The Value of Personal Information
Evidence from Empirical Economic studies

Moritz GODEL, Annabel LITCHFIELD & Iris MANTOVANI
London Economics

Abstract: EC data protection policy is promoted with reference to economic benefits. However, the value of personal information in legitimate business models is rarely discussed. Various economic studies have tried to measure individuals' valuation of different kinds of personal data. We review empirical papers from the last 10 years and find evidence that more disclosure is associated with higher valuations. We find that the current research efforts can be extended to yield insights into the pricing of personal information, taking into account the actual value such information creates in legitimate business applications.

Key words: consumer research, privacy, behaviour, experiments, new economy.

■ The protection of 'personal data' in the European Union

The European Commission (EC) defines 'personal data' as "any information relating to an identified or identifiable natural person [...] who can be identified, directly or indirectly, [...] by reference to an identification number, or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity." [1] In practice, this means anything from a name, a photo, bank details, medical information, an email address, an IP address or a post on a social networking website, as long as it makes the 'data subject' in question traceable.

[1] Directive 95/46/EC, OJ L 281, p. 38, 23.11.1995.

A fundamental right...

The EU Charter of Fundamental Rights establishes that every human being has the right to personal data protection in all aspects of life: at home, at work, whilst shopping or on the internet.

> "Such data must be processed fairly for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law." [2]

As explained in the commentary of the Charter, the aim of this Article is that of protecting personal data against arbitrary interference by institutions and bodies of the Union and of the Member States. [3]

As early as 1981, the Council of Europe at the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data recognised that "information power" [4] brings with it commensurate social responsibility on the part of the data users both in the private and public sectors. Because so many decisions affecting individuals are based on information stored in computerised files (e.g. payroll, medical files, social security records, etc.), it is essential that those responsible for such records ensure that the "undeniable advantages they can obtain from automated data processing do not at the same time lead to a weakening of the position of the persons on whom data are stored." This 'weakening' encompasses everything from reputational damage to outright fraud.

… and a treasure trove for data reapers

On the other hand, in light of the continuing developments in digital technology, the European Commission (EC) is keen on emphasising that there is an economic justification for safeguarding personal information. The argument goes as follows: the rapid pace of technological change has transformed the way in which the mounting volume of personal information is collected, accessed, used and transferred. As new ways of sharing and storing information have been internalised by 250 million European internet

---

2 Charter of Fundamental Rights of the European Union, *OJ C* 364, p. 10, 18.12.2000, Article 8.

3 EU Network of Independent Experts on Fundamental Rights, *Commentary of the Charter of Fundamental Rights of the European Union*, p. 95, June 2006.

4 Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

users, personal data has become a valuable asset to many businesses, which expend significant resources in collecting, aggregating and analysing information on potential customers. In this new digital environment, lack of confidence makes consumers wary of purchasing goods and services online. The EC's Eurobarometer survey on consumer attitudes concerning identity management reveals that 72% of internet users are worried they give away too much personal information; 43% say they have been asked for more personal information than necessary.

> "Given the contribution of the Information and Communication Technology (ICT) sector to overall productivity growth in Europe, trust in these services is vital to stimulate growth in the EU economy and competitiveness in the EU industry." [5]

As a corollary to this rationale, the EU is currently undergoing a comprehensive review of its legal framework on data protection so as to harmonise the rules that corporations must abide by across Member States. Regulatory fragmentation creates heavy administrative burdens, impedes the free flow of personal data and is thus an obstacle to the achievement of the Internal Market and to the advancement of the digital economy. [6]

It appears as though arguments for personal data protection, evolved from a human-rights concern, of protecting citizens against government abuse of power or criminal misuse of information, to an economic rationalisation, based on the trade-off between risk and return. In all cases there is a sense that personal information is valuable insofar as it confers a certain degree of power to those in its possession. In the case of governments it may serve to gain political power, while corporations might use it to gain market power. But what seems to justify more recent government intervention is the notion of market failure. As one of the speakers at the EU Conference on privacy and protection of personal data (19 March 2012) put it, "markets only work when governments provide a framework of trust." [7] If uncertainty about what personal information is used for undermines consumer trust in the market place then governments must intervene to restore this trust. The EC's approach is thus one of reducing the

---

[5] COM (2012) 9 final, p. 5, 25.1.2012.

[6] Speech by Viviane Reding (Vice-President of the European Commission), "Toward a new 'gold standard' in data protection," for the EU Conference: Privacy and Protection of Personal Data, Washington/Brussels, 19.03.2012.

[7] Speech by Daniel Weitzner (US Deputy Chief Technology Officer for Internet Policy), Washington/Brussels, 19.03.2012.

amount of personal information that is exchanged and restricting the ways in which the remainder is used.

What is missing in this logic is an explicit consideration of how valuable this information actually is. Policymakers acknowledge that the digital traces we leave across the web are a "treasure-trove" to marketers, major corporations and other "data reapers" [8], and there is ample evidence that businesses treat personal data as a commercial asset [9], trade it, and use it to produce goods and services [10].

■ A market-based approach to personal data

The function of prices

In a market system prices are set so as to bring supply and demand into balance. The resulting equilibrium prices act as signals between producers and consumers and determine how much is produced and how resources are distributed. Meeting economic demand (preference + willingness to pay) at the market-clearing price creates surplus for both producers and consumers, as long as the market is competitive.

In typical consumer markets, the exchange of goods and services is mediated by money: people pay to receive goods and services and trade takes place if both sides benefit from the exchange. In an online setting, personal information is sometimes traded in this way. For example, members of online research panels receive money for disclosing information relating to their browsing habits and their socio-economic situation.

Typically, however, the disclosure of personal information online is better conceptualised as a payment in kind [11]. Examples are ubiquitous and include a variety of nominally free services such as web-based email, search

[8] See Ed Markey (US Congressman), Washington/Brussels, 19.03.2012.

[9] See World Economic Forum (2011). A survey of businesses conducted by ENISA (2011) found that 47% of service providers by ENISA saw personal data as a commercial asset.

[10] ENISA (2011): 82% of businesses collect personal data from users to be able to perform the services they provide.

[11] For further discussion of the benefits and costs of disclosure see ACQUISTI (2010).

engines, mobile apps, etc. Advertising revenue is often at the heart of these business models: consumers give up personal information either explicitly (e.g., by filling in a form when subscribing to a service) or the information is harvested when they visit certain websites (e.g., search engines). This information is then used by the website/application owners to sell advertising space. Advertisers pay a premium for being able to serve ads to consumers with certain observable characteristics and/or behaviours. Online retailers and providers of online content also use personal information to tailor their offering to individual consumers, thereby increasing sales. Finally, a third type of business model uses personal information to produce new services through the combination (e.g., Google's Street View) and/or statistical analysis (e.g., refined individual credit scores) of personal data, either revealed or observed.

A market for personal data?

Against this background, SHAPIRO & VARIAN (1997) formulated the key economics argument in the debates about online privacy:

> "The right way to think about privacy [...] is that it is an externality problem. I may be adversely affected by the way people use information about me and there may be no way that I can easily convey my preferences to these parties. The solution to this externality problem is to assign property rights in information about individuals to those individuals. They can then contract with other parties [...] about how they might use the information."

There are clearly problems with the practical implementation of this solution, not least owing to the rapid expansion of the volume of personal data available online [12] and the ever increasing sophistication of large-scale algorithmic data analysis. Moreover, more direct interventions, such as fines for harmful disclosure, provide alternative means of forcing firms to internalise the externalities. In addition, as BERESFORD *et al*. (2010) point out, the enforcement of contracts runs into problems because "many contracts involving personal data are incomplete or highly opaque, as they typically lack clear-cut information about secondary uses and sharing of personal information". Moreover, as SHAPIRO & VARIAN (1997, based on LAUDON, 1996) explain, "there is already a large market in personal

[12] The World Economic Forum (2011) reports a 2010 estimate that "by 2020 the global volume of digital data will increase more than 40-fold".

information. But the property rights are held by those who collect and compile information about individuals--not by the individuals themselves. These third parties buy and sell information that can impose costs on those individuals, without the individuals being directly involved in the transactions. This is what generates the externality." Finally, the issue of externalities arising from the disclosure (and non-disclosure) of personal data is more complex than the above quote suggests. Externalities emerge not only because of a lack of property rights over personal data that allows commercial exploitations without compensating individuals, or because of secondary data use that consumers have difficulty controlling. Externalities are also present in cases where any one individual's data is of little commercial value, but value is created by combining the data of many individuals. Often in these cases it is not obvious to individuals that it is the collective disclosure decisions that enable a certain service to be delivered, or the way in which more data results in a better/more relevant service (e.g., the network effect by which the attractiveness of online social networks increases with the number and level of detail of available profiles).

In the light of these difficulties SHAPIRO & VARIAN (1997) envisaged a "drawn-out period of confusion" in the absence of explicit recognition of such contracts under privacy law and regulation and monitoring necessary to enforce them. However, there are signs that the idea of a private market for personal information is regaining support. Business models based on free market exchange of data like Digital Media Auditing (DMA) [13] are emerging in the online advertising space, while from the regulation side approaches aimed at increasing transparency and user awareness regarding the use of personal information online have found widespread acceptance [14].

What price?

One important open question regarding market-based solutions to the issue of privacy is that there is no quantification of the economic value they create. If property rights can be assigned to photos, email addresses, or web

[13] Which uses tracker cookies in conjunction with other revealed personal data from consenting individuals (see PHILLIPS *et al*., 2012).

[14] For example in the context of the implementation of the EC's Cookies Directive, where effective communication of data use issues has been a central theme (for example see the ICC UK's 'Cookie Guide', 2012). However, regarding the effect of increased transparency, note the emerging literature on the 'Paradox of Control', e.g., BRANDIMARTE *et al*. (2010), TUCKER (2010).

searches, how much are consumers willing to sell them for? How much are other interested parties willing to pay for their disclosure? [15]

In this paper, we aim to contribute to the ongoing debate by interrogating the economic literature about insights into what prices are assigned to personal data by consumers in empirical economic studies and the factors that affect them. Survey-based studies and economic experiments, in the laboratory and in the field, are particularly instructive because they can isolate through their design the effects of individual factors (such as prices, specific types of information, trustworthiness of suppliers, etc.), which typically remain hidden in more complex real-world markets, where there are many confounding factors and interactions. In our review of the evidence, we concentrate on the results with respect to observed prices and their determinants. Caveats and gaps in the evidence are discussed.

■ Evidence from the economic literature

Numerous studies over the last 10 years have attempted to add empirical substance to debates about the value of privacy and personal data. Given the opacity that shrouds a lot of the real-world markets in which personal data is exchanged, the literature is centred on survey-based (stated preference) methods and experimental designs. We present here a number of empirical studies that provide insights into valuation of personal data on the supply side, that is, from the perspective of individuals disclosing personal information. The demand side, i.e., the valuation of personal data by data controllers, which would have to be explored in order to gain an understanding of the market value of personal data in different settings, is typically absent from this literature.

An early exploration of the value of personal data was undertaken by HANN *et al*. (2002). Using conjoint analysis, the authors test monetary

[15] We are concentrating here on transactions in which businesses derive a legitimate economic benefit from personal information. Personal information that is disclosed purely out of necessity (e.g., billing addresses) and not processed to create added value, or information that is used for criminal purposes, is excluded in this consideration. It is clear that data minimisation, privacy by design and privacy enhancing technologies (PETs) are preferable approaches in these situations. In addition, consumers might attach a value to privacy/non-disclosure that is not related to the ability of data controllers to exploit personal data commercially. The potential for a market in personal data thus does not negate the role for non-market interventions to comply with user preferences regarding the use of personal data.

valuations associated with different 'concern dimensions' that have been found to be relevant in the disclosure of personal information in digital contexts [16]. They find that their respondents value improper access and secondary data use more highly than possible errors in their personal records. More precisely, the possibility to review such records held by other parties for errors is valued at between \$15.46 (€$_{2002}$16.3) and \$19.32 (€$_{2002}$20.4), restrictions on access at between \$29.18 (€$_{2002}$30.9) and \$36.47 (€$_{2002}$38.6) and restrictions on secondary use of the data at between \$39.83 (€$_{2002}$42.1) and \$49.78 (€$_{2002}$52.6). The last figures could be interpreted as the price ranges for buying information for secondary use. HANN *et al*.'s study is limited by the fact that the information content of the hypothetical transactions is not specified.

An interesting set of data points is provided by ACQUISTI & GROSSKLAGS (2005). They conducted a survey in which individuals were asked for their valuation of a number of personal data items in online transaction scenario involving a generic 'marketing company'. Data items ranged from basic (full name, address and phone number) to intrusive (social security number, health data, email content and 'description of sexual phantasies'). The firm and the way the data might be used is described in stark terms:

> "A marketing company wants to buy your personal information. You do not know and you cannot control how the company will use that information. You know that the company will effectively own that information and that information can be linked to your identity."

Participants are asked in an open-ended question for how much money they would disclose the information. In a second question, the disclosure is linked to a purchase scenario: the question is how large a discount on a \$500 (€$_{2005}$402) purchase would need to be given in order to disclose the information.

Unsurprisingly, the authors find great differences in the valuation of different types of data, with high average valuations for social security numbers, health-related information and content of personal emails being valued most highly. Personal contact information (phone number, home address) is in the middle of the value range and basic identification data (name, email address, job title towards the bottom). The authors do not

[16] The dimensions are: collection, error, secondary use, and improper access. See SMITH *et al*. (1996) and STEWART & SEGARS (2002).

provide average valuations, but overall valuations are very high, with an average of 20% of respondents across all data categories reporting a reservation price >$500 (€$_{2005}$402), even for basic data items like a personal email address.

In the purchase-related scenario, average valuations are lower than in the simple scenario where data items are disclosed for a fixed price, although the difference is less pronounced in the case of less valuable information (job title, interests outside work, full name).

The paper offers strong support for the thesis that valuation is context specific and subject to behavioural biases (anchoring bias in the purchase scenario). However, the open-ended question format used by the authors to elicit consumer preferences is itself known to be prone to biased results (over-valuation), so that the quantitative findings in terms of a price for the supply of data items appear dubious. Interestingly, the methodology section of the paper reveals that the study participants were happy to provide anonymised (non-personal) data (demographic information, attitudes to risk and privacy issues) to the researchers for a compensation of $16 (€$_{2005}$13). This type of compensation for disclosure, ancillary to much of the empirical research in this area, is typically not evaluated.

One of the few papers attempting directly to specify a price point for selling personal information is GROSSKLAGS & ACQUISTI (2007). In an experiment involving students, the authors find that subjects show a clear willingness to trade personal information (including weight and IQ test scores) for small amounts. Specifically, most subjects accepted to sell weight and test score information for €$_{2007}$0.20. Note, however, that again the value of the information is a construct of the research design and not related to a (potentially beneficial) commercial use of the data. Rather than treating it as a reliable point estimate, the authors conclude that €$_{2007}$0.20 "is a price that lies within the set of values at which people are willing to sell, but does not lie within the set of values that people are willing to spend to protect" their personal information.

These results contrast markedly with a study of similar design by HUBERMAN *et al*. (2006). In an experiment using an auction design (reverse second-price auction, where the individual quoting the lowest price for the information is paid the second lowest price), the authors find values of $57.56 (€$_{2006}$45.8) for age and $74.06 (€$_{2006}$59.0) for weight data.

GROSSKLAGS & ACQUISTI (2007) note that difference might be explained by the profile of the subject (students *vs*. older participants in Huberman's experiment) and by a priming effect induced by the experiment design (Huberman's subjects were given an upper limit of $100 (€$_{2007}$80) for their bids).

HUBERMAN *et al*. (2006) can also show that valuation varies across individuals and is related to the information content as well as the attitudes that govern the perception of the information: subjects' valuation of weight data increases with their body mass index (BMI) and their self-perception with regards to weight (feeling over/underweight). This confirms that valuations differ both across and within data categories depending on idiosyncratic perceptions of sensitivity.

The value of data on individuals' location was tested by DANEZIS *et al*. (2005). In a carefully designed auction experiment (second price), subjects were asked to submit bids stating the compensation they would require to give permission to monitor their location (via their mobile phones) for a period of 28 days. The location data would be retained and subjects were told it might be reused in unspecified future research. The results show a mean valuation of £27.4 (€$_{2005}$40.1), rising to £32.8 (€$_{2005}$48.0) if subjects are told that there is commercial interests in the data. It is noteworthy that the distribution of bids shows a wide spread, with 15% of the sample bidding £1 (€$_{2005}$1.5) or less and a maximum bid of £400 (€$_{2005}$585).

In a much larger study with 1,200 participants from five European countries, CVRCEK *et al*. (2006) use a similar auction design to test the value of location privacy for individuals using mobile devices. Participants were exposed to a qualitative change in the use of the data, from academic to commercial, and then a quantitative change from a monitoring duration of one month to 12 months. Participants are found to be more sensitive to the purpose of the data collection than the duration and quantity of the data collected. The authors report median bids of €43 for non-commercial use of data, similar to the results of DANEZIS *et al*. (2005). Without presenting robust evidence, the authors suggest with a reference to a widely reported eavesdropping scandal in Greece that the wider societal climate with regards to privacy may be an important determinant of valuations.

ACQUISTI *et al*. (2009) conducted a number of experiments informed by theories from behavioural economics and decision research. Interpreting their results, the authors stress that individuals' valuation of non-disclosure depends strongly on framing, ordering and endowment effects. In an

experiment where subjects were endowed with a \$10 (€$_{2009}$7.2) gift card, an offer of \$2 (€$_{2009}$1.4) to reveal personal data (the purchases made with the card would be linked to their name) was rejected. However, fewer than 10% of those subjects endowed with a \$12 (€$_{2009}$8.6) card and disclosure as the default gave up \$2 (€$_{2009}$1.4) to protect their data. Moreover, privacy valuations are not uniformly distributed, but U-shaped and clustered around extreme, focal values.

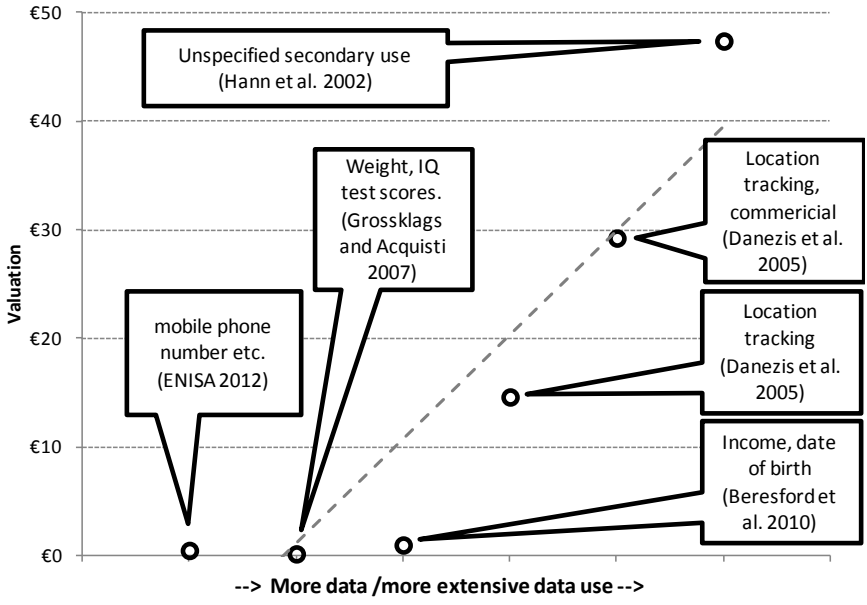
A study by BERESFORD *et al*. (2010) uses a similar setup: participants in a field experiment were given the choice between two online retailers of DVDs, both of them requiring the disclosure of customers' name, postal and email address. In addition one retailer required the disclosure of customer's monthly income and date of birth, while the other required only the year of birth and the subject's favourite colour. The price at the more data-hungry retailer was arbitrarily set €1 lower. Of 42 subjects who made a purchase, 39 chose the cheaper retailer. In a second treatment with prices equal at both retailers, customers were split approximately evenly between the two. While it is possible that subjects protected themselves by providing wrong information, the authors note that the income data provided to the retailers was 'reasonable in magnitude'. The authors highlight that the low valuations contrast with expressed privacy concerns of the subjects (with 95% reporting being 'interested in the protection of their personal information').

In the context of a larger study, ENISA (2012) carried out an experiment both in a controlled setting with university students and then in the field with members of the public recruited through online social networks. Participants were directed to a website that showed the offers of two online sellers of cinema tickets. The researchers varied the amount of data (data items) the participants had to disclose as well as the price of the tickets to test customers' sensitivity towards disclosure requirements when making purchasing decisions.

In the design the price difference between the privacy-friendly and the privacy-invasive firm is set at €0.50. The value was not chosen to reflect the value of the information participants were asked to disclose. Rather, the authors explain, they wanted it to be below the €1 value that was observed not to make a difference to people's disclosure behaviour in a previous experiment (BERESFORD *et al*., 2010, in which some of the same researchers were involved). In terms of data requirements, both firms require a full name, a valid email address and date of birth (to ensure incentive compatibility, the information given by the participants in the field experiment was validated by the researchers). Variation is then introduced in the form of

one of the firms requiring more data (e.g., a mobile phone number) or more extensive use of the data provided (email address is used for advertising). Based on observed differences between purchase decisions and disclosure and data use, the authors find that if it is "obvious that one firm collects more information than the other, all else being equal, a majority of purchases are made at the privacy-friendly firm". However, once higher disclosure requirements are accompanied by a lower price, the market share of 'privacy-invasive' firms increases dramatically from 17% (more disclosure but same price) to 69% (more disclosure but lower price) [17]. The difference is even more pronounced when the price is varied in accordance with the data usage, with the firm that uses the disclosed email addresses to deliver adverts achieving a market share of 87% if it offers a €0.50 discount compared with the privacy-friendly firm. The authors further find that more extensive use of a limited set of personal data items (email address used for targeted marketing) appears to be more easily accepted by users than a requirement to disclose additional data items, even if used less extensively.

Figure 1 - Selected quantitative estimates of the value of personal data items (Currencies converted into € using the average annual exchange rate – Eurostat – in the year of publication.)



[17] Figures refer to the controlled laboratory experiment, in the field experiment the market shares are 10% and 58% respectively.

Interestingly, the authors find no difference in terms of stated privacy concerns between individuals choosing to purchase through one of the websites and those who don't. This result is at odds with the argument (made prominently by the EC) that reported privacy concerns are evidence that the development of e-commerce is being held back by a lack of privacy protection.

The study shows that around 30% of consumers are prepared to pay a premium of at least €0.50 for a service if the provider requires less disclosure. However, another obvious message of the study is that the majority of consumers react to the price signal by disclosing more information to the cheaper provider. While the study doesn't reveal an exact price per data item/extent of usage, the €0.50 for an item of moderately sensitive personal information with limited follow-on usage might be seen as indicative.

■ Discussion

Empirical evidence shows again and again that stated opinions expressing strong preferences for privacy protection provide little guidance as to people's choices when confronted with disclosure decisions involving personal data. This is true even under controlled conditions in experimental markets with a high degree of transparency regarding disclosure requirements and primary and secondary data use. Survey evidence, which is cited prominently by the EC in its discussions of privacy policy, is thus of dubious value, given the well-documented divergence between stated attitudes and preferences and actual behaviour.

At the same time, the literature clearly shows that consumers are willing to trade personal information for money and non-monetary rewards. As HANN *et al*. (2002) note, individuals' concern for privacy is not absolute and individuals are willing to trade off privacy concerns for economic benefits. This opens the possibility for a market in personal data for legitimate commercial use.

The literature on privacy value has gained enormously from the use of experiments, conducted both in the laboratory and in the field. Studies using field experiments, where subjects do not know that they are part of an experiment (or at least are unaware of the purpose of the experiment) such as BERESFORD *et al*. (2010) and ENISA (2012), tend to confirm the

existence of the Privacy Paradox, the divergence between a stated preference for privacy and observed behaviour.

Current EC policy towards personal data protection implicitly acknowledges that personal data is a commodity, tradable and subject to the laws of supply and demand. However, the economic reasoning evident from the EC's official pronouncements is startlingly incomplete. The quantification of privacy concerns, 'with a price tag or otherwise' (PREIBUSCH, 2010), is a continuing problem. While most of the research introduced here does not present the results in these terms, taken together the results can be interpreted as suggesting, in rudimentary form, an upward sloping supply curve for personal data: a price-quantity schedule in which more data (additional data items or more extensive data use) are associated with higher payments (figure 1).

Moreover, increasing transparency and user control over personal information has been found to increase, rather than lower the propensity of consumers to disclose information online (*Paradox of Control*, see e.g. TUCKER, 2010; BRANDIMARTE *et al*., 2010). This suggests that policies aimed at strengthening consent mechanisms can in fact be conducive to the development of personal data markets, rather than antithetical, as is often assumed.

However, the literature also reveals that there are formidable obstacles to the emergence of a functioning market in personal data. Researchers have demonstrated that consumer decision-making about disclosure of personal data is afflicted by "incomplete information, bounded cognitive ability to process the available information, and a host of systematic deviations from theoretically rational decision making, which can be explained through cognitive and behavioural biases" (ACQUISTI, 2010). However, it should be noted that such obstacles are present in many markets, so that their existence alone does not preclude a wider role for markets in this area.

Limitations of the current research

In this regard, it is important to recognise the limitations of the current body of research into the valuation of privacy as a basis for understanding how markets for personal data work. A fundamental problem is the literature's focus on the concept of privacy, rather than data as the focal good, which limits its usefulness for understanding the market-based exchange of personal information.

Either implicitly or explicitly, empirical studies typically adopt the privacy-as-concealment paradigm. By positing a distinctive good 'privacy' [18] as the subject of their analysis, researchers often appear to adopt unnecessarily convoluted arguments. For example rather than giving up a benefit 'privacy' in exchange for compensation (See for example BERESFORD *et al*., 2010), disclosure can be framed as a payment (willingness to pay) in kind in (partial) compensation for goods and services received. The complement is then not 'willingness to protect' (ACQUISTI & GROSSKLAGS, 2005) but the willingness to accept lost surplus (e.g., discounts, free services) in exchange for more privacy. Empirical research from a wide variety of other markets shows that WTA > WTP, suggesting that an opt-in system for disclosure results in significantly less personal data being revealed.

Other studies are forced into surprising statements by the need to argue that the disclosure of personal data is a special case that economists should only approach with caution. ACQUISTI & GROSSKLAGS (2005), for example state that "privacy as a good differs from monetary resources and tangible goods in the sense that its valuation is based on multiple factors"; ENISA (2012) unconvincingly exclude from their analysis any transactions not mediated by money and thus assign a large part of the actual market for personal data to the realm of 'social' rather than 'economic' exchange.

PREIBUSCH (2010) argues that privacy is a non-price attribute. Firms can use privacy as a means of differentiating themselves from their competitors: "when selling at higher prices but with an overall more privacy-friendly design, the latter becomes a quality parameter". Again the conceptualisation is not obvious if disclosure can be seen as an implicit price/medium of exchange. The reluctance to adopt a coherent terminology is surprising given that a lot of the empirical work ends up assigning monetary values to 'privacy', thereby acknowledging that personal information is convertible into money: PREIBUSCH (2010), for example, goes on to state that "a plurality of Web shoppers regularly subdue their privacy concerns to the promise of material gain". We would argue that this is evidence of an implicit understanding that the disclosure of personal information represents an economic exchange. The issue from a privacy protection standpoint is not the so far elusive goal of 'turning privacy into a

[18] As ACQUISTI (2010) explains, "Privacy means too many things, its associated trade-offs are too diverse, and consumers valuations of personal data are too nuanced" to allow an "all-encompassing economic assessment of whether we need more, or less, privacy protection".

competitive advantage', but the much more attainable goal of ensuring the adequate functioning of the existing market for personal data.

An important limitation of the literature when it comes to its relevance to actual information markets is the fact that prices in the reviewed studies are not chosen with reference to the actual value of personal information. Instead, the selection of price points appears arbitrary in most cases. The difference between the results of HUBERMAN *et al*. (2006) and GROSSKLAGS & ACQUISTI (2007), who both assign values to information on their subjects' weight, is very large, but driven entirely by the experimental design. While the papers are instructive about the influence of framing on valuation, the numeric estimates provide no guidance as to the true market value of the information that is exchanged.

Taking into account the actual value of personal data in commercial applications appears as a logical extension of the research agenda and should be of broad commercial and policy interest. A clearer picture of the actual trade-offs involved in consumers' disclosure decision would require not only an understanding of the economics of commercial data use [19], but also of the externalities that have long been recognised as crucial impediments to a market-based privacy regime [20].

A further obstacle to accurate valuations is the lack of incentive compatibility of a substantial part of the empirical literature. When it comes to unwanted disclosure a natural reaction is to increase privacy by providing false information. This kind of information self-defence is little understood, although surveys suggest that it is widespread in practice [21]. While some authors address the problem in their research design [22], it potentially has a severe distorting effect on valuations reported by others.

A final observation is that the empirical research into the value of personal information appears somewhat stagnant. Recent studies like BERESFORD (2010) and ENISA (2012) show no markedly improved

19 For example, as PHILLIPS *et al*. (2012) mention, a lot of uncertainty still exists about the costs and benefits of behavioural online advertising.

20 Including both the negative externalities (secondary data use) explained by VARIAN (1997) and the positive externalities associated with network effects in online social networks, etc.

21 PREIBUSCH (2010) reports survey evidence from Germany that one in three consumers report giving false phone numbers when required to disclose them in web forms.

22 GROSSKLAGS & ACQUISTI (2007), HUBERMAN *et al*. (2006) and ENISA (2012) all take steps to verify information provided by the subjects in their experiments.

understanding of the issue than earlier studies such as HANN *et al*. (2002). While researchers have been able to implement increasingly realistic experiments, a more realistic valuation of personal data and how the surplus is shared between producers and consumers has not emerged.

■ Conclusions

The indications are that the market for personal information continues to be dysfunctional in many respects (i.e., the situation described by LAUDON (1996) remains largely unchanged). Media coverage of data protection issues often leads to 'vague fears' on the part of consumers (PREIBUSCH, 2010) and there is active obfuscation by businesses when it comes to privacy practices (BONNEAU & PREIBUSCH, 2009). Explicit payment for personal data remains the exception and implicit compensation is often opaque, leaving consumers vulnerable to exploitation and undermining trust between data users and individuals.

All this points to the continuing relevance of this strand of research, but with great potential for a research agenda aimed at developing a better understanding of the supply function in information markets. What information consumers are willing to provide, for which uses, and at which price will form a crucial part of future research in this area.

A clearer understanding of the monetary value of personal data is desirable, not least with regards to the EC's policy agenda: consumers who understand the trade-off of costs and benefits are less likely to refrain from taking part in online activities out of a vague sense of risk and fear of exploitation. Transparent pricing is further desirable, because it helps to bring about an equilibrium in data usage that satisfies consumers desire to keep information hidden as well as the data requirements of businesses that use personal information for value creation.

Economic experiments have a role to play in price discovery. The current literature has a marked weakness in this regard as valuations are not connected to actual commercial value (and externalities from disclosure, as well as the cost of non-disclosure, are ignored).

Disclosure of personal data can be part of a voluntary, mutually beneficial economic exchange. Businesses for whom such exchange is an integral part of their business model would do well to promote awareness of the

economics of information disclosure to create a clear distinction between welfare-enhancing data use and the abuse of personal data. Explicit pricing of personal information is one way to achieve this. At the moment, this is a blind spot in EC privacy policy.

References

Journal articles, research reports and working papers

ACQUISTI, A. (2010): "The Economics of Personal Data and the Economics of Privacy", Background Paper #3, Joint WPISP-WPIE Roundtable, *The Economics of Personal Data and Privacy: 30 years after the OECD Privacy Guidelines*.

ACQUISTI, A., JOHN, L. & LOEWENSTEIN, G. (2009): "What is privacy worth?" Twenty First Workshop on Information Systems and Economics (WISE), December 14-15, 2009.

ACQUISTI, A. & GROSSKLAGS, J. (2005): "Privacy and rationality in individual decision making", *IEEE Security & Privacy*, January/February 2005, pp. 24-30.

BERESFORD, A. R., KÜBLER, D. & PREIBUSCH, S. (2010): "Unwillingness to pay for privacy: a field experiment", IZA DP, 5017.
http://bit.ly/aiRdHI (accessed 10 June 2012).

BONNEAU, J. & PREIBUSCH, S. (2009): "The Privacy Jungle: On the Market for Data Protection in Social Networks",The Eighth Workshop on the Economics of Information Security (WEIS 2009). http://bit.ly/dAV4B (accessed 12 June 2012).

BRANDIMARTE, L., ACQUISTI, A. & LOEWENSTEIN, G. (2010): "Misplaced confidences: privacy and the control paradox", Ninth Annual Workshop on the Economics of Information Security (WEIS, 2010). http://bit.ly/O8OAaP (accessed 17 September 2012).

CVRCEK, D., KUMPOST, M., MATYAS, V. & DANEZIS, G. (2006): "A study on the value of location privacy", *WPES'06*, October 30 2006, Alexandria, Virginia, USA.

DANEZIS, G., LEWIS, S. & ANDERSON, R. (2005): "How much is location privacy worth?" http://infosecon.net/workshop/pdf/location-privacy.pdf (accessed 05 June 2012).

ENISA:

- (2011): "Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments". http://bit.ly/JVaRAN (accessed 10 June 2012).
- (2012): "Study on monetising privacy: and economic model for pricing personal information". http://bit.ly/AoeVDv (accessed 05 June 2012).

GROSSKLAGS, J. & ACQUISTI, A. (2007): "When 25 cents is too much: an experiment on willingness-to-sell and willingness-to-protect personal information", WEIS 2007. http://bit.ly/fVSi1v (accessed 15 June 2012).

HANN, I.-H., HUI, K.-L., LEE, T. S. & PNG, I. P. L. (2002): "Online Information Privacy: mesaure the cost-benefit trade-off", *2002 Twenty-Third International Conference on Information Systems*.

HUBERMAN, B. A., ADAR, E. & FINE, L. R. (2006): "Valuating Privacy", *Proceedings of the Workshop on the Economics of Information Security* (WEIS '06).

ICC UK (2012): "Cookie Guide". http://bit.ly/H9DvwD (accessed 28 May 2012).

LAUDON, K. C. (1996): "Markets and privacy", Association for Computing Machinery, *Communications of the ACM*, 39, 9, pp. 92-104.

PHILIPS, J., CAPE, P. & VOGELS, M. (2012): "Creating the ultimate cookie recipe", ESOMAR Live presentation, 03 April 2012.

PREIBUSCH, S. (2010): "Experiments and formal methods for privacy research", Paper presented at the Privacy and usability Methods Pow-Wow (PUMP) 2010.

SHAPIRO, C. & VARIAN, H. (1997): "US Government Information Policy". http://bit.ly/MwJhtU (accessed 10 June 2012).

SMITH, H. J., MILBERG, S. J., & BURKE, S. J. (1996): "Information privacy: measuring individuals' concerns about organizational practices", *MIS Quarterly*, 20:2, pp. 167-196.

STEWART, K. A. & Segars, A. H. (2002): "An empirical examination of the concern for information privacy instrument", *Information Systems Research*, 13:1, pp. 36-49.

TSAI, J. Y., EGELMAN, S. CRANOR, L. F. & ACQUISTI, A. (2011): "The Effect of Online Privacy Information on Purchasing Behaviour: an Experimental Study", *Information Systems Research*, Vol. 22, No.2, June 2011, pp. 254-268.

TUCKER, C. (2011): "Social networks, personalized advertising, and perceptions of privacy control", NET Institute Working Paper No. 10-07; MIT Sloan Research Paper No. 4851-10. http://bit.ly/iT1ATt (accessed 17 September 2012).

WATHIEU, L. & FRIEDMAN, A. (2007): "An Empirical Approach to Understanding Privacy Valuation", Working paper.

World Economic Forum (2011): "Personal data: the emergence of a new asset class". http://bit.ly/fEnXO8 (accessed 11 June 2012).

EU/EC documents

Charter of Fundamental Rights of the European Union (2000) OJ C364.

Commission (EC): "Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century" COM (2012) 9 final, 25 January 2012.

Council of Europe (1981): "Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", ETS No. 108. http://bit.ly/NhNIgN (accessed 23 May 2012).

Directive (EC) 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L281.

EU Network of Independent Experts on Fundamental Rights (2006): "Commentary of the Charter of Fundamental Rights of the European Union". http://bit.ly/KyE5ua (accessed 13 May 2012).

Speeches

Speech by Daniel Weitzner (US Deputy Chief Technology Officer for Internet Policy), EU Conference: Privacy and Protection of Personal Data, Washington/Brussels, 19.03.2012. http://bit.ly/GQdh18 (accessed 05 June 2012).

Speech by Ed Markey (US Congressman), EU Conference: *Privacy and Protection of Personal Data*, Washington/Brussels, 19.03.2012. http://bit.ly/MvOF03 (accessed 09 June 2012).

Speech by Viviane Reding (Vice-President of the European Commission), "Toward a new 'gold standard' in data protection," for the EU Conference: *Privacy and Protection of Personal Data*, Washington/Brussels, 19.03.2012. http://bit.ly/GDiE63 (accessed 05 June 2012).