A Welfare Analysis of Secondary Use
of Personal Data[*]

Nicola Jentzsch[†]

DIW Berlin

Preliminary Version - Do not quote.

May, 2010

Abstract

Personal information on individuals is increasingly shared between companies that do not belong to the same industry. Such exchange may occur for purposes of risk assessment, identity verification or cross-marketing. Secondary purposes of data use are regulated under the European Data Protection Directive, but implementation in Europe differs from one country to another. At the EU level, there is currently a controversial discussion whether such sharing is benefitial from a consumer's perspective. In this paper, I discuss the impact of data protection regimes on firms' capabilities of information sharing and price discrimination. Data protection regimes induce rent-shifting among firms and consumers and it can be shown that given data protection rules not all consumers benefit equally from compensation for information disclosure.

1 Introduction

Information technologies allow firms to increasingly collect, process and exchange detailed personal profiles on individuals. For instance, financial service providers share credit histories of their clients through credit bureaus, but in some countries also with firms outside of their industry such as insurance companies, mail order industry and telecom providers. Travel information on individuals is shared among airlines and additionally with transportation firms, hotel chains and travel agents. Secondary use of personal data occurs, if information collected for one purpose is subsequently re-used in a secondary transaction for another, sometimes unrelated purpose. Even government authorities engage in secondary transactions. For instance, in Great Britain the voter registration list is accessed by credit bureaus for address verification and in Germany civil registers (*Melderegister*) can be accessed by the GEZ, an organization collecting fees for public broadcasting. Compatibility and incompatibility of secondary uses of personal information are high on the European Union's agenda and considered in the Article 29 Data Protection Working Party. Yet, welfare effects of such uses are controversial and often remain obscure for consumers and regulators alike.

In this article, I analyze different regulatory approaches in the European Member States with regard to secondary use of personal information, that is the sharing of information among non-rivals. In the European Union, data protection laws frame privacy policies and practices of companies and limit the range of feasible contractual agreements. They also frame consumer choices about disclosure of their personal information. At the EU level, the Data Protection Directive of 1995 (Directive 95/46/EC) holds in Art. 6,1(b) that personal data must be collected for "*specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.*" The interpretation of this principle and tests for compatibility differ remarkably across the EU Member States. This article concentrates on the sharing of credit information for secondary purposes which are not related to credit. This plays a role when analyzing the welfare effects of sharing of risk information among non-rivals.

This article is an applied analysis, which does intend present theoretical innovations, but rather concentrates on analyzing data protection rules. I am primarily interested in how such rules induce rent-shifting among market participants and affect welfare of consumers. Further, I

concentrate on the sharing of credit risk information as well as valuation information, both are of vertical type. A simple model of monopolistic sellers is used, who sequentially interact with four different types of consumers and who may or may not share consumer information, depending on the privacy regime. Three privacy regimes are analyzed: anonymity, disclosure and interim regimes (full and partial consent). Data protection regulations impact on information sharing as well as price discrimination capabilities of firms. In the context of this model, such regulations induce rent-shifting among firms and consumers, where consumers obtain higher rents, when they need to be compensated for information disclosure. However, it can also be shown that not all consumer types benefit equally from compensation - this is the case when the firm chooses to set a screening price, which allows identification of all consumers, but compensation of only a share of them.

In the legal discussion in this paper, I present examples of secondary information use based upon a small-scale survey of European Data Protection Supervisors. Three countries are used as examples for interpretation of compatibility and incompatibility of data use. Evaluating whether the use of data was compatible or not with its primary purpose is defining the boundaries between illegal information leakage and legal information sharing. The analysis shows the different interpretations of the secondary use principle leading to quite different welfare effects, seen from a theoretical perspective. Although there is much open for future research, recent theoretical developments may provide indications and guideposts for policy-making.

The subject matter of secondary use ranks high on the European policymakers' agenda. At the European Commission, there is also currently a discussion of a major revision of the European data protection framework underway. For this overhaul, however, privacy economics and consumer choices ought to be far better understood as they currently are. In future, the model presented here will be expanded to account for imperfect commitment and strategic bundling of contract clauses by firms to induce information sharing.

The paper is organized as follows: chapter 2 discusses the economics of privacy. Chapter 3 provides a review of the theoretical literature on information sharing among non-rivals. Chapter 4 presents the model, chapter 5 the legal background and chapter 6 concludes.

2 Insights into Privacy

Today there is a thriving literature on the economics of privacy, its welfare effects and information sharing among institutions. Of increasing interest recently is behavior-based pricing based upon the purchase history of the consumer. There is now an extensive literature devoted to such pricing and its effects under competitive conditions (Fudenberg and Villas-Boas 2005) or in the monopoly case (Acquisti and Varian 2005). In banking and finance, there is also an increasing number of articles on the sharing of borrower information - these models capture information exchange among competitors and explain how information sharing arises endogenously (Pagano and Jappelli 1993), how reputation effects lengthen with credit history (Vercammen 1995), and how information sharing acts as a borrower discipline device (Padilla and Pagano 2000). Diverging from these approaches, I concentrate on sharing of risk data among non-rivals. Works in this area of non-rival information sharing are few, maybe because competitive implications fall away, when data is shared across different industries. However, there are a number of interesting questions with regard to the social welfare effects that arise from such data sharing. Moreover, there is a lack of understanding the institutions that regulate information sharing and how they frame decisions of firms and their price discrimination capabilities and feasible actions. This is why more needs to be contributed in the area of law and economics.

2.1 Types of Personal Information

In the following, I discuss identification, personal information of horizontal and vertical type and their economic effects. In the model, only the sharing of vertical information is discussed.

2.1.1 Identification Information

It is the act of identification, which creates personal information. For identification, identification parameters (identifiers) are needed. These must be unique, universal, permanent and if possible technically measureable. Identifiers are name, address, age, ID number and increasingly biometric features such as fingerprints or facial metrics. Individuals, however, can also be identified through patterns of interaction in telecommunication or social networks.[1] Once

---

[1]In fact, identification is increasingly possible *without* personal identifiers as individuals leave all kinds of personal traces in electronic transactions that make them identifiable.

an individual is identified, information about that individual can be personalized and merged from different sources. Identifiers are codified in legal documents such as ID cards, passports or driver's licenses. The concept of "identity" associates the set of personal identifiers with preferences revealed in economic transactions (e.g. 'location' in models of spatial differentiation). The legal definition of *personal information* encompasses the aforementioned identifiers, and states that personal information is

> "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;" (Article 2(a), EU DPD).

Personal information receives special protection compared to non-personal information, because of the potentially adverse welfare effects that may arise from it. *Non-personal information*, on the other hand, is not directly attributable to one person, but instead identifies an object. For instance, IP numbers identify computers and serial numbers SIM cards. Both do not (perfectly) identify the owner of the computer or phone. The boundaries, however, are often blurred. In the Google Inc./DoubleClick merger, the European Commission (2008) did not treat IP numbers as personal information, but acknowledged that a "'user' in this context means a specific browser on a specific computer. Generally this is a very good proxy for a specific person."

2.1.2 Horizontal and Vertical Personal Information

Personal information can be of horizontal or vertical nature - a difference that is of profound importance in economic modeling. As explained by Stole (1995: 530): "horizontal preferences are naturally incongruous across firms – a strong preference for one firm implies a weaker preference for the others. Vertical preferences, in contrast, are harmonious across firms – a customer with a high marginal valuation of quality for one firm will have similar preferences for other firms as well; all firms prefer these customers." Incentives to share information among competitors and non-competitors change with the type of information shared. *Vertical information* invokes best-response symmetry among competing firms, whereas *horizontal information* invokes best-response asymmetry. In the symmetric case, firms are aligned in their responses, once new

information about consumers arrives, both react similarly and there is an incentive to collect and exchange information. For instance, if high credit risk associated with a consumer is revealed, both firms would like to charge a risk premium and both benefit from exchanging such information. In credit reporting, this holds for positive and negative information. In the asymmetric case, firms do not react the same way once new information arrives, while one competitor sets a high price for a specific group of consumers, the other will set a low price for them.

The exact nature of information is often a question of empirical evidence, relating to whether and how the demand for the goods of both firms are correlated. The same holds for risk associated with transacting with the consumer. For example, if credit risk is highly correlated with insurance risk,[2] firms prefer lower over higher risks to whom a risk premium is charged, which essentially denotes vertical information. In such a case, cross-industry third-party sharing may imply beneficial secondary re-use of personal data.

In other instances, a high valuation of one good (e.g. Mercedes) may almost automatically imply a low valuation of another (e.g. BMW). One and the same information, however, can exhibit best-response symmetry and asymmetry depending on what other information a firm holds (this portfolio effect is discussed in Jentzsch, Sapi and Suleymanova 2010). When information is shared among non-rivals, no competitive effects arise. The incentive to sell information to other companies, however, is tamed by data protection rules and possible liability if data is shared for incompatible purposes. In general, cross-industry information sharing can be beneficial for firms, but welfare effects might be ambivalent for consumers, something discussed in greater detail in the following sections.

3 Information Sharing among Non-Rivals

In general, two types of information transactions ought to be differentiated: *information sharing* and *leakage*. Whereas in information sharing is legal and legitimate, information leakage (as used in this article) is illegal and describes cases, where information is accessed in an illegal way. In the context of the legal analysis in this paper, sharing would be associated with compatible purposes of information use and leakage with incompatible purposes of information use.

---

[2]For a discussion, see O'Neill (2007).

In Ben-Shoham (2005), for example, it applies to cases, where the firm collecting the information cannot commit to keeping it private. The main interest in this paper is on information leakage. There is only a limited number of models of data sharing of among non-rivals.[3] Non-rivalry does not induce competitive effects and depending on the set-up, externalities arising from contractual relationship with the first firm cannot be internalized through transaction with the second. Consider a monopolist, who sequentially trades with a consumer and who can internalize information externalities (such as committing not to use information in his second-period offer). It is the same institution acting in two periods, adjusting contractual variables. Such adjustments cannot be undertaken, however, if two different firms are present and subsequent contracts with the consumer are made by a different firm (Ben-Shoham 2005: 3).

In Taylor (2004), two monopolies sequentially trade with consumers in markets for electronic retailing. Consumers have high and low valuations and their tastes for the products offered by the firms are positively, but imperfectly correlated. Since consumers can be identified, personalized offers can be made. In the first period, firm 1 posts a price and consumers make their purchase decision. The next actions depend on the exogenously given privacy regime. There is (i) a confidential regime (personal information remains in firm 1); (ii) a disclosure regime, where firm 1 offers the in-house list including prices and identities for sale, an offer that firm 2 can either accept or reject; and (iii) in case of rejection, firm 2 sets uniform prices, in case of acceptance, firm 2 can price discriminate. The interesting cases arise with the introduction of naive and sophisticated consumers. The latter anticipate effects of the sale of the list and maximize over several periods. When consumers are naive, the confidential and the disclosure regime produce the same outcomes, which critically depend on the elasticity of demand. If demand is elastic enough, firm 1 declines to sell information and firm 2 posts uniform prices. In the case where demand is inelastic, information sale creates welfare improvement.[4] Results, however, change when consumers are sophisticated. Now the ones with high valuations are at risk of being offered higher prices by firm 2, which can price discriminate based upon the purchase profile. They will strategically reduce demand in period 1 or purchase at the lower price. This is different to the model presented herein, where consumers need to be compensated for disclosure. Again,

---

[3]Non-rivals can be modeled as differentiated oligopolists, which reduces the welfare effects discussed herein, see Taylor (2004).

[4]Note that this result holds for positively correlated tastes.

both privacy regimes produce the same efficient outcomes, but when the in-house list is useless (i.e. not differentiating the consumer types due to their strategic behavior), firm 1 prefers the confidential regime, as demand reduction in turn reduces profits. The other result is reversed - if demand is inelastic the commitment not to sell the list increases welfare.[5] In the model discussed herein, consumers cannot strategically invalidate the list, as in the disclosure regime they are assumed to be naive. Given data protection rules, they demand compensation for disclosure, which in turn gives rise to informational externalities.

In Calzolari and Pavan (2006) two firms, an upstream and a downstream seller, sequentially interact with the consumer, whose tastes for the goods offered are positively correlated. The authors endogenize the disclosure policy of firms. In their model, the upstream firm 1 is Stackelberg leader and the downstream contract with firm 2 can be influenced in two ways: through direct contractual externalities and through indirect informational externalities (disclosing information about customers). The authors discuss how the menu of contract offers must be designed to strategically control for both types of externalities. There are three conditions under which the upstream firm ought to grant full privacy protection for consumer information: (i) if there is no interest by the first seller in the level of downstream trade; (ii) if the valuations of the consumer are positively correlated; and (iii) if preferences are separable. If any of these conditions is violated, the disclosure is strictly optimal, even without side-payments. In the situation, where disclosure reduces the upstream level of trade it renders a positive welfare effect only if it is inefficient to sell upstream to the low type. In all other situations, it yields a Pareto improvement (a similar setup is provided in Ben-Shoham 2005, though with a more general distribution of buyer valuations). In Ben-Shoham (2005) consumers benefit from information leakage, because the price discount in the first market is enjoyed by all inframarginal buyer types. Table (1) summarizes the main results with respect to consumer welfare.

In Akcura and Srinivasan (2005), a monopoly firm shares information about a consumer's decision with a third party, which conducts marketing (implying a cost for the consumer). The authors show that the firm prefers an information/price combination, where it can extract a higher amount of information from the consumer, paying him a proportion of the obtained

---

[5] These results are in line with the monopoly case in Acquisti and Varian (2005), where sophisticated consumers would strategically delay purchase or use an anonymization technology.

Table 1: Welfare Effects of Information Sharing

Authors	Valuations	Consumer Welfare	Commitment
Akcura & Srinivansan (05)	Positive correlations	Increases with cross-selling if privacy insensitive	Commitment, endogenous privacy policy
Calzolari & Pavan (06)	Positive and negative correlations	Ambivalent and depending on beliefs towards consumers	Commitment, endogenous privacy policy optimal
Ben-Shoham (05)	Positive and negative correlation	Consumers are compensated for leakage (they benefit)	No commitment, leakage
Taylor (04)	Positive correlation	Welfare depends on elasticity of demand, welfare reversals with sophisticated consumers	Endogenous and exogenous privacy policies regulations

revenue from information sale. Privacy regulations are in that sense positive as they reinforce commitment to an optimal level of cross-selling by the monopoly. The results herein are in line with this outcome, but it is additionally shown that not all consumer types benefit equally for the externality that disclosure by some types has on others. Further in the model below, different property rights distributions are allowed. Other works not discussed herein due to brevity are Kahn, McAndrews and Roberds (2000), as well as Dodds (2008).

The model presented herein differs from the above set-ups in the following ways. Consumers are described by two parameters (and not only one), which are both vertical in nature and differ in the specification of property rights associated with them. Essentially, the firms react in the same way to both types of information, but consumers have different control rights over them. In addition, consumers are sophisticated and depending on the existing data protection rules, may demand compensation for their information. The compensation in turn depends on whether full or partial consent is needed for information sharing.

4 The Model

In the following, a model of two monopolistic sellers is assumed as in Taylor (2004). Slightly diverging from him, consumers in the setting below are described by two variables (risk and valuation). Data protection rules influence the expectations of individuals about the commitment of firms to specific data uses. The main interest here are welfare implications of data protection rules, which limit the feasible actions concerning data handling practices of firms and consumers alike. Data protection in general influences information sharing and price discrimination capabilities of firms.

4.1 Firms and Consumers

Firms. There are two monopolistic sellers, 1 and 2. This set-up captures (legitimate) secondary uses of personal data. Consumers first purchase at firm 1 and then at firm 2. Exogenous privacy regimes limit the feasible actions of firms and consumers. Depending on the regime, firm 1 may be prohibited from disclosing consumer data to firm 2 or may sell consumer data (the whole set or partially). In some cases, firm 1 has to obtain the consent from the consumer (opt-in). Firm 1 will always sell consumer data, whenever allowed and whenever firm 2 proposes a non-negative payment. Both firms sell one good which cannot be resold. If firms have consumer data, they can set discriminatory prices.

Consumers. There is a continuum of consumers with the total mass of 1. Consumer n is described by a pair of parameters (v_i, r_j), where v_i is the consumer's valuation and r_j is her risk. Consumer valuations $v_i \in \{v_L, v_H\}$ with $0 < v_L < v_H < 1$. Risk is denoted by $r_j \in \{r_L, r_H\}$ with $0 < r_L < r_H < 1$. There are four consumer types, given by the pairs (v_L, r_L), (v_L, r_H), (v_H, r_L) and (v_H, r_H), or LL, LH, HL, and HH. Further, it is assumed that (v_i, r_j) are fixed across periods. Consumer sophistication depends on the regime: consent informes them about information uses and leads to sophisticated consumers.

Table 2: Probabilities Associated with v and r

Risk \ Valuations	v_H	v_L
r_H	$\alpha\beta$	$(1-\alpha)\beta$
r_L	$\alpha(1-\beta)$	$(1-\alpha)(1-\beta)$

10

Additionally, $\alpha = \Pr\{v_i = v_H\}$ and $\beta = \Pr\{r_j = r_H\}$. Table (2) gives the probabilities associated with the different types. To simplify analysis, it is assumed that $p_{LH} = p_{HL}$ and that $\frac{v_H}{v_L} = \frac{1-r_L}{1-r_H}$, resulting in (1)[6]:

$$v_H = v_L \frac{1 - r_L}{1 - r_H} \tag{1}$$

Once consumers purchase at firm 1, information about them is truthfully revealed during the contractual relationship. If firm 1 compiles a list of customers, the ones on the list are perfectly identified. If firm 2 purchases the list, the company can price discriminate based upon consumer types. Note that firm 1 can never price discriminate before it sets prices (only at the end of period 1 it identifies consumer types). In the following, only very basic versions of EU data protection rules are considered. The regimes are derived from the legal analysis of data protection rules with respect to the secondary use of personal information in the EU-27 countries. Table (7) presents the laws and Table (8) the interpretation as well as whether data from different sources can be merged for creditworthiness assessment (in essence, cross-industry data sharing). The countries are grouped into three categories (these will be expanded in future):

(1) Anonymity: No sale of information from one market segment to another is allowed (e.g. Poland);[7]

(2) Disclosure Regime: Sale of data from one firm to another in another market segment is allowed. Such allowance exists, where data transfer is justified with an '*overriding legitimate interest*' of the company collecting the data on the consumer. I assume that this rule - held in Article 7(b) EU-DPD - does not require consent.[8] Country examples are Austria, Spain and United Kingdom;

(3) Interim Regimes: The sale of data is allowed under specific conditions. The most important condition is obtaining consent from the consumer. In the model below, there are two different types of consents: complete consent (v_i, r_j) and 'partial consent' for (v_i) only. Consent

---

[6] In further extensions of the model, these two types are differentiated due to differing property rights specification relating to v_i.

[7] This is grossly simplified, of course. The regime might be better fitting examples of firms in developing countries, which refrain from information sharing due to the lack of legal rules.

[8] Note that this differs from opt-out. In opt-out decisions, the consumer has a choice of opting out of the data transfer. In the disclosure regime as assumed here, the consumer doesn't, she can only reject the whole contract.

may differ in its quality (freely given, informed, etc.), but this is at this stage outside of the present analysis. Country examples for Interim Regimes are Germany and the Czech Republic.

4.2   Timing of the Game

- **Stage 1:** Nature draws types of consumers n, who perfectly observe their own type. Firm 1 posts offers at which consumers may purchase. At the end of stage 1, firm 1 can identify and profile consumers and may sell customer data based upon the existing privacy regimes.

- **Stage 2:** The next actions by market participants depend on the prevailing privacy regime, as discussed above, (1) Anonymity Regime; (2) Disclosure Regime; and (3) Interim Regimes. Two types of consent are envisaged: (i) *full consent* and (ii) *partial consent.*

- **Stage 3:** Depending on the information obtained, firm 2 can post discriminatory prices to different consumer types. Consumers may accept or rejects the offer of firm 2.

4.3   Anonymity Regime

In the Anonymity Regime, the main question is which consumer segments firms will target. In the Anonymity Regime both firms are initially incompletely informed about the consumer and play the same game. There are no informational links between the two market segments. Consumer utility in the case of a uniform price $\bar{p}$ depends on her type and is given by

$$U_i(\bar{p}) = v_i - (1 - r_j)\bar{p}, \tag{2}$$

where $(1 - r_j)$ denotes the risk that the consumer does not pay the price (payment risk). (2) can be solved for the reservation price (3):

$$\bar{p}_{ij} = \frac{v_i}{(1 - r_j)}. \tag{3}$$

Prices for the different types of consumers depend on their valuations and payment risks: $p_{HH} = \frac{v_H}{(1-r_H)} > p_{LH} = \frac{v_L}{(1-r_H)}$ and $p_{LH} = p_{HL} = \frac{v_L}{(1-r_H)} > p_{LL} = \frac{v_L}{(1-r_L)}$. In addition, $LH = HL$. If the firm sets the $LH-$price (or HL), types served are LH, HL and HH.

4.3.1 Profits in the Anonymity Regime

In the following, the profits of the firms in the different price-setting scenarios are compared. We proceed by deriving profits from setting the price either for $HH-, LH-$ or $LL-$types. The profit function of both firms at the uniform price (per consumer) is:

$$\pi_{ij} = \bar{p}_{ij}(1 - r_j) \tag{4}$$

A firm can set the highest price for the $HH-$types. At this price, only $HH-$types will be attracted. The fraction of consumers buying is described by $\alpha\beta$ denoting the probability of meeting a consumer with the feature v_H, who also has r_H and who therefore would buy at this price.[9] Profits obtained from $HH-$types are:

$$
\begin{aligned}
\pi_{HH} &= \frac{v_H}{(1 - r_H)}(1 - r_H)\alpha\beta \tag{5} \\
&= \alpha\beta(v_L \frac{1 - r_L}{1 - r_H}) \tag{6}
\end{aligned}
$$

The profit a firm can make from the LH price-setting is obtained in (7). Setting this price, attracts three groups of consumers, $HH-$, $LH-$ and $HL-$types:

$$\pi_{LH} = \frac{v_L}{1 - r_H}\left[\alpha\beta(1 - r_H) + (1 - \alpha)\beta(1 - r_H) + \alpha(1 - \beta)(1 - r_L)\right] \tag{7}$$

If the firm sets the price at the lowest level possible, $LL-$pricing, it will attract all consumer types. The profit from setting the $LL-$price is given by

$$\pi_{LL} = \frac{v_L}{1 - r_L}\left[\begin{array}{c} \alpha\beta(1 - r_H) + (1 - \alpha)\beta(1 - r_H) + \\ \alpha(1 - \beta)(1 - r_L) + (1 - \alpha)(1 - \beta)(1 - r_L) \end{array}\right] \tag{8}$$

Simplification yields

$$\pi_{LL} = \frac{v_L}{1 - r_L}(\beta r_L - \beta r_H - r_L + 1) \tag{9}$$

---

[9]It may be assumed that the frequency of occurrence of the combination of parameters is subject to some empirical distribution in the general population.

Comparison of Profits - In the next step, the firm needs to compare π_{HH}, π_{LH} and π_{LL} for making a choice on pricing. First $\pi_{LH} \lessgtr \pi_{HH}$ are compared. The profit from $HH-$price setting was obtained in (5), using the assumption (1), v_H can be eliminated:

$$\pi_{LH} = v_L\beta + \frac{v_L}{1-r_H}\alpha(1-\beta)(1-r_L) \lessgtr (v_L\frac{1-r_L}{1-r_H})\alpha\beta \tag{10}$$

The comparison of $\pi_{LH} \lessgtr \pi_{HH}$ yields

$$\beta + \alpha(1-\beta)\frac{1-r_L}{1-r_H} \lessgtr \alpha\beta\frac{1-r_L}{1-r_H} \tag{11}$$

It depends on the parameter values, which side yields the larger profit (and which price will be set), where β is a function of the parameters α, r_L and r_H. $If \beta \longrightarrow 0$, π_{LH} is greater than π_{HH}. If $\alpha \longrightarrow 0$ the same holds. In the case, where $r_H \longrightarrow 1$, the RHS-term in (11) becomes very large, which reduces the importance of parameters α and β.

Table 3: Parameter Values for LH-HH Comparison

Parameters	Result Comparison π_{LH} and π_{HH}
$\beta \longrightarrow 0$	$\pi_{LH} > \pi_{HH}$
$\alpha \longrightarrow 0$	$\pi_{LH} > \pi_{HH}$
$r_H \longrightarrow 1$	$\pi_{LH} < \pi_{HH}$
$r_L \longrightarrow r_H$	$\pi_{LH} < \pi_{HH}$

In the case of $r_L \longrightarrow r_H$ (otherwise $r_H > r_L$ is violated), it is the other way round and the term in (11) becomes small. The interpretation of the result is as follows: if there is a large share of high risks and the risk associated with these is rather high, it is profitable to set p_{HH}. If $\beta > \frac{1}{2}$, then a high $HH-$price will be set. Consider as threshold $\frac{1}{2}$, then the following rules can be derived: if $\beta > \frac{1}{2}$ then set price p_{HH}, if r_H is high; and if $\beta < \frac{1}{2}$, then set price p_{LH}, if r_H is high. The above discussion can be associated with the reporting of the borrowers across market segments. For example, it can be assumed that in a given population in a country, the minority of borrowers is of high risk and their overall share in the total population is rather low.[10] Next,

---

[10]For a reference to an empirical distribution, see FICO Score website (where 7% of the population scores at 549 and below and 93% scores above). Source: www.myfico.com/crediteducation/creditscores.aspx

the case of comparing price-setting for LH and LL.

$$\pi_{LH} \lesseqgtr \pi_{LL} \tag{12}$$

$$\beta + \alpha(1-\beta)\frac{1-r_L}{1-r_H} \lesseqgtr \frac{1}{1-r_L}(\beta r_L - \beta r_H - r_L + 1) \tag{13}$$

As above, the outcome of the comparison of π_{LH} and π_{LL} depends on the parameter values, which are noted in Table (4). From this table, one can derive the price-setting of the firms in specific combinations of parameter values.

Table 4: Parameter Values for LH, LL Comparison

Parameters	Result Comparison π_{LH} and π_{LL}
$\alpha \longrightarrow 1$	$\pi_{LH} > \pi_{LL}$
$\beta \longrightarrow 1$	$\pi_{LH} > \pi_{LL}$
$\beta \longrightarrow 0$	Result depends on α, if r_L close to r_H, then $\pi_{LH} < \pi_{LL}$
$\alpha \longrightarrow 0$	Result depends on β, if r_L close to r_H, then $\pi_{LH} < \pi_{LL}$
$r_H \longrightarrow 1$	$\pi_{LH} > \pi_{LL}$
$r_L \longrightarrow r_H$	$\pi_{LH} > \pi_{LL}$

For instance, if $\alpha \longrightarrow 1$, a firm would choose to set $LH-$prices and if $\beta \longrightarrow 1$ the same holds. α and β are the frequency of occurrence of specific types. Further research needs to investigate the above based upon empirical distributions of parameters in the general population.

4.3.2 Consumer Welfare in the Anonymity Regime

Consumer surplus (CS) is the difference between the consumer's willingness to pay (here: valuation) and the actual price paid by her. The price cannot exceed the willingness to pay. Therefore, $CS_i = v_i - (1-r_i)p_i$. To obtain consumer surplus, the price needs to be introduced in the utility of the different consumer types. First assume that the company sets the $HH-$prices, were only $HH-$types are attracted and their rent is fully extracted by firm 1. All other types do not buy:

$$CS_{HH} = (v_L\frac{1-r_L}{1-r_H}) - (1-r_H)p_{HH} = 0. \tag{14}$$

If the firm sets the price at p_{LH}, it attracts the three consumer types LH, HL and HH. Consumer surplus is only left for the $HH-$type:

15

$$CS_{LH} = \alpha\beta \left[(v_L \frac{1-r_L}{1-r_H}) - (1-r_H)p_{LH} \right] \tag{15}$$

$$= \frac{\alpha\beta - (-r_H - r_L)v_L}{1 - r_H} \tag{16}$$

$LH-$types as well as $HL-$types do not obtain any rent. If the firm sets the lowest price, LL, the following rents result (positive for HH, LH and HL):

$$CS(p_{LL}) = -\frac{(\beta(-1+r_H) + \alpha(-1+r_L))(r_H - r_L)v_L}{(-1+r_H)(-1+r_L)} \tag{17}$$

At $LL-$prices, $LL-$types obtain no consumer surplus. The comparison of consumer rents is presented in Table (5). In the Anonymity Regime, the largest welfare is obtained by consumers, where p_{LL} is set. All consumers are priced into the market, and three consumer groups obtain rents. The Anonymity Regime serves as benchmark for the other regimes.

Table 5: Comparison of Consumer Welfare in the Anonymity Regime

Price-setting	Which consumers purchase?	Consumer Surplus (CS)		
		HH	LH, HL	LL
p_{HH}	HH	0	Do not buy	Do not buy
p_{LH}, p_{HL}	LH , HL and HH	pos.	0	Do not buy
p_{LL}	LL, LH, HL and HH	pos.	pos.	0

4.4 Disclosure Regime

In the Disclosure Regime, the consumer has no decision power in the information transaction. I assume that consumers are not informed about the information transaction and therefore act naively. In its price-setting decision, firm 1 now includes considerations about the value of the list, which it can produce through screening by price-setting. The value of the list is based on its informational content (discrimination power). Note that there are no differences in the informational value of the list if p_{LH} or p_{LL} are set, as the former price will automatically reveal all $LL-$types (who do not buy). The largest increase in the list's value occurs, when firm 1 shifts its price-setting from p_{HH} to p_{LH}. In setting p_{LH} , the firm produces full identification.

4.4.1   Profits in Disclosure Regime

Firm 1 and firm 2 are now diverging in their price-setting strategies. Firm 1 can never price-discriminate. The more consumers firm 2 can identify, the greater its discriminatory profits, denoted with a *tilde*. $\widetilde{\pi}_{HH,LH}$ denotes profits of firm 2, which can discriminate on $HH-$types, but sets $LH-$prices for the rest of consumers and $\widetilde{\pi}_{HH,LL}$ if $LL-$prices are set.

Price of the list - The value and price of the list is the gain firm 2 obtains by setting discriminatory prices (in comparison to the pricing in the Anonymity Regime). The firm can fully appropriate this gain as consumers do not have to be compensated (this is the main difference to Interim Regimes).[11] The price of the list, p^{list}, can be defined as

$$p_{HH}^{list} = \max\left\{\widetilde{\pi}_{HH,LH}, \widetilde{\pi}_{HH,LL}\right\} - \max\left\{\pi_{HH}, \pi_{LH}, \pi_{LL}\right\}, \tag{18}$$

where the last term on the LHS denotes profits in Anonymity Regime, which depend on parameter combinations. Likewise, the list derived from setting p_{LH}, where FPD stands for *full price discrimination*:

$$p_{LH}^{list} = \widetilde{\pi}^{FPD} - \max\left\{\pi_{HH}, \pi_{LH}, \pi_{LL}\right\} \tag{19}$$

Firm 2 compares the different profits it makes under the various price-setting scenarios. If firm 1 sets $HH-$prices, firm 2 obtains the $HH-$list and will set for the rest of consumers LH:

$$
\begin{align}
\widetilde{\pi}_{HH,LH} &= \pi_{HH} + \left[\alpha(1-\beta) + \beta(1-\alpha)\right]p_{LH} \tag{20} \\
&= \frac{(\alpha(1-\beta) + (1-\alpha)\beta)v_L}{1 - r_H} + \frac{\alpha\beta + (1-r_L)v_L}{1 - r_H} \tag{21}
\end{align}
$$

If firm 1 sets $HH-$prices, firm 2 can as well set $LL-$prices for the other consumers,

$$
\begin{align}
\widetilde{\pi}_{HH,LL} &= \pi_{HH} + (1-\alpha\beta)p_{LL} \tag{22} \\
&= \frac{(1-\alpha\beta)v_L}{1 - r_L} + \frac{\alpha\beta(1-r_L)v_L}{1 - r_H} \tag{23}
\end{align}
$$

---

[11]Here, it would be sufficient to assume that the costs of rejecting information sharing is too high for the consumer in order to use this option.

In the case where firm 1 sets either LH or $LL-$prices, firms 2 can fully discriminate, both cases, $\widetilde{\pi}_{LH,LH}$, and $\widetilde{\pi}_{LL,LL}$ are therefore equivalent, all consumer types obtain personalized prices:

$$\widetilde{\pi}_{LH,LH} = \pi_{LH,LH} + (1-\alpha)(1-\beta)(\frac{v_L}{1-r_L}) \tag{24}$$

$$= \frac{(-1+r_H-\alpha r_H+\alpha r_L)v_L}{-1+r_H} \tag{25}$$

Comparison of Profits - Depending on the price-setting, firm 1 can derive different lists. It will max $\{\pi_{HH}, \pi_{LH}, \pi_{LL}\}$. The company has an incentive to charge p_{LH} as this produces the most valuable list. As soon as firm 2 is able to discriminate (even just on one type), joint profits rise. Firm 1 will set a price for the list, which sets firm 2 indifferent to purchasing or not. The sale of the list leads to pricing in of more consumer types, which is the standard price discrimination result.

4.4.2 Consumer Surplus in Disclosure Regimes

For brevity, consumer rents are presented in Table (6). In the Disclosure Regime, firm 2 can appropriate all consumer surplus by buying the list from firm 1. While firm 1 cannot discriminate, it can sell the list at the end of period 1 and is strictly better off doing so. It has an incentive to set a price, which produces a list with the greatest discrimination power and thus value.

Table 6: Consumer Welfare in the Disclosure Regime

Cases	Firm 1	Firm 2	Consumer Surplus at the Firms
(1)	$p_{HH} + p_{HH}^{list}$	(a) p_{HH} and p_{LH}	At 1: $HH = 0$, no purchase: LH, HL, LL
			At 2: $HH = 0$, $LH, HL = 0$, no purchase: LL
		(b) p_{HH} and p_{LL}	At 1: $HH = 0$, no purchase: LH, HL, LL
			At 2: $HH = 0$, $LH, HL = CS > 0$, $LL = 0$
(2)	$p_{LH} + p_{LH}^{list}$	$p_{HH}, p_{LH}, p_{HL}, p_{LL}$	At 1: $HH = CS > 0$, $LH(HL) = 0$, $LL = 0$
			At 2: All obtain 0
(3)	$p_{LL} + p_{LL}^{list}$	$p_{HH}, p_{LH}, p_{HL}, p_{LL}$	At 1: $HH, LH, HL = CS > 0$, $LL = 0$
			At 2: All obtain 0

Compared to the Anonymity Regime, consumer welfare will always be smaller in Disclosure Regimes - a standard discrimination result (see also Acquisti and Varian 2005, and Taylor 2004). Where welfare is maximized depends on the combinations of parameter values which determine

price-setting. Table (6) reiterates that in all cases, it depends on the first firm's pricing strategy to what extent the second can price discriminate. From a price discrimination perspective, (2) and (3) are equivalent, in both cases, firm 2 can set personalized prices for all consumer types. Such data protection regimes, therefore, lead to a decrease in consumer welfare (and to a re-distribution of rents to the discriminating firm).

4.5 Interim Regimes

4.5.1 Assignment over v_i, r_j

In the context of the above, data protection regimes assign property rights to information. This may occur in the form of opt-in (for a full-scale opt-in versus opt-out analysis, see Boukaert and Degryse 2006). In the case, where there is a full assignment over (v_i, r_j) to consumers, firm 1 needs to obtain consent from the consumer. To obtain such consent, it needs to compensate the consumer (who is sophisticated) for the foreseen price change in period 2. Firm 1 will partially compensate the consumer out of the revenues from the list's sale - this is a shifting of rents induced by data protection laws. However,

- If firm 1 sets $HH-$prices, it must compensate $HH-$types for the sale of the list. $HH-$types might now obtain higher prices compared to the case, where they are pooled with other types;

- If firm 1 sets $LH-$prices, it must compensate $HH-$ and $LH-$types ($HL-$types), but not all others w*ho are automatically identified* (firm 2 knows about consumers, who are not on the list that they must be of $LL-$type).

Data protection regimes lead to a re-distribution of rents among participants in terms of assigning property rights over information. However, under the above assumptions, not all consumer types benefit equally. Extreme risk distributions aside, firm 1 will choose to set p_{LH}, which identifies all consumers. But the firm will need to obtain consent only from the HH, LH as well as $HL-$types as it has collected information on them. Firm 1 *must not obtain consent* and therefore must not compensate $LL-$types (which is contingent on consent). It has only indirectly collected information on these consumers.

This is highly problematic from a data protection perspective, as the firm would not qualify as "data controller" under the law (e.g. the EU-DPD). This result, of course, also depends on the number of consumers. Inferences on other types are more difficult as the number of existing consumer types increases. The theoretical discussion above shows that not all consumer types benefit equally from data protection.

4.5.2 Assignment over v_i

A future extension of the above model are (partial) assignments of property rights. For example, in some European countries, negative information (r_j) does not need consent for sharing with other firms across industry boundaries, whereas consent needs to be obtained for positive information v_i. Firm 1 in this case would have to negotiate with the consumer about disclosure of v_i. Assume that r_j can always be shared, consumers with v_H would need to be compensated for data sharing and such sharing would in turn automatically identify those with v_L. Therefore, in this sub-case of the above, regulations induce partial compensation of the consumer.

All in all, the above shows that data protection regimes impact on the firms' information sharing and price discrimination capabilities and lead to a rent-shifting among participants.[12] It depends on the parameter values, which prices are set by firm 1. In future, empirical distributions of types ought to be used for numerical simulations. However, if we do not assume extreme distributions, the tendency would be to set a price that produces the most valuable list and leads to only limited consumer compensation. Disclosure Regimes locate the property rights at the firms, and therefore lead to greater rent-extraction to the detriment of consumers. Vertical information hereby leads to aligned reactions, where higher risk leads to higher prices at the second firm (and additional firms, if data was shared with others). In negotiation regimes (Interim Regimes), firm 1 has to compensate consumers for information sale and discriminatory prices in the second period.[13] However, such assignment of property rights does not benefit all consumer types equally - due to the existing informational externalities.

---

[12]This may be compared to the analysis of Hermalin and Katz (2006).

[13]This is at this stage artificial. Consumers are very likely to not know what their information is worth, similar is introduced in Dodds (2008).

4.6 Future Extensions

The above model is basic, largely based on Taylor (2004), and needs to be extended in future to better reflect insights from the legal analysis on secondary information use. From a *theoretical perspective*, a model extention could be the relaxation of unit demand for consumers. Further, the use of a value function, instead of a utility function might be interesting (Weber 1994) - that is more behavioral assumptions about consumer behavior (Acquisti and Grossklags 2004, 2005, Margulis 2005). Imperfect property rights specification might be explored in association with uncertainty over data uses (Dodds 2008).

From an *applied point of view*, it would be interesting to join *information sharing* and *leakage* (Ben-Shoham 2005), which captures both compatible and incompatible information use. Expectation of the latter will be an important element in a consumer's decision whether to share information with a firm. In addition, much more needs to be invested in analyzing indirect effects of information disclosure. Data protection might improve firms' commitment as it creates legal liability. Where there is no data protection, a firm might be unable to commit (Armstrong 2006). Imperfect commitment might create leakage: One example of externalities (in another context) is the recent controversy around FaceBook collecting information not only on their users, but also non-users (by copying the electronic address books of FaceBook users).[14]

Another interesting question relates to the effects of combinations of horizontal and vertical information, where consumers must expect different reactions of the firms towards their information or are uncertain about the firm's reaction. Combinations of information might yield synergies, where two items of personal data combined reveal a third type (such as income). The joint effect in this case would be greater than the sum of the information items alone.

A very important matter is the quality of consent consumers give. Essentially, companies have an incentive to strategically reduce the quality of the consent to maintain action options open with respect to the information collected. This may surface as overly euphemistic language in contracts with regard to data transfers, permanent changing of privacy terms or confusion of consumers through very lengthy privacy policies.[15]

---

[14]Moore, T. (2010) Facebook Under Attack in Germany Over Privacy, Time Online, April. 13, 2010. www.time.com/time/world/article/0,8599,1981524,00.html.

[15]The latter is a strategy applied by FaceBook, among many other companies.

To be able to extract a greater share of the rent from data sharing, companies tend to increase the costs of rejecting such sharing by bundling consent clauses for the sharing of different information types together with other contractual clauses. This way the costs of rejecting a 'sharing clause' are increased, because the consumer can only accept or reject the whole contract. This could be simply avoided by introducing ticking boxes in contracts.

There are more open questions. At the moment, we are only at the beginning of better understanding the impact of cross-industry data sharing (in the real-world). The potential reputation effects associated with it can be either positive or negative. In addition, to consumers they are often unclear. Consumers are inter-temporally mobile in types and can often not foresee what impact the sharing information today will have on their welfare tomorrow. One question relates to the optimal adjustment of the disciplinarian effect of credit information sharing, if a potential default can lead to exclusion from multiple industries in future when data is shared across industries. Consumers who will be severely affected by such reputation systems are the financially vulnerable ones, who are prone to income shocks.

A more general question relates to the benchmarks used in such research - total anonymity or total disclosure - both of which are extreme corner solutions of a range of social options for privacy regulation.

5 Regulation of Secondary Use of Personal Data

The privacy regimes chosen above are gross simplifications as the legal discussion below shows. Secondary information use is a highly controversial subject, which relates to whether personal data are processed in a manner compatible with the purpose for which they were originally collected (inducing information sharing, as discussed above). If data were not processed in a compatible manner, leakage would result. In Art. 6, 1(b) ('Principles relating to data quality') of the EU-DPD it is stated that Member States shall provide that:

> "[personal data must be] collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;"

The acts in the individual Member States implementing this principle are listed in Table 2. The subject of "incompatibility of data processing" ranks high on the Article 29 Data Protection Working Party as there are considerable differences in how Member States interpret this principle. The implementation of the Directive differs in the EU Member States and discretionary decisions by the Data Protection Authorities have further fragmented the regulatory landscape.

5.1 European Approaches

Evaluating whether the use of data was compatible or not with its primary purpose is defining the boundaries between information leakage and information sharing. In Article 29 Data Protection Working Party (2003: 7), it is explained that some Member States include the criterion of reasonable expectations of individuals to assess compatibility (Belgium, Ireland), in other states a 'balance of interest' test is used (Germany), sometimes stressing all circumstances surrounding the processing (Netherlands). Yet, in other Member States, a 'fairness test' will be sought (Greece). These differences are attributed to the vagueness of the principle (Korff 2002: 63). Table (8) shows that in some countries, the over-riding legitimate interest assumes that data sharing is permitted (Austria, Spain and United Kindom). As stated above, I classified these as 'no consent needed'.[16] In other countries, explicit consent is needed for data processing. There is a great variety observable here. For example, in Denmark consent is obtained for negative credit information sharing and only this information is shared. In Poland and Germany, consent is needed for positive information, but not negative information, which can be shared among banks (essentially rivals). Other (positive) information in Poland is shared among other institutions outside of banking and not pooled with bank data. In Finland, consent is as well needed and only negative information can be merged across sectors. This shows that the above analysis ought to be expanded to also model such regimes. Therefore, the data uses (described here as 'merging'), which are considered as compatible or not differ. The legal tests of compatibility can take quite different forms. Three country cases are used as examples to illustrate this problem. As outlined above, once data uses are ruled to be 'incompatible', information leakage would occur.

---

[16] This might be an over-simplification, as data controllers might still obtain consent, but is still quite different from more stringent regimes.

5.2 Three Country Examples

As illustration of the differences that exist in the interpretation of the secondary use principle, I use three examples: Germany, Netherlands and Ireland.

5.2.1 Germany: Balance of Interest Test

In Germany, authorities apply 'balance of interest' tests (*Rechtsgüterabwägung*) to determine the permissibility of secondary processing of personal data for purposes diverging from the original purpose (*Zweckbindung*).[17] For this determination, the data controller's legitimate interest is balanced with possible countervailing interests of the data subject. These rules were originally developed for the public sector and are now applied to the private sector (Korff 2002: 65). For instance, the State Data Protection Officer of Bremen balances the interests of a lessor versus those of a potential tenant for judging the legitimacy of access to data at a credit reporting agency. The secondary use of information here is the use of the tenant's credit history for rental purposes, which diverges from credit-granting purposes in the primary transaction. Whereas the lessor has a legitimate interest to reduce the risk associated with leasing the apartment to a potential defaulter, the lessee's interest is to have an apartment, which is of existential importance as core of private life.

After balancing both parties' interests, the authority states that the creditworthiness test conducted by the landlord must be geared to the specific lease agreement. The lessor might access the database of a credit reporting agency only insofar as the data concerns legal claims derived from former lease relationships of the lessee.[18] To be able to judge the legitimacy of the secondary uses of their personal information, consumers in Germany must conduct a sophisticated legal balancing their own interests versus those of the other party. The question here is whether the request (of the lessor, for instance) is in excess of what the lessor is supposed to know about the potential lessee. Table (8) shows that in Germany, the merging of different data categories is considered to be allowed, but is subject to dispute.

---

[17] The Article 29 Data Protection Working Party holds that the Directive does not prohibit re-use for different, but for incompatible purposes (Opinion 7/2003, p. 6).

[18] The Düsseldorfer Kreis (an informal association of supervisory authorities in charge for data protection) noted that creditworthiness assessments by lessors are only possible under specific circumstances (Beschluss des Düsseldorfer Kreises vom 22. Oktober 2009).

5.2.2 Ireland: Reasonable Expectations Test

In Ireland, the Irish Data Protection Commissioner has interpreted the principle of incompatibility of data processing in a narrower way and bases decisions on the 'test of reasonable expectations.' The wording of the clause on use and further processing of personal information in the law (section 2(1)(c)(ii) of the Data Protection Act) is very similar to the EU-DPD.[19] The key aspect are the expectations of those who supply the data: use and disclosure is compatible, if it is done in a way data subjects would expect it to occur. There are activities, which do not fall under this rule, such as out-sourcing of data protection activities, and other situations stated in section 8 of the Data Protection Act. This 'reasonable expectations' approach is also taken into consideration by the Article 29 Data Protection Working Party.

One legal case, where this principle came to test in Ireland, was a complaint filed by an individual, because an insurance company used personal information for the cross-marketing of a credit card issued by another financial institution.[20] This other institution in turn contacted the potential credit card customer to inquire about the size of the credit line sought. The Irish Commissioner concluded that the insurance company kept personal data for the purpose of administering the insurance policy and for related secondary purposes. However, cross-marketing based upon the customer database constituted a different and unrelated purpose (that is direct marketing of a third-party product). Further, the company could not produce evidence that the unrelated purpose was supported by the necessary consent. Thus, the Commissioner determined that the insurer was in contravention of section 2(1)(c)(ii) of the Act. Note that this approach is combined with the prohibition of merging data from different sources for creditworthiness assessment (see Table 2).[21]

---

[19] This refers to the consolidated informal version of Data Protection Acts 1988 and 2003, available online form the Data Protection Commissioner in Ireland.

[20] CASE STUDY 1/01 Bank and insurance company –cross-marketing of a third-party product –incompatible use and disclosure –fair obtaining and processing –small print and transparency.

[21] Only recently, the Law Reform Commission in Ireland has made suggestions to reform the system of credit reporting.

5.2.3 Netherlands: Weighting Factors Test

The Consumer Credit Act (Wet consumentenkrediet, Wck) in the Netherlands holds that all financial institutions engaged in extending loans to natural persons falling within the scope of the Wck should join a 'system of credit registrations' (Wck, sect. 14(2)).[22] The relevant articles are 6-15 of the Dutch Data Protection Act (Wet bescherming persoonsgegevens, Wbp). In answering the question whether a specific use of data is compatible with its original purpose, several factors play a role. They are stated in a non-exclusive way in section 9, paragraph 2 of the Wbp and are further explained in greater detail in the Explanatory Memorandum to the Act. Cross-sector exchange is anchored in article 8f and implemented by providers in their general conditions to the contract. The Wbp evokes what could be called 'weighting factors test', which appears to be the most complicated of the three discussed herein. For the determination of compatibility of secondary purposes, a number of factors have to be taken into account.

According to the Guidelines for Professional Data Processors, these factors are: (i) the relationship between original purpose and the purposes of further processing; (ii) nature of the data; (iii) consequences of the secondary processing for the data subject; and (iv) way of acquiring and appropriate safeguards. The sensitivity of information can as well play a role, the more sensitive the data, the less it may be assumed a priori that its secondary use is compatible if different from the primary use. When answering the question of compatibility, all factors have to be considered. The Wbp also lists a number of cases where incompatible processing is possible, for instance in the interest of state security or for prevention and detection of criminal offences.[23] In the Code of Conduct for the Processing of Personal Data by Financial Institutions, it is additionally explained that none of the factors in itself is of crucial importance, rather, they have to be assessed and weighted in their specific context. This means that the factors' weights might change from one circumstance to another. In the Netherlands, the merging of data is allowed for credit assessment purposes (see Table 2). There are two court decisions, which contain legal considerations about the proportionality of cross-sector exchange and its impact

---

[22] The Bureau Krediet Registratie, BKR operates such a credit registration system. The nature of the recorded data, the conditions for recording, use and provision and the rules for removing the data are laid down in the BKR rules and regulations. There is also a BKR code of conduct.

[23] See also Dutch Data Protection Authority (2001), Privacy Audit Framework under the new Dutch Data Protection Act (Wbp), Version of April 2001, downloadable from the authority's website.

on individual consumers.[24] In a related case reported in the Netherlands, a former managing director of a company made a complaint to the Dutch Data Protection Authority (DPA) after a reporting agency linked his name to a bankruptcy of the company, in which he was not involved anymore by the time the bankruptcy occurred.[25] There were two problems: the erroneous report and the score calculated from the data, which was required for a mobile phone subscription for which the person had applied (thus, cross-industry sharing).

If information sharing is allowed for credit purposes, the definition of the term 'credit' is of importance. In several EU Member States it is controversially discussed, whether short-term payment deferrals ought to be considered as being 'credit.' For example, since January 2009, all short-term energy and rental debts are registered in the National Debt Information System (*Landelijk Informatiesysteem Schulden, LIS*), organized by the credit bureau BKR. The information will be primarily provided by housing corporations and energy providers. The design of this system was rejected twice in the past by the DPA, it claimed that data processing had been insufficiently demarcated and that the group of people with access to the system would have been too large. The DPA also advised in February 2009 that the side effects of LIS would be disproportional for the individuals listed in the system, and whose record implies a negative financial situation.

---

[24]These decisions are in Dutch and are available from the author.

[25]Wishaw M.S., Mr. R.W.A., De gewaardeerde klant. Privacyregels voor credit scoring [*The valued client -credit scoring and privacy*] Dutch DPA, September 2000. Background Studies & Investigations 18.

6 Conclusions

Personal information is increasingly shared among firms for purposes of cross-marketing or risk assessment. Such sharing might sometimes occur among rivals and sometimes among non-rivals, giving rise to welfare effects. What is considered as compatible or incompatible purpose for data use and sharing differs across the European countries. This paper uses economic theory to model different privacy regimes related to the sharing of risk information among non-rivals. I concentrate on credit and valuation data both being vertical information, which induces similar reactions across firms.

The three privacy regimes (Anonymity, Disclosure and Interim Regimes) analyzed herein are a gross simplification of regulations that exist in the EU Member States - but the proposed model can be used in future to expand the analysis. Through modeling is can be shown how data protection regulations shift property rights to information and induce compensation in cases, where firms need to obtain consent from consumers to be able to share information with other companies. In the Anonymity Regime, information transactions between firms are not allowed and welfare depends on parameter values, which determine price-setting behavior of firms. In the Disclosure Regime, the price setting of companies is influenced by the value of the list they can produce though screening. Extreme risk distributions aside, the screening firm will set a price which allows identification of all consumers. In addition, it will sell the list and the firms will appropriate all consumer surplus.

In the Interim Regimes - a part which needs to be better developed in future - consumers are compensated for information disclosure. The firm has an incentive to set a price, which identifies all consumers, but then compensate only a share of them. There is one consumer group, which is 'automatically' identified and which will not be compensated. From a data protection point of view, this is problematic insofar as the company only indirectly collects information on these types. Negotiations over information disclosure of positive (valuation) or negative (risk) information will lead to partial compensation of consumers. Also here disclosure might indirectly qualify other consumer types.

Future research ought to be devoted to a better understanding of information sharing versus leakage and privacy choices made by consumers. Incompatible data uses lead to leakage, whereas compatible uses lead to sharing. What is regarded as compatible and incompatible, however,

differs a lot across European countries. I presented a table with interpretations of the rules as they currently exist in a selection of European countries and discussed to what extent merging of data from different industries is allowed or not. Three countries were used as examples to show how different the interpretations are with respect to compatible and incompatible uses - something that needs to be clarified at the European level in future.

There is no simple answer to the question, which data protection regime provides the highest welfare from a theoretical point of view as this depends on a number of conditions. However, there are indications that pure Disclosure Regimes re-distribute consumer surplus to firms, which can better conduct price discrimination and do not need to compensate all consumer types. Consumer welfare derived from Anonymity Regime depends on the parameter values, here price setting can lead to exclusion of consumers. Surplus in the Interim Regimes, on the other hand, critically depends on negotiations and consent. While some consumer groups might be compensated, others might not obtain compensation. One major question related to Interim Regimes is negotiation power as well as quality of the consent obtained from the consumer. Firms might have a strategic incentive to reduce the quality of the consent to keep their options open for selling the information in the marketplace.

References

[1] Acquisti, A., Grossklags, J., 2004. Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting, in: Camp, L.J., Lewis, S. (Eds.), Economics of Information Security. Kluwer Academic Publishers, Dordrecht and Boston, 165-178.

[2] Acquisti, A., Grossklags, J., 2005. Uncertainty, Ambiguity and Privacy, presented at the 4th WEIS (2005), Boston, MA, June 2-3, 2005.

[3] Acquisti, A., Varian, H., 2005. Conditioning Prices on Purchase History, Marketing Science 24(3), 367-381.

[4] Armstrong, M., 2006. Price Discrimination, Department of Economics, University College London, http://else.econ.ucl.ac.uk/papers/uploaded/222.pdf

[5] Article 29 Data Protection Working Party, Opinion 7/2003, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm

[6] Ben-Shoham, A., 2005. Information in Sequential Trade, Mimeo, Harvard University.

[7] Boukaert, J., Degryse, H., 2006. Opt In Versus Opt Out: A Free-Entry Analysis of Privacy Policies, CESifo Working Paper No. 1831.

[8] Calzolari, G., Pavan, A., 2006. On the Optimality of Privacy in Sequential Contracting, *Journal of Economic Theory* 130 (1), 168-204.

[9] Dodds, S., 2008. Welfare Implications of Confidentiality and Consent in Privacy Regulation, Mimeo, Carleton University.

[10] European Commission, 2008. Regulation (EC) No 139/2004, Merger Procedure, Case No COMP/M.4731- Google/DoubleClick, Brussels.

[11] Fudenberg, D., M. Villas-Boas, 2005. Behavior-Based Price Discrimination and Customer Recognition, Working Paper, http://groups.haas.berkeley.edu/marketing/PAPERS/VILLAS/surveypaper.pdf

[12] Hermalin, B., Katz, M., 2006. Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy, Quantitative Marketing and Economics 4(3): 209-239.

[13] Jentzsch, N., Sapi, G., Suleymanova, I., 2010. Customer Data Acquisition and Sharing among Rivals, Mimeo, DIW Berlin.

[14] Kahn, C., McAndrews, J., Roberds, W., 2000. A Theory of Transactions Privacy, Working Paper 2000-22, Federal Reserve Bank of Atlanta.

[15] Korff, D., 2002. Comparative Summary of National Laws, EC Study on Implementation of Data Protection Directive, Brussels.

[16] Margulis, S.T., 2005. Privacy and Psychology, Mimeo, Grand Valley State University.

[17] O'Neill, I. 2007. Disparate Impact, Federalism and the Use of Credit Scores in Pricing Insurance Products, *Loyola Consumer Law Review* 19 (2), 151-178.

[18] Padilla, A.J., Pagano, M., 2000. Sharing Default Information as a Borrower Discipline Device. *European Economic Review* 44 (10), 1951-1980.

[19] Pagano, M., Jappelli, T., 1993. Information Sharing in Credit Markets, *Journal of Finance* 48 (5), 1693-1718.

[20] Stole, L., 1995, Nonlinear Pricing and Oligopoly, *Journal of Economics and Management Strategy*, 4(4), 529-562.

[21] Taylor, C.R., 2004. Consumer Privacy and the Market for Customer Information, *RAND Journal of Economics* 35 (4), 631-650.

[22] Vercammen, J.A., 1995. Credit Bureau Policy and Sustainable Reputation Effects in Credit Markets, *Economica* 62 (248), 461-478.

[23] Weber, E., 1994. From Subjective Probabilities to Decision Weights: The Effect of Asymmetric Loss Functions on the Evaluation of Uncertain Outcomes and Events, *Psychological Bulletin* 115 (4), 228-242.

Table 7: Relevant Data Protection Legislation in Europe (2009)

Country	Interpretation	Applicable law or regulation (sections)
Question: Is it allowed - in your country - to merge data from different sources (credit data and telecom data, for example) for conducting creditworthiness assessment?		
Austria	Yes	Federal Law on the Protection of Personal Data, 2000
Belgium	No	Law on the Central Individual Credit Register, 2001
Bulgaria	Yes, consent	Law for Protection of Personal Data, ...
Czech Republic	Yes, consent	Czech Data Protection Act No. 101/2000
Cyprus	n/a	Cyprus Data Protection Act
Denmark*	Yes**	Act on Processing of Personal Data, 2000
Estonia	n/a	Estonian Personal Data Protection Act, §11
Finland	Yes	Data Protection Act, Credit Reporting Act (527/2007)
France*	No	Act No. 78-71 amended by Act of 6.8.2004
Germany	Yes	Federal Data Protection Act
Greece*	No	Law 2472/1997
Hungary*	No	Act LXIII of 1992
Ireland	No	Data Protection Act of 2003, Sect. 2(1)(c)(ii)
Italy	No	Code of Practice for Credit Bureaus
Latvia*	Yes	Personal Data Protection Law (23.3.00)
Lithuania*	Yes	Law on Legal Protection of Personal Data of 21.1.03
Luxembourg	n/a	n/a
Malta	Yes, consent	Data Protection Act of 14.12.01
Netherlands	Yes	Data Protection Act of 2000, Sect. 6-15, 9
Poland	Yes, limited	Banking Act of August 29th, 1997
Portugal*	No	Law 67/98 of 26.10.98 (Law for Protection of Personal Data)
Romania	No	Decision no. 105/2007
Slovakia	No	Act No. 428/2002 Coll. on Protection of Personal Data
Slovenia*	No	Personal Data Protection Act of 2004
Spain*	Yes	Ley Organica 15/1999 de 13 de diciembre
Sweden	No	Credit Information Act of 1973
United Kingdom	Yes	Data Protection Act of 1998

Source: EU Data Protection supervisors. Some titles of laws have been shortened, some have been amended since enactment. Only main statutes applicable are given. n/a denotes 'not available'; *Expert Group on Credit Histories and/or the author; **Under certain conditions, it may be allowed to merge data from different markets for the purpose of creditworthiness assessments.

Table 8: Secondary Use of Personal Information in the EU

Country	Consent and Allowance for Data Integration
Austria	Overriding legitimate interest and therefore permissible
	Credit bureaus distribute positive, negative information
Czech Republic	Consent is needed - but data are not pooled cross-market
	Credit bureaus distribute positive, negative information
Bulgaria	Consent is needed
	Credit bureaus distribute positive, negative information
Denmark	Merging of data is allowed under specific circumstances
	Credit bureaus store only negative data, only this type is shared
Germany	Partial consent - but data are not supposed to be pooled cross-market
	For data sharing among banks - consent needed for positive data
	Credit bureaus share positive and negative information
Finland	Consent is needed - there is very broad definition of consumer credit
	Credit bureaus can merge only negative information
Latvia	Consent is needed - data can be merged (if there are legal grounds)
	Positive and negative information is shared (public register)
Lithuania	Consent is needed - third party disclosure for legitimate interests
	Credit bureaus distribute positive and negative data (retailers, utilities)
Malta	Consent is needed - debtor only informed about data transfer
	Contract might specify information processing for similar purposes
Netherlands	Consent is needed - weighting of factors around such processing
	Credit bureaus share positive and negative information (retailers, utilities)
Poland	Partial consent - but data are not supposed to be pooled cross-market
	Repayment data (utilities, etc.) distributed over business bureaus
	For data sharing among banks - consent needed for positive data
Spain	Overriding interest - common filing systems are allowed, all have access
	Credit bureaus distribute positive and negative data (retailers, utilities)
United Kingdom	Overriding interest - data from different sources can be merged
	Credit bureaus share positive and negative data (retailers, utilities)

Source: EU Data Protection Supervisors & Expert Group on Credit Histories. Information on types of data shared and with whom is derived from the World Bank Doing Business database.