic Privacy, in: eCommerce Conference on eTransformation.

Brandeis, L. D. / Warren, S. D. (1890): The Right to Privacy, in: Harvard Law Review, Vol. 4 / No. 5, 193–220.

Buss, S. (2013): Personal Autonomy, URL: http://plato.stanford.edu/archives/spr2014/entries/personal-autonomy/ (accessed: 27/07/2014).

Chevlappa, R. K. / Pavlou, P. A. (2002): Perceived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions, in: Logistics Information Management, Vol. 15 / No. 5/6, 358–368.

Christman, J. (2003): Autonomy in Moral and Political Philosophy, URL: http:// plato.stanford.edu/archives/fall2008/entries/autonomy-moral/ (accessed: 15/07/2014).

Cohen, J. E. (2000): Examined Lives. Informational Privacy and the Subject as Object, in: Stanford Law Review, Vol. 52 / No. 5, 1373–1438.

Overfeld, M. (2014): So funktioniert die Dating App Tinder – Ein Selbstversuch, URL: http://www.derwesten.de/wirtschaft/digital/so-funktioniert-die-dating-app-tinder-ein-selbstversuch-id9714611.html (accessed: 01/09/2014).

Faden, R. R. / Beauchamp T. L. (1986): A History and Theory of Informed Consent, Oxford: Oxford University Press.

Federal Trade Commission (2000): Privacy Online. Fair Information Practices in the Electronic Marketplace, URL: http://www.ftc.gov/sites/default/files/documents/reports/privacyonline-fair-information-practices-electronic-marketplace-federal-trade-commissionreport/privacy2000.pdf (accessed: 27/07/2014).

Goodwin, C. (1991): Privacy. Recognition of a Consumer Right, in: Journal of Public Policy and Marketing, Vol.10 / No. 1, 149–166.

Grimm, R. Prof. Dr. (2005): Digitale Kommunikation, München: Oldenbourg Wissenschaftsverlag.

Hann, I. H. / Hui, K. / Lee, S. / Png, I. (2002): Online Information Privacy: Measuring the Cost-Benefit Trade-Off, in: 23rd International Conference on Information Systems, Himma: K.E.

Tavani, H. T. (2008): The Handbook of Information and Computer Ethics, Hoboken: Wiley.

Horn, D. (2014): Facebook und WhatsApp – bekommen wir nur die Datenschutzdebatten, die wir verdienen?, URL: http://wdrblog.de/digitalistan/archives/2014/02/ facebook_und_whatsapp_-_bekomm.html (accessed: 28/07/2014).

Kant, I. (1785): Werke in zwölf Bänden, Frankfurt am Main.

Kaplan, R. S. / Norton, D. P. (2004): Strategy Maps. Converting Intangible Assets into Tangible Outcomes, Cambridge: Harvard Business Press.

Knijnenburg, B.P. /Kobsa, A. (2013): Making Decisions about Privacy: Information Disclosure in Context-Aware Recommender Systems, in: ACM Transactions on Interactive Intelligent systems Vol. 3 / No. 3.

Kobsa, A. (2001): Tailoring Privacy to Users' Needs, Berlin: Springer Verlag.

Kupfer, J. (1987): Privacy, Autonomy and Self-Concept, in: American Philosophical Quarterly, Vol. 24 / No. 1, 81–89.

Laufer, R. S. / Wolfe, M. (1977): Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory, in: Journal of Social Issues, Vol. 33 / No. 3, 43–51.

Li, H. / Xu, H. / Sarathy, R. (2010): Understanding Situational Online Information Disclosure as a Privacy Calculus, in: Journal of Computer Information Systems, Vol. 51 / No. 1, 62–71.

Mill, J. S. (1859): On Liberty in Focus, London: Routledge.

Moor, J.H. (1997): Towards a Theory of Privacy in the Information Age, in: Computers and Society, Vol. 27 / No. 3, 27–32.

Moor, J. H. / Tavani, H. (2001): Introduction to Computer Ethics. Philosophy Enquiry, in: Ethics and Information Technology, Vol. 3 / No. 1, 1–2.

Phelps, J. / Nowak, G. / Ferrell, E. (2000): Privacy Concerns and Consumer Willingness to Provide Personal Information, in: Journal of Public Policy & Marketing, Vol. 19 / No. 1, 27–41.

Rössler, B. (2001): Der Wert des Privaten, Berlin: Suhrkamp.

Savage, S. J. / Waldmann, D. M. (2013): The Value of Online Privacy, Boulder: University of Colorado at Boulder.

Solove, D. J. (2002): Conceptualizing Privacy, in: California Law Review, Vol. 90 / No. 4, 1087–1155.

The free dictionary (2014): digital+communication, URL: http://www.thefreedictionary.com/digital+communication (accessed: 01/09/2014).

Threema Homepage (2014): Privacy, URL: https://threema.ch/de/privacy.html (accessed: 30/07/2014).

Westin, A. (2001): Opinion Surveys: What Consumers Have to Say about Information Privacy, Washington D. C.: U.S. Government Printing Office.

Westin, A. (2003): Social and Political Dimensions of Privacy, in: Journal of Social Issues, Vol. 59 / No. 2, 431–453.

Winer, R. S. (2001): A Framework for Customer Relationship Management, in: California Management Review Reprint Series, Vol. 43 / No. 4, 89–107.

Weigert, M. (2014): Threema hat 2,8 Millionen Nutzer, URL: http:// netzwertig.com/2014/05/02/nutzerzahlen-versiebenfacht-threema-hat-28-millionen- nutzer/

(accessed: 29/07/2014).

Young, P. (1978): Introduction: A Look at Privacy, New York: John Wiley & Sons.

ZenMate Blog 1: URL: https://blog.zenmate.com/the-zenmate-effect/ (accessed: 27/07/2014).

ZenMate Blog 2: URL: https://blog.zenmate.com/the-enigma-of-encryption/ (accessed: 27/07/2014).

ZenMate Homepage: URL: https://zenmate.com/ (accessed: 27/07/2014).