Privacy evaluation: what empirical research on users' valuation of personal data tells us

Internet Policy Review. Journal on internet regulation
Volume 3 | Issue 2

Privacy evaluation: what empirical research on users' valuation of personal data tells us

Federico Morando
Director of Research and Policy & Research fellow, Nexa Center for Internet & Society, Politecnico de Torino, federico.morando@polito.it

Raimondo Iemma
Managing director and doctoral researcher, Nexa Center for Internet & Society, raimondo.iemma@polito.it

Emilio Raiteri
Researcher, "Cognetti de Martiis" Economics and Statistics department, emilio.raiteri@unito.it

The EU General Data Protection Regulation is supposed to introduce several innovations, including the right of data portability for data subjects. In this article, we review recent literature documenting experiments to assess users' valuation of personal data, with the purpose to provide policy-oriented remarks. In particular, contextual aspects, conflicts between *declared* and *revealed* preferences, as well as the suggestion that personal data is not conceivable as a single good, but instead as a bundle, are taken into account, also discussing potential shortcomings and pitfalls in the surveyed experiments. Data portability is supposed to increase consumer empowerment; still, several technological preconditions need to apply to make this right actually enforceable.

Keywords: Privacy, Personal data, Economic value

Article information

Received: 27 Mar 2014 **Reviewed:** 17 Apr 2014 **Published:** 20 May 2014

Competing interests: The author has declared that no competing interests exist that have influenced or be perceived to have influenced the text.

URL:
http://policyreview.info/articles/analysis/privacy-evaluation-what-empirical-research-users-valuation-personal-data-tells-us

Citation: Morando, F. & Iemma, R. & Raiteri, E. (2014). Privacy evaluation: what empirical research on users' valuation of personal data tells us. *Internet Policy Review*, 3(2). doi:10.14763/2014.2.283

Acknowledgement: This article has been drafted in the context of the "Privacy, Identity, Trust and Reputation Mechanisms" joint research activity of the European Network of Excellence on Internet Science (EINS). Part of the research activity underlying this article has been supported by an unrestricted contribution from Telecom Italia to the Nexa Center for Internet & Society at Politecnico di Torino (DAUIN). The authors also wish to thank the Internet Policy Review reviewers and editors for their constructive criticism and suggestions.

It could be argued that the European Commission proposal for a General Data Protection Regulation (PDF) is far more 'Internet-aware' than its predecessor (still in force) Directive 95/46/EC (PDF), by taking into account challenges related to data exchange happening online. Several rules are being enhanced, e.g., *ex ante* privacy assessment for the data controller, new requirements in terms of 'privacy by design' and 'privacy by default' measures, as well as stronger sanctions in case of breach. Moreover, new rights are being introduced, such as data portability (Article 18), for which the data subject has the right to obtain from the data controller a copy of the data, and transfer it to another information system. While the measures may be effective in some regards, there is reason to question if the underlying assumptions about user's valuation of privacy are being taken into account sufficiently. As a contribution to this discussion, we report a review of the recent economic literature aimed at empirically assessing users' (i.e. in particular, internet users') valuation of their personal data1, suggesting possible limitations and pitfalls in the experiments, and drawing policy-oriented remarks focused on data portability.

As far as the scope of this article is concerned, we derive the definition of 'personal data' from the one suggested in the OECD Privacy Guidelines (1980), i.e. "any information relating to an identified or identifiable individual (data subject)"2.

As indicated by the OECD (2013), with 'value of personal data' we may mean their market valuation, or the valuation expressed by individuals (the latter being the focus of the article at hand). Examples of market valuation methodologies encompass the calculation of the ratio between an indicator of performance of a data holder (i.e. capitalisation, or annual income) and the number of users, thus deriving the value of a single profile; the observation of market prices for personal data; as well as the cost of a data breach (Ponemon and Symantec, 2011). Individual valuations are instead inferred through surveys and/or economic experiments.

THE ECONOMICS OF PERSONAL DATA

If one matches the exponential reduction in the cost of managing information with the exponential growth in the amount of information shared in a digital environment by users, the trivial outcome is that organisations are increasingly in the position of holding information about individuals. A single consumer can experience both benefits and costs from the disclosure of personal information (Hann, 2007). At the same time, an organisation gains clear advantages from being able to increase its knowledge about consumers' identity and behaviour. Still, it may deem detrimental for its own business to design too invasive policies (Acquisti, 2010). For all actors, what seems to matter is that personal data (regardless of its amount) is used in an appropriate context (Nissembaum, 2004). Back in 1996, Varian suggested that some forms of annoyance may arise when the seller/service provider has too little (and not 'too much') information about the user. Others, such as Acquisti (2010), include 'psychological discomfort' amongst the negative externalities affecting consumers receiving customised ads.

DO PEOPLE VALUE PRIVACY?

THE PRIVACY PARADOX

Spiekermann et al. (2001) suggest that even privacy conscious individuals are likely to share sensitive information with strangers, in particular online. As observed by the authors, most

people do not "live up to their self-reported privacy preferences". Applying the "revealed preferences" theory3, this and similar evidence has been used to argue that our society, quite simply, does not place much value on privacy.

The conflict between *declared* and *revealed* preferences seems to be the starting point of the empirical assessment of the value of personal data online analysed here. Consumers express concerns regarding misuse of personal data, e.g., they describe themselves as worried and state their high evaluation of personal data and privacy, in response to various kinds of questionnaire-based surveys. Yet, they continue to provide personal data on social networks, online shopping, and other sites.

Similar conclusions are reached in other studies. For instance, Acquisti and Grossklags (2005) report in a sample interviewed in the US, that almost 90% of individuals declared to be moderately or very concerned about privacy, but more than 20% of the people in the same sample admitted to have disclosed their social security number (a very sensitive piece of information) for discounts or better services. Almost 30% did the same with their phone number.

Similarly, Beresford et al. (2012) built an experiment whose conclusions suggest that people are not sensitive to privacy concerns in their actual behaviour, even if they state they are: in a sample of 225 German students, participants were willing to provide information about their monthly income and date of birth for a one Euro discount. Even in a context of equal prices, the choice between two different firms to purchase a DVD seemed to give a virtually zero premium to the more privacy-friendly vendor. Nevertheless, in the post-experimental questionnaire, 75% of the participants indicated that they have a very strong interest in data protection.

THE ROLE OF CONTEXTUAL INFORMATION

However, as observed by Acquisti and Grossklags 2005, "[i]ndividuals make privacy-sensitive decisions based on multiple factors, including (but not limited to) what they know, how much they care, and how costly and effective they believe their actions can be." Therefore, the dichotomy between expressed and revealed preferences does not necessarily imply irrationality or the existence of a paradox. Indeed, an entire strand of literature questions the idea that less privacy is the social norm and it argues that privacy valuations are extremely sensitive to contextual effects.

The endowment effect

Acquisti et al. (2009) investigate individual privacy valuations in a series of experiments informed by behavioural economics. The authors highlight that discussions about privacy valuations often conflate two different types of transactions: the ones in which individuals are offered benefits in exchange for their personal information, and the ones in which individuals are offered protection of their personal information, but at some cost. Therefore, they investigate the presence of any significant difference between the "willingness to pay"4) to protect individuals' privacy and their "willingness to accept" money (WTA5) in order to give up privacy protection. The latter authors hypothesise that individual privacy valuations are not as stable or internally consistent as the standard economic perspective assumes and argue that preferences about privacy may critically depend on the context and in particular on initial endowment. They test their hypothesis in a series of experiments in which subjects were asked to choose between gift cards that varied in terms of privacy features and monetary values. Then they investigated subjects' willingness to keep versus exchange a specific gift card as a function of initial endowment. More than half of subjects endowed with a completely anonymous $10 gift card rejected an offer of $2 to reveal their future purchase data. By contrast, fewer than 10% of

subjects endowed with the identified $12 card chose to give up $2 to protect future purchase data. These results imply that consumers endowed with different levels of privacy protection valued the same good, i.e. future privacy protection, in a substantially different way. Most of the consumers whose privacy was fully protected did not considered $2 as a price high enough to sell their future purchasing data, while nine out of ten of the not protected individuals estimated $2 as a too high price to buy protection for future purchase data.The results of the experiment therefore suggest that when consumers feel that their privacy is protected, they might value it much more than when they feel their data has already been, or may be, revealed.

Privacy complexities

Many internet users feel that privacy policies are complex and hard to communicate. Despite this general feeling, some authors show that more prominent privacy information will induce consumers to incorporate privacy considerations into their online purchasing decisions.

Tsai et al. (2010) ran an online shopping experiment, in which different sets of participants were asked to test a new search engine whose results were annotated with icons, and to purchase two different products online, one characterised by low privacy concern and the other by higher privacy concerns (AA batteries and a sex toy, respectively) using their personal credit card. Some of the participants were exposed to icons based on an analysis of the site's privacy policy (while, in two control conditions, the icons either indicated ostensibly irrelevant information or were absent). Results showed that participants in the privacy information condition were more likely than those in the control conditions to make purchases from websites offering medium or high levels of privacy, even when the price was higher than the price on other sites, for both products. Quite surprisingly, the premium to privacy was similar in purchasing the batteries and the sex toys.

In a similar experiment performed by Egelman et al. (2012), 25% of the participants (confronted with four screenshots including permission requests for activities such as internet access, location, audio recording) stated a willingness to pay a $1.50 premium on a $0.49 Android application, in order to grant the fewest possible privacy permissions.

Individuals' heterogeneity

Several studies find various groups or clusters of individuals, with homogeneous intra-group characteristics and significant inter-group heterogeneity in terms of privacy preferences. For instance, Hann et al. (2007) find three different clusters in terms of privacy evaluation: 'privacy guardians', i.e. people who attach a relatively high value to information privacy; 'information sellers', who tend to give away personal information with little regard for privacy policies; and 'convenience seekers', people who prefer convenience with little regard for money or website privacy policies. According to these authors, privacy guardians are the vast majority (between 70% and 85% of their sample), but other experiments and analysis identify similar groups with completely different proportions. For instance, according to Westin (2001), 'privacy fundamentalists' are about 25% of the sample, in Krasnova et al. (2012) 'Privacy-concerned' represent 33% of the full sampled population, while McKinsey (2010) identifies a much smaller set of highly privacy-concerned people (about 1%).

TRADING PRIVACY

PRIVACY STATEMENT AND POTENTIAL SUBSTITUTES

Despite the commonly shared experience that privacy notices are frequently neglected, there is

empirical evidence that the existence of a privacy statement makes people more available to share data, even for free (Hui et al., 2007; Tsai et al., 2010; Hann et al., 2007; Tucker, 2012).

That said, privacy statements only represent one condition and, not necessarily a sufficient one, to create a trusted relationship with the users of an online service. For instance, Joinson et al. (2010) find the existence of a compensatory relationship between privacy and trust, therefore recommending to businesses eager to collect users' personal information to increase their trustworthiness (e.g., with a 'professional' look & feel of their website), rather than providing users with stricter privacy policies.

CONVENIENCE AND PERSONALISATION

Several studies (Hann et al., 2002; Hann et al., 2007; Tucker, 2012) show that individuals are willing to trade personal information in order to gain convenience in terms of time saving and personalisation of web services. As already mentioned, several studies, such as Hann et al. (2007), identify various groups of users, some of which are more willing to exchange their data in exchange of monetary incentives and some others in exchange of other forms of convenience, in particular time-saving features. This is not surprising, since, for instance, the opportunity cost of time greatly differs amongst people.

SOCIAL REWARDS

Even in the absence of any monetary or other tangible rewards, social rewards are attractive in balancing privacy concerns and governing individuals' behaviour as well (Jiang et al., 2013).

For instance, in social networks the social reward increases with the size of one's network. Therefore a larger network is expected to lead to higher disclosure levels, as observed by Krasnova et al. (2009).

MONETARY INCENTIVES

Most of the recent surveys and experiments that deal with privacy evaluation confirm that financial incentives lead people to disclose more information or that people concerned about privacy are willing to pay a premium price in order to avoid disclosure (see, e.g., Beresford et al., 2012; Carrascal et al., 2011). For instance, Hann et al. (2007), analysing the results of a survey conducted in the US and Singapore, find that a sufficiently large monetary reward significantly increased the relative attractiveness of a website regardless of its privacy policy. Carrascal et al. (2011) carried out an experiment in which they monitored online activities of participants and asked them (through pop-up windows) the minimum value they would accept to sell a specific piece of personal information to a private company. While the price asked for different kinds of private information showed great variability, participants generally proved to be willing to trade private information for monetary rewards. As far as WTP to protect information is concerned, Hann et al. (2002) show that the disallowance of secondary use of personal information is worth between $40 and $50. Similarly, Krasnova et al. (2009) observe that, on average, a user would be ready to pay between 14 and 17 Euros per year, if the social network providers refrained from using his or her demographic information for personalised advertising. Bauer et al. (2012) organised an experiment in which participants were asked to make a bid to migrate their Facebook profile information to Google Plus, asking participants to simulate the situation in which Facebook was about to be shut down. They find out that, on average, participants would pay 9.40 Euros to save their personal profile.

LIMITATIONS AND PITFALLS IN THE REVIEWED EXPERIMENTS

The limitations of the surveys and experiments reported above have not to be underrated. In particular, each analysis seems to be very context-dependent. In many cases, participants are - by definition - aware of the fact that their declarations and behaviour are produced in the framework of an experiment, even though the actual objectives of the simulation may not be *ex ante* disclosed to the participants. What is important in this respect is that participants are not actually experiencing tangible/intangible gains and losses. In fact, it would be arguably unsustainable to observe choices without the participants' consent, since this could entail a violation of their privacy, and/or other rights. Moreover, results are not independent from the way questions are formulated, and scenarios sketched. It is the case, for instance, of the already mentioned endowment effect (Acquisti et al., 2009).

Moreover, the actual definition of personal data varies amongst experiments and what is actually measured in each case is the value of preserving a certain subset of one's personal data, with respect to a certain set of perceived risks. In particular, Huberman et al. (2005) demonstrate that the more undesirable a personal trait *vis-à-vis* the group average is, the more valuable a single piece of private information will be. Therefore, if for instance we hypothesise that a piece of information (e.g., weight) is valuable only if its level is far away from the average (and maybe mainly if it is higher than that), the underlying distribution of the valuations for individuals will be extremely skewed. The same goes with the work of Carrascal et al. (2011), which reports how people attach different value to different pieces of personal information (offline vs online generated personal data). Moreover, most of the studies considered in this paper refer to disclosure as a dichotomous variable. In their settings, an individual may disclose or not disclose a specific piece of information. However, individuals may in fact decide to misrepresent and report a false information instead of not disclosing. That would be especially the case for services that require some degree of disclosure in order to obtain access (Jiang et al., 2013).

Finally, some kind of 'selection bias' can be recognised. Experiments are frequently conducted with undergraduate students as participants, and, in general, they involve categories of individuals characterised by a higher willingness to participate (e.g., because they are sensitive to a reward, or simply because they tend to have more free time than others). As a result, samples might be not sufficiently representative of internet users as a whole (and even less of human beings in general).

MAKING DATA PORTABILITY ENFORCEABLE

LESSONS LEARNED FROM THE SURVEY

What is fairly evident from the experiments reported above is that people differ in their valuation of personal data, and in their willingness to trade privacy for money and/or for some forms of convenience. Another point that seems to emerge is that contextual factors matter. As noted by Nissembaum (2004), "no arenas of life are not governed by norms of information flows", which are rooted in contexts that are more specific than what is suggested by the pure 'private' vs 'public' dichotomy, i.e. crossing them, or belonging to a plurality of distinct realms. When contextual elements are taken into account (including the cost and benefit of taking care of one's privacy in a given context), users seem to be willing to assign a non-negligible value to

their privacy and therefore businesses could use privacy strategically, leveraging the protection of private information as a competitive advantage. More generally, the empirical literature reviewed in this article seems to support the ongoing evolution in the data protection domain. At least in certain situations, people seem to devote limited attention to the protection of their personal data, and it becomes a meme that privacy is somehow old-fashioned, yet new or stronger rights are granted to individuals. This situation could be justified by a certain degree of paternalism of a legislator who thinks that there is indeed a privacy paradox, and that the actual preferences of individuals are the ones they declare and not the ones they reveal. However, properly taking context into account frequently dispels this paradox, still making clear that privacy does matter and deserves legal protection, but also that it is not always easy/feasible enough to change one's behaviour just because of data protection related reasons. Therefore, putting some burden on the shoulders of those who systematically treat large amounts of data - and are frequently the cheapest cost avoiders6 for personal data risks related to a specific business - may be a good policy choice. This would support *ex ante* privacy impact assessments and similar obligations included in the proposed EU General Data Protection Regulation.

As a further aspect to be considered (or, possibly, as a further specification of the concept of relevant context), the discrepancy between what people respond in a survey and their actual behaviour may be due to the fact that personal data is not conceivable as a single good, but should be considered as a bundle of goods to which different individuals attach different values. When asked in a survey about the value they assign to personal data/privacy protection they could probably think to the most valuable information they have in their 'privacy bundle'. In a real life context or a real life-like experiment the required information to access a service or to perform a specific task may be of low value.

IMPROVING DATA PORTABILITY

The complexity and multidimensionality of any serious discussion about personal data suggests that another welcome development in the domain of data protection regulation may consist in facilitating the emergence of intermediaries allowing people to easily manage their own personal data in a customised way (to accommodate for individuals' heterogeneity, leaving room for convenient and personalised services), keeping low the transaction costs involved in the process and possibly monetising some data exchanges (since there is evidence that people do trade privacy for money, to a certain extent), and keeping safe the data which is most sensitive for any single person (which is an activity performed, so far, just by the individuals themselves7).

In this regard, new markets may be based on the new rights granted by the EU General Data Protection Regulation, e.g., the right to data portability, that would give the opportunity for the data subject to obtain a copy of the data from the controller, and transmit it into another processing system. For instance, personal data could be managed by agents that perform services on behalf of the individual, such as 'personal data vaults'. Intermediaries assisting users in consumption choices by analysing and benchmarking their current consumption patterns (exploiting the so-called smart disclosure (HTML) paradigm) are other examples of business-oriented re-uses of personal data.

Empowering users' ability to manage their own data would arguably make less burdensome long term implications. In fact, one may submit that individuals act to protect their privacy as a result of a comparison between the advantages and costs of keeping data under control (i.e. reaching the optimal level of control over personal data). Frequently, the value of sharing data is high in the short run, but one may change his mind (or simply his subjective situation) in the longer run: today, despite the existence in the letter of the law of a broad set of rights actionable by

individuals, the cost of actually managing one's personal data is still very high (and possibly on purpose), also because users may miss the long run implications of their short run choices, and harmful effects may appear only later, when unexpected data combinations are performed downstream (Solove, 2013). Making data portability actionable would let users directly govern such combinations as they best see fit.

However, to make this opportunity as attractive as it may seem on paper, several conditions need to apply. Broadly speaking, actual data portability would be enhanced by reducing the cost of management of one's data also in the medium/long run through technological means mandated by law (e.g., following technical guidelines designed by data protection authorities, in order to avoid a quick obsolescence of the law). The role of technological means to monitor one's personal data should not be underrated. Even without implementing sophisticated approaches, such as privacy by design, some simple arrangements could have a relevant impact here. For instance, the establishment of a centralised registry in which data controllers should simply list all the data subjects present in their databases (e.g., by e-mail, phone number, tax number, or other of a set of predefined and unique identifiers) may be a first step to make data portability rights enforceable in practice, trivially by making users easily aware of which data controller is holding what data. Today, this is practically impossible and data subjects just notice cases in which they feel directly bothered (e.g., when contacted) by data controllers. Moreover, there are cases in which some data controllers become, e.g., a source of significant disturbance (think about undesired e-mails, text messages, or phone calls), or they just start being mistrusted by the data subject. In these cases, it would be precious to have a simple and cheap way to check if the data controller actually declared to have data about the data subject, to check which data, received from whom, under which prerogatives, as well as which services would be discontinued asking for the deletion of such data. It is a common direct experience (at least, in Italy) that the aforementioned check is quite burdensome for the data subject.

In conclusion, the extreme context-dependency of the evaluation of personal data suggests that general rules are important, but also case-by-case arrangements are needed. On the one hand, this supports the idea that business specific duties are appropriate, e.g., an *ex ante* personal data impact assessment may be used to evaluate the specific data protection risks related with a given business model and technology applied to a certain set of data. On the other hand, it is appropriate to also allow individuals to customise their own level of care, depending on their own subjective evaluation of which contexts are more delicate for them in terms of data protection. To do that, individuals may need the support of infomediaries (e.g., to apply big data analytics techniques in a defensive way), which could become a reality if some technical and legal preconditions apply: technology and standardisation are needed to make data portability actually enforceable, and it should become clear that it is possible to delegate the exercise of data portability related activities, so that third parties may build new data related business models, at the service of data subjects.

METHODOLOGICAL APPENDIX

We limited the scope of this survey to studies that make use of field experiments and survey methodologies to induce the users of privacy-sensitive services to assign a value to their personal data and to reveal their preferences on privacy protection. Moreover, since we are mostly interested in studies that provide an assessment of how much individuals care about, and value their personal information online, we dedicate special attention to works that analyse the privacy valuation issue in the internet environment. For this reason, most of the surveyed

studies are not older than a decade.

In order to identify relevant contributions on this specific topic, we searched the Google Scholar database mainly using the following keywords: 'economics of privacy', 'value of personal data', 'users' valuation of personal information', 'empirical analysis', 'field experiment', 'online information privacy'. The bibliography of *prima facie* relevant works was then iteratively analysed, following citations. We limited our survey only to articles appearing in international peer reviewed journals, belonging to the economic, the legal, and the information system fields, and to proceedings of globally renowned conferences that devoted attention to the economics of privacy, such as e.g., the European Conference on Information Systems (ECIS) and the Symposium On Usable Privacy and Security (SOUPS). After a preliminary analysis of several titles and abstracts, some 30 contributions were scrutinised in depth (about two thirds of these most relevant works are concentrated in the 2010 decade).

We then considered if the works we collected provided insights about three main issues: whether an article adopted any empirical methodology to estimate the value that users assigned to privacy; whether the study tried to investigate which contextual factors affected the personal assessment of private information; and whether work suggested an objective formula to estimate the value of personal data on the basis of specific individuals' attributes.

REFERENCES

Coase, R. (1946). The Marginal Cost Controversy. *Economica, New Series, 13*(51), 169-182.

Acquisti, A, Leslie, J., and Loewenstein, G. (2009). What is privacy worth. *Workshop on Information Systems and Economics* (WISE).

Acquisti, A. (2010). The economics of personal data and the economics of privacy, *Background Paper for OECD Joint WPISP-WPIE Roundtable 1*.

Bauer, C.; Korunovska, J., and Spiekermann, S., (2012). "On the value of information - what Facebook users are willing to pay" (2012). *ECIS 2012 Proceedings. Paper 197.* Available at: http://aisel.aisnet.org/ecis2012/197

Beresford, A., Kübler, D., and Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters 117.1* (2012): 25-27

Besmer, A., Watson, J., and Richter Lipford, H. (2010). The impact of social navigation on privacy policy configuration. *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM.

Canny, John (2002). Collaborative filtering with privacy. *Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on*. IEEE

Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & de Oliveira, R. (2013, May). Your browsing behavior for a big mac: Economics of personal information online. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 189-200). International World Wide Web Conferences Steering Committee.

Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice architecture and smartphone privacy:

There'sa price for that. In *The Economics of Information Security and Privacy* (pp. 211-236). Springer Berlin Heidelberg.

Gentry, C. (2009). *A fully homomorphic encryption scheme* (Doctoral dissertation, Stanford University).

Goldfarb, A., & Tucker, C. E. (2011). Privacy regulation and online advertising. *Management Science, 57*(1), 57-71.

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24*(2), 13-42.

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2002, December). Online Information Privacy: Measuring the Cost-Benefit Trade-Off. In ICIS (p. 1).

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: an exploratory field experiment. *Mis Quarterly, 31*(1), 19-33.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research, 24*(3), 579-595.

Joinson, A. N., Reips, U. D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction, 25*(1), 1-24.

Joinson, Adam N., Alan Woodley, and Ulf-Dietrich Reips. "Personalization, authentication and self-disclosure in self-administered Internet surveys." Computers in Human Behavior 23.1 (2007): 275-285.

Krasnova, H., Hildebrand, T., & Guenther, O. (2009). Investigating the value of privacy in online social networks: conjoint analysis.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering, 4*(3), 127-135.

McKinsey (2010, September). Consumers driving the digital uptake. Technical report, McKinsey and Company and IAB Europe.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev., 79*, 119.

OECD (2013), "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", OECD Digital Economy Papers, No. 220, OECD Publishing. http://dx.doi.org/10.1787/5k486qtxldmq-en

Schwaig, K. S., Segars, A. H., Grover, V., & Fiedler, K. D. (2013). A model of consumers' perceptions of the invasion of information privacy. *Information & Management, 50*(1), 1-12.

Solove, D. J. (2013). Introduction: Privacy Self-Management and the Consent Dilemma.

Symantec and Ponemon Institute (2012, March). Cost of Data Breach Study.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254-268.

Tucker, Catherine (2010), The Economics Value of Online Customer Data, www.oecd.org/dataoecd/8/53/46968839.pdf

Tucker, C. E. (2012). The economics of advertising and privacy. *International journal of Industrial organization, 30*(3), 326-329.

Turow, J., King, J., Hoofnatle, C. J., Bleakley, A., & Hennessy, M. (2009). Americans reject tailored advertising and three activities that enable it. *Departmental Papers (ASC)*, 137.

Varian, H. R. (2002). Economic aspects of personal privacy. In *Cyber Policy and Economics in an Internet Age* (pp. 127-137). Springer US.

World Economic Forum, Personal Data: The Emergence of a New Asset Class (2011). Available at: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

FOOTNOTES

1. A brief methodological appendix is available at the end of the paper.

2. In particular, we focus on the 'digital footprint' of an individual, i.e. all data left behind by users within their use of digital services, and the personally unique arrangement that makes someone identifiable just upon the specific combination of her system information. As noted by the OECD (2013), personal data is in fact collected online in different ways: (i) data can be voluntarily shared by a consumer; (ii) data can be observed or recorded, with or without consumers' knowledge, or explicit consent; (iii) data that can be inferred. In other cases (Acquisti, 2010), personal data remains protected, either because it was intentionally not disclosed by a consumer, or because the service provider is not able to access it.

3. The revealed preferences theory suggests that preferences of consumers can be inferred - through appropriate methodologies - by their purchasing habits and choices.

4. WTP is the maximum price a person would be willing to pay to acquire a good she did not own.

5. WTA can be defined as the lowest price a person would be willing to accept to part with a good.

6. In law and economics, the **cheapest cost avoider** is the party which can prevent (or abate) a potential damage at the lowest cost. In the domain of torts - e.g., in defining the law about car accidents - the cheapest cost avoider should bear the responsibility in case of damages, so that he/she receives an incentive to invest in precaution.

7. Technological developments such as big data analytics may challenge home-made solutions in this domain.