HAL
archives-ouvertes.fr

Privacy: What Are We Actually Talking About?

Philip Schütz, Michael Friedewald

▶ To cite this version:

Philip Schütz, Michael Friedewald. Privacy: What Are We Actually Talking About?. 6th International Summer School (ISS), Aug 2010, Helsingborg, Sweden. pp.1-14, 10.1007/978-3-642-20769-3_1 . hal-01559452

HAL Id: hal-01559452
https://hal.inria.fr/hal-01559452

Submitted on 10 Jul 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution| 4.0 International License

Privacy: What are we actually talking about?

A multidisciplinary approach

Philip Schütz and Michael Friedewald

Fraunhofer Institute for Systems and Innovation Research, Karlsruhe, Germany
E-mail: {philip.schuetz, michael.friedewald}@isi.fraunhofer.de

Abstract. This paper presents a multidisciplinary approach to privacy. The subject is examined from an ethical, social, and economic perspective reflecting the preliminary findings of the EU-funded research project PRESCIENT. The analysis will give a comprehensive illustration of the dimensions' unique and characteristic features. This will build the basis for identifying overlaps and developing synergetic effects, which should ideally contribute to a better understanding of privacy.

1 Introduction

Privacy is an essential fundamental human right, which preserves individuals from arbitrary intrusion into their personal sphere by the state, corporations or other individuals. In a globalised world with ever new emerging technologies privacy issues have evolved into one of the most salient, ubiquitous and pressing topics of our society today. The information age with its new forms of communication, data storage and processing contests the current concept of privacy to an extent and in ways never seen before. The imperative to deal with these new challenges becomes an increasingly prominent feature not only in media coverage but also in private and public policy-making.

However, the current media attention to privacy-related topics poses the risk of a shallow and non-scientific debate. Being a moving target, the concept of privacy is above all elusive. It is evolving over time and people define and value it differently [1]. That is exactly why it remains tremendously important to work at the theoretical base of the concept and to keep on asking: What are we actually talking about?

Recognising that privacy is a multifaceted concept, this paper proposes to examine the subject from different scientific perspectives. Reflecting the preliminary findings of the EU-funded research project PRESCIENT [2], the multidisciplinary approach embraces the dimensions of ethical, social, and economic aspects.[1] The following sections are intended to give a comprehensive illustration of the perspectives' unique and characteristic features. This will form the basis for identifying overlaps and developing synergetic effects, which should ideally contribute to a better understanding of privacy.

[1] Although being considered in PRESCIENT, the legal perspective as a section of itself has been left aside in this paper in order to avoid redundancies with an already extensive literature on legal aspects of privacy.

2 The different perspectives

2.1 Ethical perspective

Ethics is often falsely understood as moral rules providing individuals and society with a guidance. Yet ethics is not etiquette, it is not a manual to be followed, rather it is a philosophical enquiry about concepts involved in practical reasoning. Ethics as a part of philosophy deals with moral principles such as good and evil, virtues or justice.

This section will to explore the ethical value of privacy. Why do we consider privacy as something worthy to protect? Where does the desire for privacy derive from? Assuming that privacy is part of two constitutive human polarities, mainly the desire to be independent and the need to be part of a community, we will trace the biological, anthropological, psychological and religious antecedents of this polarity.

Research on territoriality and overcrowding shows that virtually all animals seek periods of individual seclusion. Although being social animals, humans have shown throughout their evolution behaviour of defending their territories and avoiding overcrowding the latter often functioning as an intensifier of stressful condition [3]. In frequently seeking small-group intimacy, individuals search for relieve of stress dropping the role they are assigned to play in community. At the same time, however, particularly humans have developed to the highest degree the ability of empathy, a capacity to reproduce the emotional and mental patterns of others, which makes them not only in their rationale to survive but also in their very neurological structure dependent on other human beings.[2] That is why isolation can be much more pathological than overcrowding [5].[3]

Supported by various anthropological studies, aspects of privacy can be found in modern but also preliterate societies throughout history all over the world [6]. Hence, the individual's need for a certain degree of social distance at some point in time seems to occur in every culture and time period, although social obligations as a must of any gregariousness imply some limitations to the choice of seeking this distance. As Westin puts it, the concept of privacy seems to be a "cultural universal", which would militate in favour of an intrinsic value of privacy [7].

However, feminist anthropologists view privacy mainly as a "trap of domesticity" to women [8]. This "trap" would develop through the division between domestic affairs as essentially private and predominantly female, and the exclusively male and public realm of war and politics.[4] Picking up the same train of thought, Pateman argues that the private and public spheres are two sides of a social contract, which includes primarily a

[2] According to the most accredited theories, empathy is generated by „automatically and unconsciously activated neural representations of states in the subject similar to those perceived in the object" [4, p. 282].

[3] Research on overcrowding and isolation suggests that the degree of control concerning the ability to choose between solitude and gregariousness is decisive in affecting the physical and psychological state of the individual.

[4] Post-modern and feminist scholars have devoted influential studies on the sexual origins of privacy in the early Greek civilization. Sophocles' Antigone was used as an example for the introduction of the distinction between the private, familial and womanly (oikia) and the public, political, and masculine (koinos) realm [9].

"sexual contract" that distributes social roles and defines "areas of influences" between men and women [10].

Arguing furthermore from a psychoanalytic point of view, Freud understood privacy as involving a dichotomy between "civilized society, which demands a good conduct" of its citizens, and instinctual behaviour of the individual [11]. Since society has allowed itself to be misled into tightening the moral standards to the greatest possible degree, the creation of the private realm serves above all as a safety valve for all of the instinctual constraints weighing heavily upon the individual [11,7].

Even more revealing is his seminal essay on "Das Unheimliche" (The Uncanny) [12]. The German term "Unheimlich" derives from the meaning of "not homey" ("unfamiliar" or "outside of the family"), which is "the name for everything that ought to have remained secret and hidden but has come to light", says Schelling's definition, from which Freud starts. He eventually defines the uncanny as "anything we experience that reminds us of earlier psychic stages, of aspects of our unconscious life, or of the primitive experience of the human species". The *id* as part of Freud's structural model of the human psyche (*id*, *ego* and *superego*) contains most of these uncanny elements. There is in other words a literally dark side to privacy which implies a dimension the individual will never be able to master or understand completely.

Freud then notices that also the antonym "heimlich" ("homely" or "familiar"), which nowadays actually means "secret", conveys the meaning of private in the sense of "within in the family". Surprisingly, he discovers that familiarity represents an integral part of uncanniness. It consequently seems that the uncanny as well as the familiar (homely) are two sides of the same coin which both constitute the core sphere of inner personal privacy.

The concepts of modesty, intimacy and shame reflect furthermore emotions, behaviour patterns and externalised decisions which are based on the interplay within one's psyche between the id and the superego. The private realm therefore depends on a process of negotiating the boundary between the inner part of the self and the external world of the other selves. This negotiation is influenced both by personal attitudes (subjectivity) and by social and cultural norms.

In a religious context the inner part of the self represents a sacred place where the individual can seek intimacy with God.[5] Even beyond the Christian or other monotheistic religions the attempt to establish a bond or a contact with God(s) consists commonly of a meditation phase of an individual or an exclusive group, in which privacy is sought.

Eventually, political philosophy has had another major influence on today's conception of privacy. Especially in the Western hemisphere liberalism was shaping the idea of a state that ensures its citizens the protection of life, liberty and property, an idea originated by Locke in *Two Treatises of Government*. The legal notion of privacy as a fundamental right but also as an instrument to achieve other basic rights is based on these liberal conceptions in which privacy is mainly seen as a protective sphere that shields

[5] The biblical allegory of Adam and Eve, being happily nude while sharing with God the holy space of paradise, tries to show that perfect intimacy with God. When they taste from the forbidden fruit and consequently break the alliance with God, shame and distrust represented by the need to hide themselves in clothes begin to appear.

the individual from intrusions of the state.[6] Complementary to this negative defensive right, Westin suggests a rather positive right conception of privacy which enables the individual to exercise control over his/her information.

2.2 Social perspective

Privacy is often seen in contrast to the public, although there is a social value to privacy. The perceived duality between private and public value frequently results in a supposed need of balancing the two against each other, which is explored in this section.

Humans are individualistic and herd animals at once. They represent Hobbes' *homo homini lupus* and Aristotle's *zoon politicon* at the same time. This inner dualism can be best described by Schopenhauer's *hedgehog's dilemma*, which comprises the idea to identify the optimal distance between being "alone" and "together".[7]

So Moore is right when he argues that "the need for privacy is a socially created need. Without society there would be no need for privacy" [6, p. 73]. However, this only reflects the personal dilemma, with which individuals are regularly confronted. The tension between individual and community remains even if the hedgehog's dilemma is solved, because the optimal distance would differ from situation to situation and would be due to various personal preferences not applicable to everyone.

That is why balancing the individual well-being against the common good runs frequently into severe difficulties. One is that the notion of balancing or making trade-offs suggests literally a zero-sum game where an increase in security, for example, automatically results in a reduction of privacy. However, these kinds of trade-offs, often presented in public as axiomatic, seem not to take the complexity of social values into their account. "The value of privacy should be understood in terms of its contributions to society. [...] When privacy protects the individual, it does so because it is in society's interest.", argues Solove [15, p. 173].

Theoretically, privacy as well as other values such as national security, transparency, free speech or other human rights generate a complex net of interwoven and consequently interdependent values of society which can flexibly shift into one or another direction. The network structure could function as a model for the interaction of these social values.

In legislative, judicial and administrative practice, there is the inevitable need of balancing different and overlapping values against each other. Therefore it becomes crucial to consider how such balancing processes can be effectively designed and implemented. One of the main features of balancing processes should be the testing of necessity and proportionality. Aharon Barak advocates

> "the adoption of a principled balancing approach that translates the basic balancing rule into a series of principled balancing tests, taking into account the importance of the rights and the type of restriction. This approach provides better guidance to the balancer (legislator, administrator, judge), restricts wide

[6] Warren and Brandeis later extend this idea defining privacy as "the right to be left alone" [13].

[7] Though the hedgehog needs the warmth and affection of his fellow hedgehogs in his surrounding, he will expect to inevitably get hurt by their spiny backs [14, p. 396].

discretion in balancing, and makes the act of balancing more transparent, more structured, and more foreseeable." [16, p. 2]

So in the case of balancing national security against privacy, for instance, there are at least four minimum core principles to be considered: 1) The principle of the rule of law, 2) the principle of proportionality, 3) the principle of favouring moderate intrusiveness as well as 4) the principle of the lesser technological privacy intrusiveness and the principle of directly proportional incremental authority to the privacy intrusiveness of the technology used [17, p. 142].

The pursuit of the greater good has often led to tremendous affliction throughout world's history. That is why inalienable rights protect the individual from intrusions of the state. These fundamental rights and their core principles must not be subject to negotiation and should include an adequate protection of minorities in order to avoid Tocqueville's *tyranny of the majority*.

However, privacy has also a "dark side" to it. Not only could terrorists take advantage of a constitutionally guaranteed private sphere to organise their attacks, but also is transparency and accountability in general challenged in cases like bank secrecy or discretionary earnings of politicians. From a feminist perspective, as already pointed out, the socially constructed realm of privacy threatens to continue to serve as a shield against the public, covering domestic violence and abusiveness of men against women.

Though seemingly in conflict, social values such as privacy and transparency are all equally important. The Gordian challenge, with which society is continuously confronted, consists of striking the right balance between these social values.

2.3 Economic perspective

This section examines privacy from an economic point of view. Although the notion of privacy in the economic discourse is mainly understood as informational privacy dealing with data protection issues, this paper tries to consider the costs and benefits beyond the mere perfect/imperfect information topos of economic theory.

In order to be able to effectively analyse the economic value of privacy, we have to initially shed light on the main actors protecting and intruding upon privacy. The actor-centred approach hypothesises that the decisions of the data subject (DS) as well as those of the data controller (DC) are based on the rationale of the *homo economicus* carefully balancing the costs and benefits and aiming for the maximal profit.[8]

The decisions of the DS include a dual choice model in which the DS can opt for "disclosing" or "retaining" personal information. The DC's options of actions involve the collecting, aggregating, storing and processing of personal information as well as the reactions to privacy breaches.[9]

[8] The EU data protection directive defines the DS as "an identified or identifiable natural person", whereas the DC is referred to as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." [18]

[9] Due to the growing quantity of possible DC actors, the analysis limits itself to private business entities, although public authorities represent one of the most important bodies collecting and controlling personal data. This must be, however, subject to further research.

The data subject: Costs created by disclosing personal data are scientifically extremely hard to grasp, because they are at the core of exactly that essence and complex value of privacy, which is a fundamental part of the essentially contested concept of privacy itself. Frequently, individuals value these types of costs differently and in addition privacy incidents often do have indirect and long-term effects on the DS.[10] Consequences are therefore hard to anticipate and it seems that individuals perceive long-term impacts as a rather indirect, controllable and less perilous harm to themselves. That's why the DS often underestimates or does not consider the long-term risks in giving away personal information [20, p. 11].

However, more and more individuals are confronted with privacy problems frequently resulting from their lax attitude towards sharing private information or being forced to disclose personal data. This can result in social sorting or other discriminatory practices by DCs. There is furthermore an increasing risk of being the victim of online and offline crime such as burglary,[11] identity theft, cyber stalking and bullying, character assassination as well as other forms of harassment.

Another cost factor of sharing voluntarily personal and private data involves that peers, colleagues or prospective employers may form an opinion about the data subject based on a one-time superficial and maybe misleading impression. The consequences can go from mere embarrassment to the failure of a job interview. Feeling annoyed by unsolicited advertisement, but also being uncomfortable with advertisements that reflect too much knowledge about themselves, Internet users suffer more often than expected the aftermath of continuously disclosing personal and private information.

In many instances, however, they are actually able to choose between disclosing or retaining personal data. Nonetheless, individuals tend to decide in favour of short-term and tangible benefits although being aware that there is a value to privacy. The research of Acquisti and Berendt deals with exactly this gap of stated preferences, i.e. the (partial) awareness of the consequences of giving away personal information, and actual behaviour [20,22]. Lack of information and transparency about the commercial or governmental usage of personal data often eases the individual's decision to disclose personal data [23].

Convenience aspects are one of the most important drivers for disclosing personal data [24, p. 4]. DCs offer a plethora of supposed advantages and seemingly free services to the DS in order to get hold of personal data.

Acquisti characterizes the benefits of disclosing personal information as relatively small and short-term rewards [20]. These include direct and indirect monetary incentives such as little gifts or discounts on products in exchange of the customer's personal data. All of these price deductions such as student, senior citizen and even volume discounts are part of a positive price discrimination strategy. But there are also immaterial rewards which can involve social benefits, e.g. when the DS tries to avoid peer-group pressure (particularly in social networks) by willingly sharing private information [23].

[10] The data subject's perception of these effects heavily depends on the information he/she receives and on previous experiences with privacy intrusions, the latter being called the "life cycle element" [19, pp. 31].

[11] The Dutch website PleaseRobMe.com highlights the dangers of sharing too much information on the Internet about your locations [21].

Furthermore, Lenard and Rubin argue that the very existence of the Internet as we know it today with a myriad of seemingly free services such as search engines, e-mail accounts, social networks, news, etc. heavily depends on consumers' willingness to disclose personal information [25, p. 163]. Taking these offers for granted, users underestimate the cost-benefit rationality that underlies the business models of many providers.

The trade-off between exchanging personal data and services mostly free of charge is based on an asymmetric allocation of information. Not knowing that their personal data is collected and processed, users are often deluded concerning their reasonable expectation. Since knowledge and education about the economic value of personal data plays a decisive role, a new form of digital divide, perhaps a "privacy divide", threatens to develop in society and the long-term need of a Privacy-E-inclusion of citizens could come into existence [26, p. 16].

Nevertheless from an economic point of view the increasing demand for goods like privacy or data protection would foster the supply and development of new technologies, laws and entrepreneurial codes of conduct as well as new business models which will offer new strategies to deal with privacy issues. It must be admitted, however, that there is little empirical evidence for a strong demand response.

In retaining personal information, the DS bears, of course, the costs of not-receiving the benefits for disclosing his/her personal data. In this case he/she is also part of a negative price discrimination not belonging to the group of preferred customers that enjoys discounts.

Since data protection implies to hold back certain information, individuals who are reluctant to disclose personal data could furthermore be suspected of being loners, freaks or weirdoes who have something to hide. In fact, the question why people would need privacy if they do not have anything (bizarre or illegal) to hide belongs to one of the classical arguments of DCs trying to camouflage their gain in power and profit by collecting information.[12] Here the classical but wrong statement "If you have nothing to hide..." becomes relevant [27].

However, communicating, exchanging opinions or sharing information represents an essential part of human behaviour and an important strategy to succeed in society. If you want to pursue a successful career in any field of work, networking belongs to one of the most relevant activities. That is why holding back information at a certain point of time could be disadvantageous. In the online world most of all social networks try to meet this demand of being easily, all the time and everywhere connected. Although most of the social interactions still take place in the off-line world, a trend towards more and more virtual interactions seems to be visible, especially if looking at the younger

[12] In an interview on the CNBC documentary "Inside the Mind of Google" in December 2009 Eric Schmidt, CEO of Google, was asked: "People are treating Google like their most trusted friend. Should they be?" Hitting the nail on the head, he responded: "I think judgment matters. If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place, but if you really need that kind of privacy, the reality is that search engines including Google do retain this information for some time, and it's important, for example, that we are all subject in the United States to the Patriot Act. It is possible that that information could be made available to the authorities." `http://www.youtube.com/watch?v=A6e7wfDHzew`, last accessed on 17 January 2011.

generation. Not sharing digital information could therefore lead to an isolation problem these days and even more probable in the future.

As already pointed out, the relevant literature does not specifically identify the economic advantages of maintaining informational privacy for the individual, because the concept of privacy does not generate easily quantifiable factors. Hence, difficult-to-quantify, privacy aspects are often excluded from the analysis [28].

Nonetheless, what can be seen as a benefit is that privacy serves as a defensive right against intrusions by others as well as a positive right enabling the DS to exercise control over his/her information. Westin names four functions of privacy: [7, pp. 32]

- First of all, there is personal autonomy, providing the individual with a core sphere where he/she is able to retreat not being controlled, manipulated or dominated by others, e.g. huge relevance concerning the secrecy of the ballot.
- Secondly, privacy serves as a safety valve which allows the individual to let his/her instinctual needs run more freely without having to fear embarrassment.
- Thirdly, self-evaluation and reflection can be carried out undisturbed in the private realm in order to develop one's personality and initiate learning processes. Additionally, innovative and creative thinking is spawned so that societies can continue to advance allowing their citizens to explore beyond the mainstream.
- Finally, limited and protected communication leads to an unstrained exchange of information supporting the right to free speech.

Again, it is obvious that these highly immaterial and long-term benefits for the individual are difficult to operationalise and quantify. However, they represent a crucial element in our analysis of the costs and benefits of privacy.

The data controller: DCs face a complex cost-benefit ratio in gathering, storing and exploiting the collected data as well. Although the boundaries are blurred, we should generally distinguish between sensitive (confidential) data of the corporation and collected personal information of individuals. This paper mainly deals with the latter.

Material and personnel costs of aggregating, storing and processing data represent first of all the most important direct expense factors. Although the software and hardware costs of aggregating, storing and processing data are constantly decreasing due to technological progress, the amount of data that needs to be stored and processed is skyrocketing at the same time so that data collecting companies face rapidly rising operating costs (e.g. for electric power supply). For this reason data centres are even built close to power plants or in cooler climates [29]. The energy issue becomes a more and more relevant topic, also because there is an apparent tendency towards retention of data, i.e., to collect more data than actually needed. This increases additionally the risk of overinvestment [30, p. 474].

Especially when you consider private data as a commodity that can be exploited by its owner, property rights should be furthermore taken into account as an indirect cost factor [31]. Confronted, moreover, with a complex body of rules and regulations concerning the collection, storage and usage of personal data, DCs will try to comply (at least to a certain degree) with these rules to avoid lawsuits and payments of compensations. Extra administrative and infrastructural expenses should therefore be considered.

Information security would represent one of these additional infrastructural cost factors. When storing personal data, most companies are obliged by law to protect the data through technical means (e.g. encryption) and access control measures. Moreover, back-ups and log files which show who accessed which data serve as another safeguard. Staff at all levels have to be trained how to use and manage data in a lawful way. If a company wishes to transfer data to a country outside the EU, there are serious regulatory hurdles to cross, not least of which is ensuring that the data will be adequately protected and respected to the same extent as in the European Union.

Besides, a company may need to respond to requests for access to their data by customers arguing that the data is not correct. The company will need to verify whether the data is correct or not. And when the data is compromised in some way, either through data breaches caused by a hacker attack, or when data is lost, then the DC faces a plethora of material and immaterial costs.

Data and privacy breaches can have devastating consequences for DCs. Immediate costs would include first of all the repair or replacement of the broken system while slowing down or even stopping whole business processes [32, p. 106]. If mandatory, data subjects have to be notified of the data breach, there is negative publicity, which in a long-term perspective can seriously damage the image and reputation of the data controller. Data protection authorities may require an inspection or audits, and eventually legal actions such as fines, compensations, torts or other liabilities could account for severe financial consequences for the DC.

Acquisti, Friedman and Telang have shown in their study that companies that experienced a privacy breach not only have to fear the loss of existing customers, but also suffer a statistically significant negative impact on the firm's stock exchange value [33, p. 1573]. However, stock prices tend to recover in a rather short period of time. Ultimately, privacy and data breaches can result in long-term damages for enterprises such as higher insurance premiums, severance of contractual relations, and, most importantly, an eventual harm to trust relationships with customers and/or suppliers.

Thus, DCs need to assess their security investment in relation to the probability of a privacy incident multiplied by the impact the problem will cause. Such a risk assessment is necessary in order to keep the right balance between an adequate level of data protection and an efficient and effective processing of the data [34,35]. When sanctions are unlikely or the costs of compensations do not surpass the financial benefits resulting from the collection and usage of personal data, DCs will tacitly accept these incidents and prefer to neglect privacy and data protections measures as frequently the case in these days.

Trying to exploit personal data commercially, companies aim to understand the mechanisms behind individual purchase behaviour in order to increase their profits from better market opportunities. To sell products and services, suppliers need to comprehend what their customers want or need, to stimulate the buyer's interest in their products or services and to be reasonably sure what a consumer (or different groups of customers) is willing to pay for the product or service. For this purpose many market players have been aggregating data, regardless of whether personal or non-personal, for a long time. Moreover, enterprises have collected even more data in the field of production and logistics succeeding in making the supply chain more efficient.

This general aim prevails in an age where the collection of more and more data becomes feasible and affordable due to the ever-decreasing costs for sensors, storage and computing power. The data comes from traditional sources such as loyalty cards and data trails in the Internet [36], but increasingly also from other sources such as RFID-tagged products or deep-packet inspection.

In selling personal data to third parties, companies run, of course, the risk of losing money if the added sales revenue is smaller than the benefits of providing services based on processing the personal data on their own.

There are numerous companies which found their business model on the processing of personal data creating consumer profiles and exploiting the results of their data analyses in order to make a huge profit [37]. Offering seemingly free services such as Internet searches, emails, news, games or social interaction, many Internet enterprises are part of an already huge and still rapidly growing online advertising industry [38].

3 Conclusion

This paper has presented three different approaches to privacy attempting to answer central questions such as: Why do we consider privacy as something worthy to protect? Is there a social value to privacy? Cui bono from privacy?

Although privacy is extremely context-dependent and often valued differently, the *ethical perspective* suggests that privacy represents an essential component of human identity. Trying to figure out, where the supposed human desire for privacy comes from, this section analyses a variety of antecedents tracing biological, anthropological, psychological and religious origins.

Territoriality and noxious reactions to overcrowding, for example, can be seen as biological factors causing sometimes a need for a certain degree of social distance. However, research on empathy and isolation also shows that human-beings are above all social creatures. Furthermore, notions of privacy can be found in most preliterate and modern societies, which indicates a universal value of privacy.

However, feminist anthropologists assume that privacy constitutes primarily a realm created by man in order to exert power over women. From a psychoanalytic point of view Freud helps us to realise that there is an unconscious dimension to privacy which lies beyond one's awareness.

Eventually, the influence of the early liberal movement on the notion of privacy has to be considered paving the way of today's negative and positive privacy right conception.

The *social perspective* aims to depict the tension between private and public. Being Hobbes' *homo homini lupus* and Aristotle's *zoon politicon* at once, humans face the *hedgehog's dilemma*, craving solitude and gregariousness at the time. However, privacy is not only challenged by the personal dilemma but also by conflicting social values such as national security, transparency or free speech. That is why a transparent and effectively designed balancing process must be followed in cases of curtailing privacy; otherwise, as for example Thomas Jefferson stated, there is a risk that "he who trades liberty for security [...] loses both."

The *economic perspective* resort to an actor-centred approach distinguishing between *data subject* (DS) and *data controller* (DC). In the case of the first a dual choice model of "disclosing" or "retaining" personal information presents the options of action, whereas the latter has to consider the costs and benefits of collecting, aggregating, storing and processing data as well as of potential privacy breaches.

In disclosing personal information, the DS is often confronted with costs that are neither easy to identify nor simple to operationalise and quantify. Nonetheless, more and more individuals are facing privacy problems resulting from their lax attitude towards sharing private information or being forced to disclose personal data. These problems include the risk of being a subject to social sorting or other discriminatory practices. Giving away personal information increases the threat for the DS of becoming a victim of online and offline crime. Other cost factors involve embarrassment, discomfort, annoyance, etc. But there are also a variety of benefits for the DS resulting from the disclosure of personal data. One of the most important advantages is an increased level of convenience meaning relatively small rewards such as discounts, free Internet services, etc. In retaining personal information, the DS bears, of course, the costs of not-receiving the benefits for disclosing his/her personal data. Since data protection implies to hold back certain information, individuals who are reluctant to disclose personal data could furthermore be suspected of being loners who want to hide something from the public. In today's digital society the refusal of sharing personal information could therefore easily lead to an isolation problem. Nonetheless, there are important benefits of retaining informational privacy. First of all, privacy serves in general as a defensive right against intrusions of others creating a protective sphere around the individual. Privacy as a positive right enables ideally the DS to exercise control over his/her information. Westin's four functions of privacy include personal autonomy, emotional release, self-evaluation and limited as well as protected communication.[7, pp. 32] Though mostly immaterial, these benefits are much more relevant, profound and complex than economic theory is being able to grasp.

The DC on the other hand faces various material and personnel expenses of aggregating, storing and processing personal data such as costs for property rights (if considered), compliance with state regulations and information security.

But in fact, the lucrative benefits outweigh the costs by far. The maxim *scientia potentia est* ("for also knowledge itself is power") could not be more appropriate explaining the strategy behind the DC's rampant collection behaviour of personal data. In the information society data itself has become one of the most valuable commodities. In analysing data of (potential) customers, companies, for instance, are far better off calculating and minimising risks. Aiming to understand the mechanisms behind individual purchase behaviour, commercial DCs are able to reduce transaction costs immensely. The rapidly growing online advertising industry is just one example of business that profits in a remarkable way from collecting digitally consumer information.

There is, however, a major downside to collecting personal data. Privacy and data breaches can have devastating consequences for DCs such as legal actions, slowing down or even stopping whole business processes, but also in a long-term perspective damaging the DC's image and trust relationships with customers as well as suppliers.

In conclusion, providing a comprehensive overview of three different perspectives, this paper attempts to contribute to a better understanding of privacy. The multidisciplinary analysis of privacy represents a difficult task since the different approaches have huge overlaps and are at least in parts difficult to distinguish from each other. Nonetheless, the interacting scientific points of view uncover neglected aspects and give revealing insights into the multifaceted concept of privacy. Summing up the most important findings of the different approaches, it seems that privacy has an intrinsic universal value that does not, however, stand for itself. Privacy is part of a complex social value system which components need to be kept in balance. Since economic theory reaches surprisingly fast its limits, ethical and social aspects needs to be integrated into the analysis. The economic discourse shows as well that privacy implies control and therefore power which the data subjects such as citizens but also consumers should be made aware of.

Acknowledgements

This work was carried out in the EU-funded FP7 project PRESCIENT: Privacy and Emerging Sciences and Technologies (SIS-CT-2009-244779). Important input came from David Wright (Trilateral Research & Consulting), Emilio Mordini and Silvia Venier (Centre for Science, Society and Citizenship). For more information see: `http://www.prescient-project.eu`

References

1. Nissenbaum, H.: Privacy as contextual integrity. Washington Law Review **79** (2004) 101–139
2. Friedewald, M., Wright, D., Gutwirth, S., Mordini, E.: Privacy, data protection and emerging sciences and technologies: Towards a common framework. Innovation: The European Journal of Social Science Research **23** (2010) 63–69
3. Ford, R.G., Krumme, D.W.: The analysis of space use patterns. Journal of Theoretical Biology **76** (1979) 125–155
4. de Waal, F.B.: Putting the altruism back into altruism: The evolution of empathy. Annual Review of Psychology **59** (2008) 279–300
5. Haney, C.: Mental health issues in long term solitary and supermax confinement. Crime and Delinquency **49** (2003) 124–156
6. Moore jr., B.: Privacy: Studies in social and cultural history. M.E. Sharpe, Armonk (1984)
7. Westin, A.F.: Privacy and freedom. Atheneum, New York (1967)
8. Friedan, B.: Feminist Mystique. W. W. Norton & Co., New York and London (1963)
9. Elshtain, J.B.: Public Man, Private Woman. Princeton University Press, Princeton (1981)
10. Pateman, C.: The Sexual Contract. Stanford University Press, Stanford (1988)
11. Freud, S.: Zeitgemässes über Krieg und Tod. Imago: Zeitschrift für Anwendung der Psychoanalyse auf die Geisteswissenschaften **4** (1915) 1–21
12. Freud, S.: Das Unheimliche. Imago: Zeitschrift für Anwendung der Psychoanalyse auf die Geisteswissenschaften **5** (1919) 297–324
13. Warren, S.D., Brandeis, L.D.: The right to privacy. Harvard Law Review **4** (1890) 193–220
14. Schopenhauer, A.: Parerga und Paralipomena: Kleine philosophische Schriften. Erster Band. Verlag A. W. Hahn, Berlin (1851)

15. Solove, D.J.: Understanding privacy. Harvard University Press, Cambridge, Mass. (2008)
16. Barak, A.: Proportionality and principled balancing. Law and Ethics of Human Rights **4** (2010) Article 1 http://www.bepress.com/cgi/viewcontent.cgi?article=1041&context=lehr.
17. Aquilina, K.: Public security versus privacy in technology law: A balancing act? Computer Law and Security Review **26** (2010) 130–143
18. Directive 95/46/EC of the European Parliament and of the Council of 24 october 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data. Official Journal of the European Communities **L 281** (1995) 31–50
19. Laufer, R.S., Wolfe, M.: Privacy as a concept and a social issue-multidimensional developmental theory. Journal of Social Issues **33** (1997) 22–42
20. Acquisti, A., Grossklags, J.: Privacy attitudes and privacy behavior: Losses, gains, and hyperbolic discounting. In Camp, L.J., Lewis, S., eds.: The Economics of Information Security. Kluwer, Dordrecht (2004) 165–178
21. Harvey, M.: PleaseRobMe website highlights dangers of telling world your location. The Times, 19 February (2010) http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article7032820.ece.
22. Berendt, B., Günther, O., Spiekermann, S.: Privacy in e-commerce: Stated preferences vs. actual behavior. Communication of the ACM **48** (2005) 101–106
23. Grimmelmann, J.: Privacy as product safety. Widener Law Journal **19** (2010) 793–827 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1560243.
24. Grossklags, J., Acquisti, A.: When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In: Proceedings of the Sixth Workshop on the Economics of Information Security (WEIS 2007), Pittsburgh, PA. (2007)
25. Lenard, T.M., Rubin, P.H.: In defense of data: Information and the costs of privacy. Policy and Internet **2** (2010) Article 7 http://www.psocommons.org/cgi/viewcontent.cgi?article=1035&context=policyandinternet.
26. Roussopoulos, M., Beslay, L., Bowden, C., Finocchiaro, G., Hansen, M., Langheinrich, M., Le Grand, G., Tsakona, K.: Technology-induced challenges in privacy and data protection in europe. A report by the ENISA ad hoc working group on privacy and technology, European Network and Information Security Agency, Heraklion (2008)
27. Solove, D.J.: "I've got nothing to hide" and other misunderstandings of privacy. St. Diego Law Review **44** (2008) 745–772 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565.
28. Swire, P.P.: Efficient confidentiality for privacy, security, and confidential business information. Brookings-Wharton Papers on Financial Services **2003** (2003) 273–310
29. Harizopoulos, S., Shah, M.A., Meza, J., Ranganathan, P.: Energy efficiency: The new holy grail of data management systems research. In: 4th Biennial Conference on Innovative Data Systems Research (CIDR), January 4-7, 2009, Asilomar, California, USA. (2009)
30. Hui, K.L., Png, I.: The economics of privacy. In Hendershott, T., ed.: Economics and Information Systems. Volume 1 of Handbooks in Information Systems. Elsevier Science, Amsterdam (2006) 471–498
31. Volkman, R.: Privacy as life, liberty, property. Ethics and Information Technology **5** (2003) 199–210
32. Tsiakis, T., Stephanides, G.: The economic approach of information security. Computers & Security **24** (2005) 105–108
33. Acquisti, A., Friedman, A., Telang, R.: Is there a cost to privacy breaches? An event story. In: The Fifth Workshop on the Economics of Information Security (WEIS 2006), Cambridge UK (2006)

34. Sonnenreich, W., Albanese, J., Stout, B.: Return on security investment (rosi) - a practical quantitative model. Journal of Research and Practice in Information Technology **38** (2006) 45–56
35. Anderson, R.J., Moore, T.: The economics of information security. Science **314** (2006) 610–613
36. Graeff, T.R., Harmon, S.: Collecting and using personal data: consumers' awareness and concerns. Journal of Consumer Marketing **19** (2002)
37. Hildebrandt, M., Gutwirth, S.: Profiling the European Citizen: Cross-Disciplinary Perspectives. Springer, Dordrecht (2008)
38. Evans, D.S.: The online advertising industry: Economics, evolution, and privacy. Journal of Economic Perspectives **23** (2009) 37–60