An Empirical Approach to Understanding Privacy Valuation

Allan Friedman
Kennedy School of Government
allan_friedman@ksgphd.harvard.edu

Luc Wathieu
Harvard Business School
lwathieu@hbs.edu

ABSTRACT

As privacy becomes more central to information policy debates, conceptual privacy frameworks have increasingly used economic models. However, our understanding of the motivating factors behind informational privacy behavior is far from complete. This paper uses an economic behavior experiment to assess consumer privacy sentiments in controlled conditions to better understand the tradeoffs between privacy and economic benefits. In particular, we find that consumers consider the type of personal information, and how that data will be used, rather than a broader aversion to all information collection. We also find some evidence supporting a "privacy externality" where consumers rationally oppose a data collection scheme that does not directly impact them or make use of their data, and that opting-out allows a more realistic expression of privacy preferences.

1. INTRODUCTION

There are many views on how privacy sentiments are manifest in society, from the legal perspective, the philosophical perspective and, increasingly, the economic perspective. Unfortunately, very little is known about how consumers in the context of the real world understand their privacy. We know that many individuals believe that it is important, but there are many unjustified claims about individual's priorities, values and feelings [17], to say nothing of their actions.

If the scholarly community hopes to build valid economic models of situations involving personal information, there are critical pieces missing: what people mean when they talk about privacy, what people are concerned about in situations that involve personal information, and how well people understand situations involving the flow of personal information.

This paper argues that very little is known about that currently, and bases several straightforward hypotheses on prior literature. We then propose an experiment based on a situation involving personal information in a real-world context. We evaluate the responses of 657 subjects and discuss what the subjects reactions imply about how they value privacy, and to what extent such reactions conform to a rational framework.

2. Understanding consumer privacy concerns

Building economic models around consumer privacy requires an understanding of how consumers value privacy. Survey evidence extends back decades showing that people are concerned with privacy. However, surveys to date have lacked the mechanisms to assess *how* consumers think about privacy; getting people who are truly concerned about privacy to reveal their true preferences presents its own problem. [16] Surveys also lack the trade-offs that consumers face in the real world.

2.1 Experimental work

The limited scope of experiments has made some reasonable assertions about consumer privacy behavior. Huberman, Adar and Fine [11] suggest that privacy valuation is a function of perceived deviance. While this helps clarify strength of some individuals' preferences, deviance cannot explain all preferences, particularly over data that does not fit in a normal/deviant model, such as name/address pairs. Rational privacy protection behavior can be seen in [7] but such results may depend on very explicit information on risk and reward. A series of detailed, interactive surveys [2] of users critiques the model of a rational privacy-protecting consumer, but this analysis applies to broad range of privacy lifestyle choices, rather than directly inducing trade-offs. Such trade-offs can be driven by actually watching user behavior [5, 18] or in conjoint analysis to derive values of resolving privacy concerns [10]. While these tools provide an important understanding of privacy sentiments in a specific context, or a useful dollar value, it is difficult to apply them to a larger context.

2.2 Theory and Hypotheses

We focus on a world where actors—usually in the form of businesses—seek to gain information for some anticipated benefit for themselves. This benefit can take many forms, including internal systems development and improvement [9], targeted marketing [14, 20], loyalty programs [6], or maximizing profits through price discrimination [15]. In most cases, the firm is the driving actor to collect and/or use personal information. Whether this is a problem depends on the consumer's reaction. In extreme cases, where the benefit is obvious (an emergency medical practitioner can obtain life-saving information) or negative (an increased likelihood of unwanted telephone solicitation [14]), anticipating consumer reaction is trivial. What is less understood are the more balanced trade-offs, with subtler benefits or less obvious cost or risk factors.

When the cost-benefit relationship of revealing personal information easily evident from the situation, then individuals often use heuristics based on characteristics of the situation [19]. To understand how consumers make decisions with respect to privacy, it is necessary to understand which aspects of a given privacy situation are critical to consumer privacy concerns. Experiments afford clear advantages in isolating specific factors.

One open question in privacy policy is whether to stress information *collection* or information *use.* On one hand, the mere collection of data is unlikely to cause harms, either actual or perceived. Thus, the consumer should focus on how information should be used. On the other hand, digital information is notoriously hard to control, and the consumer may have no reason to trust the collector of information to safeguard against unauthorized use. Thus, the consumer's focus would be on *control* of personal data. This perspective is embodied in the emphasis on privacy-enhancing technologies [1] and user-empowerment [3]. The focus on use, on the other hand, is manifest in the European Union's Privacy Directive that implements statutory protection on data use and transfer.

Although many people in the information privacy community have embraced the data control model, it is not clear why consumers would prefer that model. First, their information is already well spread throughout the commercial sector. After witnessing the extent to which their data is widely known, consumers may feel that it is futile to further control their information. Furthermore, while control may be a more immediate decision, the use of information is more salient for a rational actor. This leads to our first hypothesis:

> H1: Consumers will be more concerned over *use* of their personal information than *controlling* that information.

This can be demonstrated by showing that varying potential usage will alter privacy concern, but alter patterns of data collection to interfere with data control will not.

Related to the use of personal information is the type information. A reasonably rational consumer would be worried about the dissemination of information when that data could be used to the consumer's detriment, but be less concerned when the privacy loss accompanying the information collection and/or use causes little direct harm. If privacy is, in fact, an economic issue, then consumers will be sensitized of data that can cause economic harms. This leads to our second hypothesis:

> H2: Consumers will be more concerned about privacy when the data can lead to economic harms, than they would for other types of information.

The second hypothesis is related to the first, in that it also suggests that data usage, as opposed to exposure or dissemination, is key.

Some harms from privacy have are fairly concrete: if an individual has his or her credit card number stolen from an insecure database, monetary loss will follow. Other harms, such as price discrimination, are less obvious. Wathieu proposes a privacy harm from market segmentation [20]. Without extensive consumer information, a producer will not be able to effectively target niche customers in a heterogeneous market. Instead, the producer will target the majority, and the minority will consume a sub-optimal good. However, this benefits the majority, who gains from economies of scale. The critical part is that there is a "privacy externality" since a population is harmed even though their personal information was neither collected nor used. This privacy concern is a function of market structure aiding others at the expense of the majority by segmenting the market. It leads to the following hypothesis:

> H3: Consumers will feel concerned about privacy in specific market situations, even if their personal information is not used. This applies when market can be segmented at the expense of those consumers.

Beyond understanding immediate concerns in privacy evaluations, a good economic model should have the prescribed reaction. The question of whether to opt-in or opt-out of information-sharing schemes has been somewhat controversial inside the privacy community. In an opt-in system, the default is to not participate, while an opt-out allows those who do not wish to participate to withdraw. In a purely rational world, they would be identical, of course. In general, privacy activists believe that an opt-in scheme would better align with a pro-privacy regime, since it places the burden of responsibility on those actors who would benefit form information disclosure. Experimental results have shown [12] that the default option has an enormous impact on actual consumer choice. The strength of the default option in an opt-in/opt-out context has even been shown to apply critical decisions like organ-donation [13]. If we assume that people feel strongly about organ donation, then we cannot assume that apathy explains the privacy-driven opt-in/opt-out split. From this, it follows that:

> H4: An opt-in regime will meet privacy needs better than an opt-out regime.

3. Research Design

To understand how consumers treat information privacy in a complex environment and test the above hypotheses, we constructed an experiment in which participants were presented with a realistic scenario involving personal information in a marketing context and asked for their reactions. While there were no direct incentives to elicit the maximum preferences, there was no incentive to lie, or map preferences onto responses. An opinion-driven experiment allowed us to model a less-contrived set of situations that did not reduce to a simple calculation. At the same time, varying the scenario into control and test conditions gives us more information than a sample survey. There is no "right" answer for participants, either economically or psychologically. We also sought a scenario that could be generalized beyond computer-mediated environments.

3.1 Experimental scenario

To evaluate the theoretical hypotheses presented above, we looked for a situation where consumers could potentially benefit from an exchange of personal information for some market-driven good. The exchange in question had to have ramifications beyond simple marketing hassle. Affinity marketing of financial services met our needs. There has been an increase in trusted parties such as alumni organizations being asked to share their membership databases to offer targeted deals to their members. We adapted general trend to a specific scenario where the entire membership is targeted, but only some fraction of the members will receive a clear benefit. The base scenario participants were given was:

> As a service to its members your college alumni association has negotiated a special deal with a well-known car insurance company.

> The insurance company will use data (including members' name and contact information) on a one-time basis to offer alumni (via a mail and phone marketing campaign) an alumni association-endorsed deal featuring first-class service levels and a 30% discount on annual insurance premiums.
>
> Based on certain parameters specified by the insurance company, data for 20% of the alumni have been transmitted to the insurance company and all of these alumni are about to be offered the deal. At this point it is still unknown whether you are among the beneficiaries of this deal.

The scenario itself did not explicitly offer the participant a choice; they were told this is going to happen. After reading the scenario, the participants were asked four questions how they felt about the scenario. Specifically, they responded to

- How happy they were "that this deal was struck,"
- How fairly they thought the alumni association was treating them,
- How fearful they were "that this kind of activity in the insurance market might ultimately reduce your access to a low-premium contract," and
- How concerned they were about privacy in that situation.

Respondents selected from a 7-point Likert scale. In addition, participants were asked whether they would opt-out of the deal if the opportunity were available to do so, whether they would opt-in if assent was "necessary but easy," and whether they would vote authorize the initiative if they had had been on the board of alumni.

This experiment was designed to elicit honest feedback. None of the questions are asked in such a way that the respondent would be inspired to create a positive impression. The scenario was designed to have nearly balanced immediate costs and benefits, so that any conditions that made it more or less palatable would be measurable.

3.2 Conditions and Execution

Participants were chosen from a pool of volunteers in the Boston area that has self-selected to participate in experiments for compensation. 647 people were randomly divided into twelve groups, averaging around 54 participants in each group, with no group having fewer than 48 respondents. The experiment was administered via a website. The control was the scenario above, which was altered by five possible conditions.

All data shared Rather than only the 20% direct recipients' data being shared, participants are told that the "data of all alumni have been transmitted to the insurance company". The benefit will still only go to 20% of the alumni. (The control case can be thought of as "targeted" data sharing.

More relevant data The shared data is increased by replacing the parenthetical explanation of what data will be transmitted with data that is likely to be used in approximating risk factors for insurance "including members' name, contact information, degree obtained and year, honor student status, GPA, and current occupation".

More irrelevant data The shared data is increased by replacing the parenthetical explanation of what data will be transmitted with data that is less likely to be used in approximating risk factors for insurance "including members' name, contact information, membership in college associations, city of birth, and city of residence at college registration time".

Priming fear To remind participants how insurance companies can discriminate, the following paragraph was inserted into in between the second and third paragraph: "Some have wondered whether the premium paid by ordinary drivers can stay low if car insurance companies continue to use databases to offer special deals to consumers predicted to be 'safe drivers.'"

No personal benefit Participants are told that they will not receive the benefit by replacing the last sentence in the third paragraph with "At this point it has become clear that you are NOT among the beneficiaries of this deal."

Participants were given a scenario that had some combination of these conditions. They did not see other scenarios, so their responses can validly be compared on an individual basis, nor were any personal data collected about them.

4. Results

Mean responses are given for each of the twelve groups in Table 1. Significance is indicated with respect to the control group. The control group is already somewhat concerned about privacy, with 2/3 of the respondents placing their level of concern at 4 or higher out of 7, where 7 is "extremely concerned about privacy." Half of that population has their level of concern at either a 6 or a 7. While the respondents were concerned, they were not dissatisfied

Table 1: Cross-tabulations of privacy and consumer behavior data, with the mean of each treatment compared to the control group

EXPERIMENTAL CONDITIONS	CONCERNED ABOUT PRIVACY Score on 1-7 scale	CONCERNED ABOUT PRIVACY Boolean coding (1-4→0/5-7→1)	ACCEPT? (would not opt-out = 1, would opt-out = 0)	OPT-IN? (yes = 1, no = 0)
(1) Control	4.156863	0.4313725	0.67	0.61
(2) All data shared	**4.859649 ***	**0.6666667 ****	**0.51***	0.51
(3) More relevant data	**5.26 *****	**0.68 ****	**0.4****	0.56
(4) More relevant data/ All data shared	**4.949153 ****	**0.6440678 ****	0.58	0.64
(5) More irrelevant data	4.698113	**0.6037736***	0.62	0.64
(6) More irrelevant data/ All data shared	4.698113	**0.6981132 *****	0.53	0.66
(7) Priming fear	4.481481	0.5555556	**0.5***	0.56
(8) Priming fear/ All data shared	4.770833	**0.6458333****	**0.46****	0.52
(9) No personal benefit	4.431034	0.5172414	**0.48***	0.67
(10) No personal benefit/ All data shared	4.769231	**0.6730769****	0.63	0.63
(11) Priming fear/ No personal benefit	4.763636	**0.6727273****	0.58	0.62
(12) Priming fear/ No personal benefit/ All data shared	**5.052632 ****	**0.6666667****	**0.51***	0.6

*Significance wrt control: ***=(>.01), **=(>.05), *= (>.1)*

with the offer in front of them: over 80% recorded a 6 or a 7. The control shows a cautious population that is nonetheless open to a trade-off between personal data and an opportunity to save.

4.1 Information matters

Of the eleven conditions, the sharpest privacy response was when the insurance companies demanded more relevant data of the participants. Dividing the responses into a Boolean coding also demonstrated a significant difference between this group and the control. Varying the dividing mark for Boolean categorization around any other point maintains significance for that demarcation. The type of personal information has a clear effect on privacy concerns. Participants found the relevant data more worrisome for privacy issues than irrelevant data. Irrelevant data such as college activities can reveal much about the subject, but much less likely to be used for an objectionable purpose. For other Boolean divisors, irrelevant data is not even significantly different from the control case.

Given the context of the scenarios, the relevance of the information takes on particular significance. Car insurers are likely to be interested in a person's college GPA and occupation, as they could be signals for the consumer's credit and risk profile. One's hometown, on the other hand, is not terribly useful. Consumers in this experiment draw privacy distinctions between simply being in a database, providing potentially useful information, and providing useless information. This provides support for H1, since the consumer could see the relevant data as more economically salient, even if it is uncertain whether providing that data will help or hurt the individual. By caring about the type of data, the participant could be anticipating how that data would be used, possibly supporting H2.

4.2 Does data-sharing matter?

Table 2 provides substantial support for the idea that usage matters by rejecting the idea that data control is important. While Table 1 shows that some groups were significantly different from the control group when everyone's data was shared, Table 2 tells a more nuanced story. The twelve groups could be divided into six conditions, half of which sent all the data to the insurance company, while the other half sent only eligible alumni's data. Table 2 displays the difference between restricted and universal data dissemination. We use a t-test to test the assumption that the two means are identical and find little reason to reject this. Inside each group, the means for privacy concerns are statistically similar, with the exception of the control group. Dividing the control group into Boolean categories reduces the difference sharing makes, implying that the effect is fairly weak.

If the data for all alumni is shared, it implies that 80% of the alumni will lose control of their personal information for no benefit. If participants were concerned about control of their personal information, then this would raise more privacy concerns, since there was a greater chance of personal data leaving their control. Since we don't see a significant difference between the privacy concerns of a given scenario, whether or not all data was disseminated, we can be skeptical of the claim that data control is a priority for consumers. This is a more robust argument in favor of H2 arguing for use over control.

4.3 Testing Market Segmentation Theory

It is interesting to note that participants were less happy that everyone's information was shared, particularly when the subjects knew they would not be offered the deal. The top half of Table 3 further explores the relationship between privacy and the other sentiment measures. We find support for the claim of H3 that privacy is related to market opportunities. The question of fairness provoked strong responses in the experiment, but these

Responses were not closely correlated with fairness, or even happiness. In this experiment, concern about market access to good insurance rates is the best predictor of concern about privacy. If consumers were not already aware of market segmentation issues, then priming them with a reminder that their insurance fees could go up would highlight this. Simply adding an explanation of market segmentation does not significantly increase consumers' privacy fears, as seen in Table 1 for group 7. Finally, and perhaps most persuasively, participants who were not eligible for the deal but who were exempt from sharing (group 9 and 11) should not be very concerned about privacy under a standard model. No one will use their data, and no one will contact them. In fact, their concern about privacy should *decrease*. It is the use of other people's data that drives this consternation, suggesting a "privacy externality".

Table 2. Sharing: Group-wise differences between targeted data dissemination and universal data dissemination. For each category, Table 4 shows the difference between the groups, and the p-values between the control's privacy concern and other response variables.

	Privacy	Market Access
Control (contact information)	-0.702	-0.471
p-value of no effect – Likert scale	**0.0516**	0.1384
p-value of no effect - Bifurcated	0.5732	0.2433
Relevant personal information	0.31	-0.42
p-value of no effect – Likert scale	0.3777	0.1599
p-value of no effect - Bifurcated	0.7936	0.3168
Irrelevant personal information	0	0.264
p-value of no effect – Likert scale	1	0.4265
p-value of no effect - Bifurcated	1	0.6235
Priming fear	-0.28	-0.48
p-value of no effect – Likert scale	0.4617	0.1467
p-value of no effect - Bifurcated	0.6043	0.134
No personal benefit	-0.33	0.141
p-value of no effect – Likert scale	0.3394	0.6631
p-value of no effect - Bifurcated	0.8093	0.1984
No personal benefit / Priming	-0.28	-0.46
p-value of no effect – Likert scale	0.373	0.1193
p-value of no effect - Bifurcated	0.3093	0.0747

It is possible that the privacy concerns could stem from a feeling of unhappiness towards a system that does not include them. Participants who were shut out of the deal completely, as the last four groups were, might feel that corporations collecting any data when they do not benefit is a matter of privacy because they were not given the opportunity to opt-in. Participants who did not receive a personal benefit clearly expressed that they were not treated fairly, significant against the control at almost every Boolean break point. This is far more significant than the privacy effects, and is most notably absent in the base case of group 9. We also see that fair treatment has a fairly low correlation coefficient with privacy. While market segmentation may touch on fairness issues, consumers do not conflate fairness and privacy issues. This supports a case for privacy as a market segmentation issue.

4.4 Consumer reactions

The data also gives us some insight on how consumers choose to react to different situations. Participants were asked whether they would choose to opt in, or whether they would choose to opt out. The control condition show that around two-thirds would not opt out of such a program, and 60% would actually opt in. Table 1 shows that as consumer's privacy concerns increased, more participants chose to opt-out. The same conditions that prompted the most apprehension also inspired more people to decide to opt-out. However, the opt-in rate remained relatively constant. Even when privacy anxiety was at its highest in the second group, there was little statistical difference between the number who would opt out when compared to the control group.

This directly contradicts the expectations in H4. We had expected to see the privacy concern better enacted in the opt-in decision. This is further confirmed by correlation analysis in Table 3. The correlation coefficient of over .5 for opting-out is nearly double the correlative relationship between opting-in and privacy. In fact, participants chose to opt-out even when they would not explicitly vote against denying the deal to everyone.

Table 3. Correlations between Privacy Concern and other response variables

Response	Correlation Coefficient
Fear of reduced market access	0.575750265
Fair treatment	-0.209571285
Happy with the deal	-0.442187404
Choose to opt-out	0.501573985
Choose not to opt-in	0.269201342
Would vote against deal	0.213930227

5. Discussion

The above data suggests several findings. Taken together, the fact that participants drew a distinction about types of data collected but not whether their data was included hints that consumers are behaving as rational actors according to a rational economic model. Participants distinguished between types of data that have specific economic consequences. However, they failed to conclusively communicate an aversion to a greater chance of data collection (from 20% to certainty) when use was held constant. This implies that consumers focus on the *use* of information, rather than being concerned with data collection. It is not that data belonging to an individual is in a database, but rather that an individual can be affected by a third party wielding that database.

If consumers are not directly concerned with data collection, then a valid economic model can only focus on anticipated use. This seems to suggest that highly context-specific models of privacy protection, such as [4], but might fail for more generalized models where individuals simply attempt to protect their personal information. There are still many factors to consider, from certainty and value of use to the multiple dimensions of perception of exploitability.

One such dimension is Wathieu's fear of segmentation [20]. Our experiment asked consumers to consider how their life would change if insurance companies had more information about a segment of the population. Insurance companies are uniquely poised to exploit personal information by competing for low-risk customers. Any consumer who does not have a good reason to believe that he or she will be offered a preferable rate would have ample reason to oppose the use of relevant personal information—or any personal information—since this use could lead to a fragmenting of the market, where the newly-targeted niche will be offered a better deal at the expense of the more average consumer. Such a consumer would see a "privacy externality." This phenomenon bears further exploration in contexts that may have less in common with a more conventional price-discrimination model. If such an externality does exist, where one individual's decision to allow his information to be used affects another who is not given the choice, then there is room for further public policy analysis.

The finding that an opt-out regime appears to be a better vehicle for enabling privacy preferences also stands out as a significant finding. The experimental construct could explain some part of it: much of the opt-in/opt-out literature focuses on individuals answering questions while trying to accomplish some other task. The presence of a default opens the door for a cognitive-laziness model, where actors simply cannot be bothers to check a box, since their attention is on their primary task. Since the experiment was predicated on straightforward answers, we cannot use that assumption. However, cognitive laziness only explains defaults, and we observed a marked trend where the conditions had no effect on participants' decisions to opt-in, but the same conditions that inspired greater privacy concerns also encouraged more people to opt-out. Given the power of these correlations, we argue that privacy concerns are more and better made manifest through opt-out decisions than opt-in decisions.

Finally, we note that our data is not completely straightforward. In particular, we observe what appear to be interaction effects that do not have an easy explanation. In the final category where participants were primed to be wary of how premiums would change when they would not receive benefits but everyone's data would be shared, the means of all four attitude questions were significantly worse than the control, as were the means for most Boolean recoding. We believe that some interaction between those conditions drives a larger privacy concern concurrently with worrying about market access and fair treatment. However, basic linear models were unable to confirm this effect.

6. Conclusion

To understand and model privacy, more information is needed about consumer preferences than, “people want privacy.” We present evidence from an experiment that people do behave somewhat rationally when considering realistic privacy situations. We find that consumers care about data use, rather than being concerned with data collection, and they assign importance to the type of personal information in question. There also is strong evidence that an opt-out regime better captures consumer sentiments than an opt-in regime. Finally, we begin to show how consumer privacy concerns extend beyond their own information collection and extend to the personal impacts of social collection of information in a “privacy externality” effect.

7. REFERENCES

[1] Agre, P.E. and Rotenberg, M. Technology and privacy: the new landscape. MIT Press, 1997.

[2] Aquisti, A and Grossklags, J. Privacy and Rationality in Individual Decision-Making. IEEE Security and Privacy Jan/Feb 2005

[3] Berman, J. and Weitzner, D.J. Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media. Yale Law Journal 104:7. 1995

[4] Chellappa, R.K., " Consumers’ Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security," under submission

[5] Chellappa, R. K., and Sin, R., Personalization versus Privacy: An Empirical Examination of the Online Consumer’s Dilemma. Information Technology and Management, Vol. 6, No. 2-3, 2005

[6] Deighton, J. Frequency Programs in Service Industries. In Handbook of Services Marketing and Management, Teresa Schwartz and Dawn Iacobucci, eds., Sage, 2000.

[7] Earp, J.B, Poindexter, J.C., Baumer, D.L. Modeling privacy values with experimental economics. Proceedings of the ACM workshop on Privacy in the electronic society(WPES), 2004.

[8] European Community. Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31

[9] Google Privacy Policy. http://www.google.com/intl/en/privacy.html Version 07/01/2004

[10] Hann, I.H., Hui, K.L., Lee, T.S. and Png, I.P.L. Online Information Privacy: Measuring the Cost-Benefit Trade-off. Proceedings of the 23rd International Conference on Information Systems, 2002

[11] Huberman, B.A., Adar, E. and Fine, L.R. Valuating Privacy. To appear in IEEE Security and Privacy

[12] Johnson, E.J., Bellman, S., and Lohse, G.L. Defaults, framing and privacy: Why opting in ≠ opting out. Columbia Business School Working Paper (2000).

[13] Johnson, E.J and Goldstein, Daniel. Do Defaults Save Lives? Science 302, 2003

[14] Milne, G.R. and Rohm, A.J. Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives. Journal of Public Policy and Marketing, 19:2, 2000.

[15] Odlyzko, A.M. Privacy, economics, and price discrimination on the Internet. in Economics of Information Security, L. Jean Camp and S. Lewis, eds., Kluwer, 2004.

[16] Regan, P M. Legislating Privacy. North Carolina Press, Chapel Hill NC, 1995.

[17] Shostak, A. and Syverson, P. What Price Privacy (and why identity theft is about neither identity nor theft). in Economics of Information Security, L. Jean Camp and S. Lewis, eds., Kluwer, 2004.

[18] Spiekermann, S., Grossklags, J. and Berendt, B. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior, Proceedings of the 3rd ACM conference on Electronic Commerce, 2001.

[19] Tversky, A., & Kahneman, D.. Judgment under uncertainty: Heuristics and biases. Science, 185, 1974

Wathieu, L. Marketing and the Privacy Concern. Marketing Sciences, forthcoming.