Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 6 (2011) pp. 432–442

Cui Bono from Giving up or Protecting Privacy? A Basic Decision Theoretic Model

Philip Schütz and Michael Friedewald

Fraunhofer Institute for Systems and Innovation Research,
Breslauer Straße 48, 76139 Karlsruhe, Germany
{philip.schuetz;michael.friedewald}@isi.fraunhofer.de

Abstract: **The economic perspective on privacy presented in this paper resorts to an actor-centred approach deploying a cost-benefit analysis for the data subject and the data controller. In the course of this analysis a basic decision theoretic model is presented. Whereas the data subject faces the choice of "disclosing" or "retaining" personal information, the data controller has to consider the costs and benefits of collecting, aggregating, storing and processing data as well as of potential privacy breaches.**
Keywords: Privacy, data protection, impact assessment, economics

I. Introduction

Privacy advocates mostly confine their analyses of new technologies to dystopian scenarios in which surveillance societies threaten individual autonomy. Despite the eligibility of this perspective, it consistently neglects the fact that a plethora of different actors in society today actually profits from these sometimes privacy-infringing technologies in various ways.
Therefore, this paper not only tries to identify the costs but also aims to shed light on the benefits of disclosing personal data. Next to the data subject's point of view the cost-benefit analysis comprises the perspective of the data controller. In the course of this work a basic decision theoretic model for each one of these actors is developed, which ideally can contribute to a better understanding of the economic calculus of the individual as well as the private sector behind disclosing as well as processing personal data.
Although the notion of privacy in the economic discourse is mainly understood as informational privacy dealing with data protection issues, this economic approach has tried to consider additionally the costs and benefits beyond the mere perfect/imperfect information topos of economic theory.

II. Theoretical background

The background of our analysis is the concept of information economics, which is a branch of (neoclassical) microeconomic theory that studies how information affects an economy and economic decisions. In our context information economics mainly deals with two issues: *information asymmetry* and *information goods*.
Information asymmetries are related to decisions in transactions where one party has more or better information than the other. This creates a power imbalance in transactions. For George J. Stigler, one of the key leaders of the Chicago School of Economics and the intellectual fathers of information economics, privacy is one factor that increases information asymmetries because one party can retain (personal) information that might be important for the decision making of the other party [37, 43]. The existence of such information asymmetries gives rise to problems such as moral hazard[1] and adverse selection.[2] For these reasons orthodox neoclassic theory considers the protection of personal data as an undesirable market disturbance.
In recent years *behavioural economics* has extended the understanding of (economic) decision making of individuals and institutions beyond the paradigm of rational choice. Building on Herbert Simon's theory of bounded rationality [33], behavioural economics take into account that social, cognitive and emotional factors are important, especially when decisions are made under risk and uncertainty. In this context researchers such as Alessandro Acquisti explore empirically the preconditions under which individuals are trading privacy (or rather personal data) for other benefits [3].
The other important development is that (private) information is increasingly becoming a commodity and the basis of new types of businesses. These include typical information services ranging from search engines and personalised advertising to sophisticated data mining services [8].
Especially with regard to privacy-enhancing technologies (PETs) discussions are often focussed to the question of "return on investment": What are the quantifiable costs and benefits resulting either from a privacy breach event or from the deployment of PETs? In many respects the discussion about the economics of privacy is closely related to the one on the economics of information security and we have made extensive use of the existing literature on the latter issue. However, the question of ROI is often hampered by the lack of reliable data about the real costs of privacy or data security events as well as the intangible nature of the "costs" (such as loss of trust) that are hard to quantify. We are trying to summarise the scattered research that are available [32].

[1] Moral hazard occurs when a party insulated from risk behaves differently than it would behave if it were fully exposed to the risk.

[2] Adverse selection refers to a market process in which "bad" results occur when buyers and sellers have access to different information and the "bad" products or customers are more likely to be selected. See for instance [6].

Consequently, this paper is taking a closer look at the main actors protecting and intruding upon privacy, developing a cost-benefit matrix from these two different perspectives. Although economic aspects of privacy are mostly restricted to data protection, this paper tries to consider the costs and benefits beyond the mere perfect/imperfect information topos of economic theory. However, the focus remains on the economic value of data protection.
That is why the actor-centred approach embraces on the one hand the data subject being confronted with the choice of either disclosing or retaining personal information accordingly giving away or protecting privacy, and on the other hand the data controller, who faces the costs and benefits of collecting, aggregating, storing and processing personal data as well as of privacy breaches.
In most cases we also follow the neoclassic assumption that the data subjects' as well as the data controllers' decisions are based on rationale choice, carefully balancing the costs and benefits and aiming for the maximum profit.

III. Data subject-centred approaches

The European Data Protection Directive does not directly define the term data subject. Instead in Art. 2 (a) the Directive 95/46/EC [1] concentrates on personal data which

> "mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

Since the Directive refers to the data subject as a natural person, we also concentrate on data protection and privacy issues of individuals, leaving aside classical economic concepts which consider sensitive and confidential corporate as well as governmental data such as trade, industrial or state secrets as part of the information asymmetry problem.[3]
By acting in a supposed private or public sphere, individuals are constantly disclosing information about themselves. However, in many instances, they are actually able to choose between disclosing and 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 their privacy. The research of Alessandro Acquisti and Sarah Spiekermann, which empirically integrates a behavioural account of the individual perception of privacy, deals with exactly this "privacy paradox", namely the gap between stated preferences, i.e. the (partial) awareness of consequences (of disclosing personal information), and actual behaviour [5, 2, 11].[4] Additionally, the lack of information and transparency about the commercial or governmental usage of personal data often eases the consumer's decision to give up privacy [19].

A. Costs for the data subject

There are apparently two types of costs as there are two types of benefits resulting from disclosing and retaining personal data (cf. Figure 1).

1) Costs of disclosing personal data

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. In addition to the immense context-dependency and subjectivity, privacy incidents often do have indirect and long-term effects on the individual.[5] Consequences are therefore hard to anticipate and it seems that individuals perceive long-term impacts as an indirect, controllable and less perilous harm to themselves. That's why the data subject often underestimates or does not consider the long-term risks in giving away personal information [5].
However, more and more individuals are confronted with privacy problems frequently resulting from their lax attitude towards sharing personal data or being forced to disclose private information (e.g. in order to benefit from certain online services). Trying to create a bigger picture of the real person behind the collected data, data controllers sort the information into "baskets" to be able to create groups of persons sharing certain attributes. This sorting process, which is eventually used to classify the data subjects as accurately as possible, increases the risk for the individual to become a victim of social sorting and discrimination practices – especially since the profiling remains incomplete and error-prone. Deducing the social status from the zip code of the data subject, for example, data controllers can privilege high value customers through more solicitous attention and better offers. Those of low value would be consequently given fewer options. But also people of ethnic or religious minorities can become the target of discriminatory practices if sensitive data about them is disclosed. This is no new development – merchants have always made a distinction between good and bad customers - but the collection of ever more personal data makes this practice more pervasive and useful for the data processors.
Another consequence of sharing voluntarily or involuntarily personal data such as pictures involves that peers, colleagues or prospective employers form an opinion about the data subject based on a one-time superficial and maybe misleading impression. They might think that the data subject is stupid, naïve, silly, ridiculous or juvenile. Over time, people may recognise that their exuberance for sharing personal information has consequences when, for example, they go job-hunting and become concerned that prospective employers might see embarrassing pictures or misleading com-

[3] Already Alan Westin has coined the term organisational privacy in contrast to individual privacy. According to Westin [50] privacy is not necessarily a claim of individuals but also of groups or institutions "to determine for themselves when, how, and to what extent information about them is communicated to others" . Interestingly, already Westin concentrates in his theoretical work about privacy on the information topos. Bennett and Raab [10] also apply the concept of privacy to groups of people or corporations.

[4] The average willingness-to-accept (a proposal to sell personal data) is dramatically higher than the average willinness-to-protect (paying for protection of personal data) [20].

[5] The data subject's perception of these effects heavily depends on the information he/she receives and on previous experiences with privacy intrusions. Laufer and Wolfe [30] for instance deal with the latter aspect, which they call the "life cycle element".

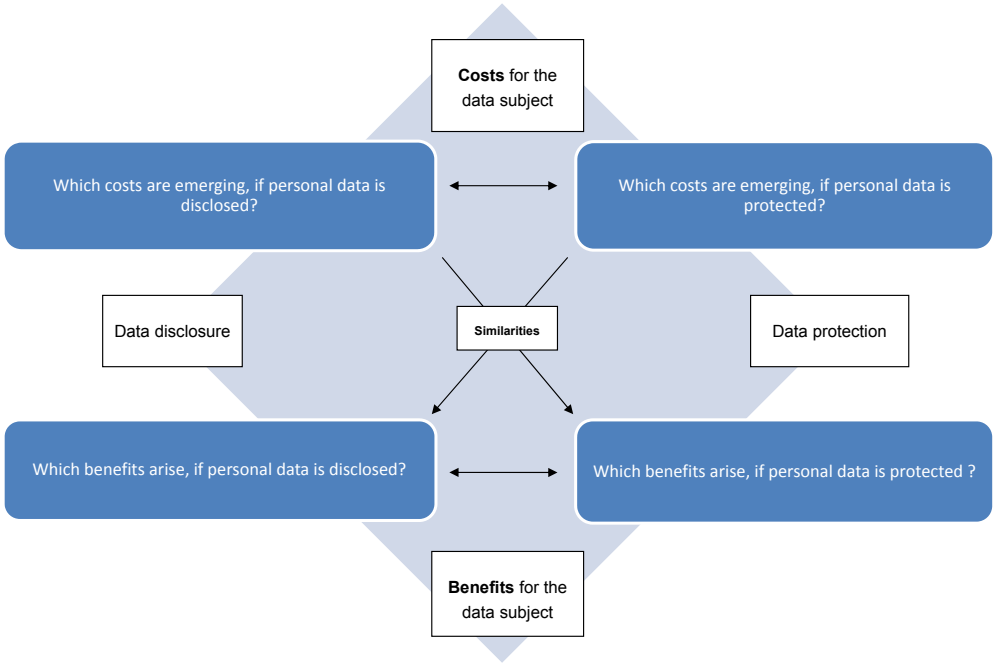

Figure. 1: **Perspective of the data subject**

ments on the wall of one's social network profile site. A survey released in March 2010 by the University of California, Berkeley, found that more than half of the young adults questioned had become more concerned about privacy than they were five years ago [25]. However, in a highly controversial project on individual medicine the same university is offering a genetic test free of charge to each freshmen and transfer student [27].

Similarly a German study concluded out that only 20 per cent of teenage users in Internet communities, compared to 50 percent of all members in online communities, provide their real name as an identity in these communities. This result suggests a higher degree of teenage sensitivity towards the need of protecting and managing their identity [13].

Furthermore, the disclosure of personal information leads to an increasing risk to become the victim of online or offline crime. If the data subject uses for example Foursquare or Twitter to tell his/her "friends" that he/she is on holidays in Greece, it's possible that burglars may be cruising Foursquare and Twitter for exactly that kind of information. A Dutch website has shown how easy it is to compile such information. PleaseRobMe.com highlights the dangers of sharing too much information on the Internet about our locations.[6] Another threat lies in identity theft which can be executed with even minimal amounts of personal data[7], such as birth dates, national insurance numbers, credit card numbers or passwords. Identity theft may have a hugely deleterious effect on their victims, psychologically as well as financially. Moreover, with easy access to our personal data particularly Internet users can become victims of cyber-stalking, bullying, character assassination and other forms of harassment.[8]

A further category of costs as a consequence of disclosing personal information involves emotional disturbances of the data subject. Being regularly spammed and exposed to constant exhortations can result in an unpleasant and stressful feeling of annoyance. Although advocates emphasise the greater usefulness of personalised advertisement for the individual, advertisement recipients are mainly, as philosopher Ira Singer [39] states, reduced to "a bundle of desires", that needs to be triggered in order to sell products or services. In a long-term perspective, particularly personalised and targeted advertising threatens to manipulate human decision-making to fit the picture of "being a bundle of desires", diminishing people's capacities of reasoned choice and thoughtful action. Thus, Singer's work also links privacy to personal development.

Evoked by sharing sensitive information with people or corporations which were initially considered trustworthy, discomfort and embarrassment represent another emotional disturbance. In addition, algorithms and data processing programs allow data controllers to confront Internet users with personalised online advertisement such as invitations to Facebook including pictures of actual off-line friends, which leave a bitter and sometimes even frightening aftertaste, re-

[6]The site's developers say they don't want to encourage criminals, only to remind people that sharing information on the Internet carries risks [22]. Another newspaper article reports about the police, warning Internet users to post their whereabouts on websites such as Twitter or Facebook, after two men were convicted of burgling a house whose owners had publicised the fact they were away on the Internet. As a reaction insurers are warning their clients that they would face higher insurance premiums if they are victims of burglary resulting from the online advertisement about their location [12].

[7]When two separate pieces of seemingly non-personal data are brought together in the process of aggregating and processing, they might be sufficient to identify an individual as Latanya Sweeney [44] has shown. In addition, what is today regarded as non-personal data might give relevant hints to identify the data subject in the future.

[8]Law enforcement officials and safety groups have focused on the Internet as an arena for such types of harassment as false impersonation and character assassination as more people voluntarily place their private lives on public display through websites such as Facebook.com and MySpace.com. But a little-discussed and more threatening phenomenon is also happening to the unwitting online, i.e. "cyber-stalking and the illegal monitoring of private information and communication of ex-lovers and spouses as a form of domestic violence" [29].

flecting too much knowledge about the advertisement recipient [47].
Having mentioned all these examples, it is nonetheless eye-catching that mainstream economic literature does not explore in-depth the imperative and necessity of privacy, which is taken for granted (What does the data subject actually lose in case of giving up privacy?).
This obvious lack of analysis and explanation of the very essence and value of privacy in economic literature derives from the fact that economists mainly focus on easily quantifiable factors. Peter Swire [45] states that

> "a variable such as the taste for privacy is 'soft' in the sense that it is difficult to quantify. In any quantitative estimates of costs and benefits, the soft variables can readily be excluded from the main analysis. Even important variables can thus be treated as an afterthought when they do not fit neatly into the analytic structure."

For this reason economists frequently equate privacy with data protection in order to evade operationalisation and quantification problems of privacy. From this point of view data protection can consequently be seen as part of the perfect/imperfect information topos of economic theory.
But there is more to privacy and data protection issues. That is why key questions remain the same: If you give away personal data, is an unpleasant feeling a cost factor? If yes, how do you deal with these "soft" variables? How do you measure and assess the risk of potential long-term effects of disclosing private information in a social network about, for example, your lax attitude towards drugs, which could result in a potential threat to your working career, if your employer discovers this information?
It is obvious that additionally a rather ethical and social interpretation of privacy is needed to fill these blanks and to deduce a broad spectrum of "soft" and "hard" cost factors for the individual arising from intruding upon his/her privacy.

2) Costs of retaining personal data and privacy

Costs of retaining and benefits of disclosing personal data are two sides of the same coin. Not receiving the benefit when disclosing personal data can therefore also be seen as a cost factor when retaining personal data.
Price discrimination or differential pricing, which can have a positive as well as a negative effect for the consumer, represents an excellent example of these two sides. If disclosing personal data is the condition of receiving products for a better price, then retaining private data inevitably leads to higher costs.
Lenard and Rubin [31] speculate that today's intensive collection in connection with new digital statistical analysis methods makes categorising and consequently discrimination of consumers even easier. Nonetheless differential pricing represents an important strategy to establish "niche" products which would otherwise not survive in a highly competitive market. Particularly informational goods, which involve high fixed costs (for their development) and low marginal costs (for their reproduction), depend on and therefore often avail themselves of such a strategy.
Since data protection implies to hold back certain information, a person who is reluctant to disclose personal data could furthermore be suspected of being a loner, a freak or weirdo who has something to hide. In fact, the question why people would need privacy if they do not have anything (strange or illegal) to hide belongs to one of the classical arguments of data controllers trying to camouflage their gain in power and profit by collecting information[9]. Here the classical but wrong statement "If you have nothing to hide…" becomes relevant [40].
However, communicating, exchanging 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 generation. Not sharing digital information could therefore very well lead to an isolation problem these days and even more probable in the future.

B. Benefits for the data subject

As there are two types of costs resulting from disclosing and retaining personal data, there are also two types of benefits (cf. figure 1).

1) Benefits of disclosing data

Convenience aspects are one of the most important drivers for disclosing personal data [20]. Data controllers offer a plethora of supposed advantages and seemingly free services to the data subject in order to get hold of personal data.
Acquisti [5] characterizes the benefits of disclosing personal data as relatively small and short-term rewards . 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 citizens 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 individual seeks to avoid peer group pressure (particularly in social networks) by willingly sharing private information.
Moreover, Lenard and Rubin [31] 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 the willingness to disclose personal information. Taking these

[9] 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." Cf.: http://www.youtube.com/watch?v=A6e7wfDHzew.

offers regularly for granted, users underestimate the cost-benefit rationality that underlies the business models of many Internet firms.
However, exchanging personal data and services mostly free of charge, the trade-off between user and provider 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 education plays an important role in order to understand these economic mechanisms behind the collection of personal data, a new form of digital divide, perhaps a "privacy divide", threatens to develop and the long-term need of a Privacy-E-inclusion of citizens could come into existence [38].
Nevertheless, from an economic point of view the increasing demand for privacy or data protection fosters the supply and development of new technologies, laws and entrepreneurial codes which will offer new strategies to deal with privacy issues. It must be admitted, however, that – at least in the case of privacy-enhancing technologies – there is little empirical evidence for a strong demand response [32].
The journalist Jeff Jarvis [28] goes even further in arguing that Internet users would create the benefit of transparency for the whole society if they all gave up their exaggerated expectation of privacy protection. Emphasising the social value of reducing privacy standards, Jarvis argues that the Internet as a public place needs to remain public (vs. private), transparent (vs. opaque), open (vs. closed) and free (vs. controlled). This obviously daring postulate stands in sharp contrast with the intrinsic and social value of privacy described by Solove [41] but in line with influential Internet entrepreneurs such as Eric Schmidt (Google), Mark Zuckerberg (Facebook) or Scott McNealy (Sun Microsystems).

2) Benefits of retaining personal data and privacy

As already pointed out earlier, the relevant literature does not specifically identify the economic advantages of maintaining informational privacy for the individual. From a legal philosophical point of view the concept of privacy mainly consists of a negative and a positive right. The first serves as a defensive right of the individual against intrusion of the state, but also of private corporations and other individuals. This idea comprises the *right to be left alone*, which leads back to Samuel Warren and Louis Brandeis' [49] seminal essay "The Right to Privacy".
Whereas the negative right to privacy creates a protective sphere around the individual, privacy as a positive right is supposed to enable the individual to exercise power and control over his/her personal and private information. According to Alan Westin this form of (informational) privacy has four functions:

- 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.
- Secondly, privacy serves as a safety valve which enables the individual to release his/her emotions not having to fear any 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 are difficult to operationalise and quantify. However, they represent a crucial element in our analysis of the costs and benefits of privacy.

IV. Data controller-oriented approaches

Data controllers[10] such as governments, other public bodies as well as private businesses and individuals face a complex cost-benefit ratio in gathering, storing and exploiting collected data. Although the boundaries are blurred, we should generally distinguish between sensitive (confidential) data of the corporation and collected personal information of individuals. The following sections mainly deal with the latter.

A. Direct and indirect costs for collecting data

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 a rapidly rising demand of investments and also operating costs (e.g. for electric power supply). For this reason data centres are even built close to power plants or in cooler climates [21]. The energy issue becomes a more and more relevant topic, because one can observe a tendency towards retention of data, i.e., to collect more data than is actually needed; this increases the risk of overinvestment [26]. The rationale behind this is that "the value [of personal data] is unknown until well after the time of capture" and that it is "potentially valuable later" [14].
Especially when you consider private data as a commodity that can be exploited by its owner, property rights should be considered as an indirect cost factor [51, 48]. Confronted, moreover, with a complex body of rules and regulations concerning the collection, storage and usage of personal data, data controllers will try to comply (at least to a certain degree) with these rules to avoid lawsuits and payments of compensations. Even though varying from country to country, these regulations normally group around the basic data protection principles such as notice, choice, purpose specifica-

[10] According to article 2(d) of Directive 95/46/EC "[Data] 'controller' shall mean 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..." [1]. Even though public data controllers are of the utmost importance representing the largest and most powerful data collectors, they are mainly left out of the analysis of this paper. The same applies for individuals in this context.

Table 1: Costs and benefits for the data subject

	Costs for the data subject	**Benefits for the data subject**
Disclosing Personal Data — Giving away Privacy	• Risk of long-term effects – Being a victim of social sorting and discrimination – Peers, colleagues or prospective employers may form a negative opinion about the data subject • Increasing risk of being the victim of on- and offline crimes – Burglary – Identity theft – Cyber-stalking, bullying, character assassination and other forms of harassment • Emotional disturbance – Feeling annoyed by e.g. unsolicited advertisement – Discomfort and embarrassment – Feeling scared when e.g. advertisement reflects too much knowledge about yourself (uncanny valley)	• Convenience aspects – Small, often material rewards – "Positive" (price) discrimination – Avoiding peer group pressure – Free Internet services – Fun and entertainment • Networking which strengthens our personal relations and increases the probability of receiving potentially valuable information
Retaining Personal Data — Protecting Privacy	• „Negative" price discrimination • Isolation • (Privacy enhancing technologies)	• Defensive right against intrusion from the state, private corporations or individuals • Westin's four functions of privacy: – Personal autonomy – Emotional release – Self-evaluation – Limited and protected communication • Personal development [39] • Being able to go beyond the main-stream (support of creativity and innovative thinking)

tion, use limitation, access and security safeguards.[11] Extra administrative and infrastructural expenses should therefore be considered. For instance when data controllers want to use the personal data in another way than originally agreed on, they are obliged to contact and seek consent with the data subject again. Furthermore, building up databases with personal information may involve the notification of data protection authorities as well as the formulation of a corporate policy on privacy, which needs to be thoroughly elaborated and put on the corporate website.

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 has 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. Customers may argue 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 data controller faces a plethora of material and immaterial costs.

B. Costs of privacy breaches

Data and privacy breaches can have devastating consequences for data controllers. Immediate costs would include first of all the repair or replacement of the broken system while slowing down or even stopping whole business processes [46].

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 data controller.

Acquisti, Friedman and Telang [4] have shown in a study that companies which 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. 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, data controllers need to assess their security investment in relation to the probability of an incident that produces some of the discussed consequences, multiplied by the impact the problem will cause [4, 32]. 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 [42, 7]. When sanctions are unlikely or the cost of compensations do not surpass the investment costs, this can also lead to the situation that data controllers take these incidents into account and prefer to neglect privacy and data protections measures.

C. Benefits of aggregating, storing and processing data

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, supplier need to comprehend what their customers want or need, to stimulate the buyer's interest in their products or services, to be reasonably sure what a consumer (or different groups of customers) is willing to pay for the product or service, and much more.

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 and used it for 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 [18], but increasingly also from other sources such as RFID-tagged products or deep-package inspection.[12] In order to give an impression of the monetary value of personal data, the following table gives an overview of the typical market value of legally and illegally collected data.

Table 2: (Underground) value of data [16]

Data item	Range of prices
Credit card information	\$0.85 – \$30
Bank account credentials	\$15 – \$850
Email accounts	\$1 – \$20
Email addresses	\$1.70/MB – \$15/MB
Shell scripts	\$2 – \$5
Full identities	\$0.70 – \$20
Credit card dumps	\$4 – \$150
Mailers	\$4 – \$10
Cash-out services	\$0 – \$600 plus 50 – 60 per cent
Website administration credentials	\$2 – \$30

In addition, many market players even collect data that they do not use at the moment because it is evident that collected data is potentially valuable later, either for optimising the own processes or as a trade good that can be sold to others. This strategy, as already mentioned, carries a high risk of overinvestment collecting potentially valuable or even useless information goods [24]. In selling personal data to third

[11] These principles comprise concepts of the OECD [34] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as well as a report on Privacy online to the FTC [35].

[12] Deep packet inspection is a form of inspecting, filtering or examining computer network packets, the data they carry and/or the header part of a packet. The packet can be inspected for viruses, spam, tampering, denial-of-service attacks or other criteria to decide if the packet passes inspection and can be sent on to its destination or if it needs to be routed to a different destination. Deep packet inspection can be used in support of different functions or applications including security, data mining, eavesdropping, censorship, anti-piracy – and targeted advertising. A packet can then be redirected, tagged, blocked or reported to some other agent in the network [9].

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 its 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 [23]. Offering seemingly free services such as Internet searches, emails, news, games or social interaction, many Internet enterprises are more or less part of an already influential but still rapidly growing online advertising industry [15].

Next to online advertisement particularly insurance companies aim at a comprehensive collection of information about their potential customers in order to calculate and minimise risks of their contract offers.

Furthermore, location based services (LBS) combine geographic data with information of public institutions or private businesses such as shops, restaurants, various services but also individuals. Spreading rapidly all over the world, mobile devices enable LBS to localise data subjects more and more precise. Deploying LBS, users are able to orientate themselves in a much faster and easier fashion. However, the private as well as the public sector are extremely interested in knowing where potential customers or criminals sojourn.

Other application areas of processing personal data are data mining services for market research (e.g. market basket analysis). But also quasi-public actors such as political parties are interested in data mining results which in the case of psephology helps them to analyse and control their electoral performances. Besides, law enforcement agencies and public administrations apply data mining on a grand scale (as in the suspended US Total Information Awareness program) in order to fight organised crime and terrorism. In these cases national security represents the often named benefit for the individual and society, justifying the aggregation, storing and processing of personal data [36].

V. Conclusions

The economic perspective on privacy presented in this paper resorts to an actor-centred approach distinguishing between data subject and data controller. 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 data subject 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 data subject of becoming a victim of online as well as offline crime. Other cost factors involve embarrassment, discomfort, annoyance, etc. But there are also a variety of benefits for the data subject 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 data subject 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 data subject 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. Though mostly immaterial, these benefits are much more relevant, profound and complex than economic theory is being able to grasp.

The data controller 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 data controller'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 data controllers 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 data controllers such as legal actions, slowing down or even stopping whole business processes, but also in a long-term perspective damaging the data controllers' image and trust relationships with customers as well as suppliers.

In a nutshell, there seems to be a deep-rooted conflict of interests when it comes to retaining personal data, not only on the public and private data controller side, but also concerning data subjects. This paper has shown that all of these actors benefit at least to some extent from the disclosure of personal data. However, there is a striking asymmetry e.g. in awareness of what data is actually processed, in access opportunities of this data and eventually the economic profit resulting from the data collection. Considering the importance of a sustainable and long-term relationship not only between consumer and (service) provider but also citizen and state, based on trust, the authors of this work are of the opinion that data subjects as well as data controllers have an interest in reducing that asymmetry.

Table 3: Costs and benefits for the data controller

	Costs for the data controller	**Benefits for the data controller**
Collecting, Aggregating, Storing, Processing Data	• Material and personnel costs • Property rights (license and usage fees) • Costs for compliance with state regulations • Costs of information security • Losing customers due to annoyance or intimidation • Risk of overinvestment	• Effective calculation and minimisation of risks (greater predictability) • Better exploitation of market opportunities (more complete market information), e.g. knowledge of consumer preferences and ability to offer personalised services • Selling of personal data or associated analysis results to third parties
Privacy Breaches	• Costs for repair or modifying the affected system • Stopping or slowing down business processes • Fines, compensations, torts or other liabilities • Loss of existing customers • Harm to trust relationships • Loss of reputation	• NONE

Acknowledgement

This work was carried out in the EU-funded FP7 project PRESCIENT: Privacy and Emerging Sciences and Technologies (SIS-CT-2009-244779). For an overview of the project see [17].

References

[1] "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 28, pp. 31–50, 23 November 1995.

[2] A. Acquisti and J. Grossklags. "Privacy and rationality in individual decision making", *IEEE Security and Privacy*, 3(1), pp. 26–33, 2005.

[3] A. Acquisti. "Nudging privacy: The behavioral economics of personal information", *IEEE Security & Privacy*, 7(6), pp. 82–85, 2009.

[4] A. Acquisti, A. Friedman, R. Telang. "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.

[5] A. Acquisti, J. Grossklags. "Privacy attitudes and privacy behavior: Losses, gains, and hyperbolic discounting", In *The Economics of Information Security*, L. J. Camp, S. Lewis (eds.), Kluwer, Dordrecht, 2004.

[6] G. A. Akerlof. "The market for 'lemons': Quality uncertainty and the market mechanism", *The Quarterly Journal of Economics*, 84(3), pp. 488–500, 1970.

[7] R. J. Anderson, T. Moore. "The economics of information security", *Science*, 314(5799), pp. 610–613, 2006.

[8] S. Baker. *The Numerati: In Which They'll Get My Number and Yours*. Houghton Mufflin, New York, 2008.

[9] R. Bendrath, M. Mueller. "The end of the net as we know it? Deep packet inspection and Internet governance", In *Annual Meeting of the American Political Science Association, Washington, D.C., 2-5 September 2010*, 2010.

[10] C. J. Bennett, C. D. Raab. *The Governance of Privacy: Policy Instruments in Global Perspective*. MIT Press, Cambridge, Mass. and London, 2nd ed., 2006.

[11] B. Berendt, O. Günther, S. Spiekermann. "Privacy in e-commerce: Stated preferences vs. actual behavior", *Communication of the ACM*, 48(3), pp. 101–106, 2005.

[12] N. Britten. "Facebook users warned of burglary risk", *The daily telegraph*, 15 Sep 2010. http://www.telegraph.co.uk/technology/facebook/8004716/Facebook-users-warned-of-burglary-risk.html.

[13] K Busemann, Ch. Gscheidle. "Ergebnisse der ARD/ZDF-Onlinestudie 2010, Web 2.0: Nutzung steigt – Interesse an aktiver Teilhabe sinkt", *Media Perspektiven*, 2010(7-8), pp. 359–368, 2010.

[14] R. Cooke, K. Scruggs. Smart surveillance - effective information for public safety. In *30th Annual Law Enforcement Information Management Conference, Grapevine, TX June 5-9, 2006*, 2006.

[15] D. S. Evans. "The online advertising industry: Economics, evolution, and privacy", *Journal of Economic Perspectives*, 23(3), pp. 37–60, 2009.

[16] M. Fossi, D. Turner, E. Johnson, T. Mack, T. Adams, J. Blackbird, B. Graveland, D. McKinney, J. Mulcahy, C. Wueest. *Symantec Global Internet Security Threat Report, Volume XV*. Symantec Corporation, April 2010.

[17] M. Friedewald, D. Wright, S. Gutwirth, E. Mordini. "Privacy, data protection and emerging sciences and technologies: Towards a common framework", *Innovation: The European Journal of Social Science Research*, 23(1), pp. 63–69, 2010.

[18] T. R. Graeff, S. Harmon. "Collecting and using personal data: consumers' awareness and concerns", *Journal of Consumer Marketing*, 19(4), pp. 302-318, 2002.

[19] J. Grimmelmann. "Privacy as product safety", *Widener Law Journal*, 19, pp. 793–827, 2010.

[20] J. Grossklags, A. Acquisti. "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.

[21] S. Harizopoulos, M. A. Shah, J. Meza, P. Ranganathan. "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.

[22] M. Harvey. "PleaseRobMe website highlights dangers of telling world your location", *The Times*, 19 Feb 2010. http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article7032820.ece.

[23] M. Hildebrandt, S. Gutwirth. *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008.

[24] J. Hirshleifer. "Private and social value of information and reward to inventive activity", *American Economic Review*, 61(4), pp. 561–574, 1971.

[25] L. M. Holson. "Tell-all generation learns to keep things offline", *The New York Times*, 8 May 2010. http://www.nytimes.com/2010/05/09/fashion/09privacy.html?ref=global-home.

[26] K.-L. Hui and I.P.L. Png. "The economics of privacy", In *Economics and Information Systems*, T. Hendershott (ed.), Elsevier Science, Amsterdam, 2006.

[27] F. Jabr. "Exposing the student body: Stanford joins U.C. Berkeley in controversial genetic testing of students", *Scientific American online*, 6 July 2010. http://www.scientificamerican.com/article.cfm?id=exposing-the-student-body

[28] J. Jarvis. "The German paradox", *YouTube video*, April 2010. http://www.buzzmachine.com/2010/04/.

[29] C. L. Jenkins. "Stalkers go high tech to intimidate victims", *The Washington Post*, 14 April 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/04/13/AR2007041302392.html.

[30] R. S. Laufer and M. Wolfe. "Privacy as a concept and a social issue-multidimensional developmental theory", *Journal of Social Issues*, 33(3), pp. 22–42, 1997.

[31] T. M. Lenard, P. H. Rubin. "In defense of data: Information and the costs of privacy", *Policy and Internet*, 2(1), Article 7, 2010.

[32] London Economics. "Study on the economic benefits of privacy-enhancing technologies (PETs)", *Final report to the European Commission, DG Justice, Freedom and Security*, July 2010.

[33] K. D. Miller. Simon and Polanyi on rationality and knowledge. *Organization Studies*, 29(7), pp. 933–955, 2008.

[34] OECD. *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*. Organisation for Economic Co-operation and Development, Paris, 1980.

[35] R. Pitofsky, M. L. Azcuenaga, S. F. Anthony, M. W. Thompson, O. Swindle. "Privacy online", *Report to Congress*, Federal Trade Commission, June 1998.

[36] R. Popp and J. Poindexter. "Countering terrorism through information and privacy protection technologies", *IEEE Security and Privacy*, 4(6), pp. 18–27, 2006.

[37] R. A. Posner. "The economic theory of privacy", *Regulation*, 9(3), p. 19–26, 1978.

[38] M. Roussopoulos, L. Beslay, C. Bowden, G. Finocchiaro, M. Hansen, M. Langheinrich, G. Le Grand, K. Tsakona. "Technology-induced challenges in privacy and data protection in Europe", *Report by the ENISA ad hoc working group on privacy and technology*, European Network and Information Security Agency, Heraklion, July 2008.

[39] I. J. Singer. "Privacy and human nature", *Ends and Means*, 5(1), 2001. http://www.abdn.ac.uk/philosophy/endsandmeans/vol5no1/singer.shtml.

[40] D. J. Solove. "'I've got nothing to hide' and other misunderstandings of privacy", *St. Diego Law Review*, 44, pp. 745–772, 2008.

[41] D. J. Solove. *Understanding privacy*. Harvard University Press, Cambridge, Mass., 2008.

[42] W. Sonnenreich, J. Albanese, and B. Stout. "Return on security investment (ROSI) - A practical quantitative model", *Journal of Research and Practice in Information Technology*, 38(1), pp. 45–56, 2006.

[43] G. J. Stigler. "An introduction to privacy in economics and politics", *Journal of Legal Studies*, 9, p. 623–644, 1980.

[44] L. Sweeney. "k-anonymity: A model for protecting privacy", *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10(5), pp. 557–570, 2002.

[45] P. P. Swire. “Efficient confidentiality for privacy, security, and confidential business information”, *Brookings-Wharton Papers on Financial Services*, 2003, pp. 273–310, 2003.

[46] T. Tsiakis and G. Stephanides. “The economic approach of information security”, *Computers and Security*, 24(2), pp. 105–108, 2005.

[47] B. van den Berg. “The uncanny valley everywhere: On privacy perceptions and expectation management”, In *Privacy and Identity Management for Life: 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2010, Revised Selected Papers*, S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes and G. Zhang (eds.), Springer, Heidelberg, Berlin, 2011.

[48] R. Volkman. “Privacy as life, liberty, property”, *Ethics and Information Technology*, 5(4), pp. 199–210, 2003.

[49] S. D. Warren,L. D. Brandeis. “The right to privacy”, *Harvard Law Review*, 4(5), pp. 193–220, 1890.

[50] A. F. Westin. *Privacy and freedom*. Atheneum, New York, 1967.

[51] J. Q. Whitman. “The two western cultures of privacy: Dignity versus liberty”, *Yale Law Journal*, 113, pp. 1151–1221, 2003/04.

Author Biographies

Philip Schütz studied political science, English literature and law at the University of Heidelberg, Germany and at the Institut d’Études Politiques Lille, France. After graduating in 2009 with an M.A. degree, he has been working as a junior researcher for the Fraunhofer Institute for Systems and Innovation Research ISI in Karlsruhe. He is engaged in the EU-projects PRESCIENT and SAPIENT and a doctoral candidate at the University of Göttingen.

Michael Friedewald is senior researcher and head of the ICT research unit at Fraunhofer ISI. His current research focus on privacy and trust issues of emerging sciences and technologies. He is the co-ordinator of the EU projects PRESCIENT and SAPIENT and a member of the Internet of Things expert group of the European Commission. Mr Friedewald holds diploma degrees in electrical engineering and economics and a PhD in Science and Technology Studies from RWTH Aachen University, Germany.