



GLOBAL JOURNAL OF ADVANCED RESEARCH  
(Scholarly Peer Review Publishing System)

# SOLVING THE DATA PRIVACY PARADOX IN THE WORLD OF “BIG DATA”: EXPLORING THE RELATIONSHIP BETWEEN INCENTIVES AND CONSUMER DATA PRIVACY RELUCTANCE

**David J. Fogarty**

Faculty Member, University of Phoenix, Phoenix AZ,  
United States of America

## Abstract

With the coming of “BIG DATA” and the increasing realization by firms as to the value of analyzing their customer data there is a real concern with how these firms can obtain legal consent from their customers to utilize the data. Focusing on the consumer data privacy issues this research explores the relationship between incentives and reducing the reluctance of consumers to allow their personal data to be utilized for commercial purposes. The findings suggest that consumers are willing to give up personal data privacy in exchange for adequate compensation. This research has interesting implications for firms which depend on data analysis and data mining to conduct normal business.

**Keywords:** “BIG DATA”, Data Privacy, Incentives, Personal Data, Consent

## 1. INTRODUCTION

Incentives are accepted in our popular culture in the US as depicted by a recent public service advertisement which shows customers at an artificial bank getting \$500 for opening an account as long as they provide their personal information and liking this to what happens frequently on the internet. Moving over to Asia a wave of concern over personal data in the Octopus stored value cards used by residents for retail purchases and public transportation fares has caused legislators to rethink privacy laws in light of complaints by a community concern group. The group was concerned that personal data in their cards would be misused by the company, retailers from whom they purchase goods, or even schools and workplaces that use cards to track attendance. This movement has been led primarily by strict data privacy measures in the EU which were put in place after WWII to prevent atrocities like the Holocaust from occurring ever again. However, these legacy laws may not have so much relevance in the world of “BIG DATA”. In the world of “BIG DATA” we must prepare to live in a paradox of tightened regulation around data protection and privacy but at the same time free flow of information to be used by business and government to provide better products or services. This research explores a partial solution to this paradox. Part of the fact is solved by the fact that most analysis of the data can be done on a depersonalized basis. However, there are always going to be privacy concerns whenever there is storage and transfer of sensitive private information and therefore this research is important and timely.



## 2. LITERATURE REVIEW AND CASE STUDIES

There is much evidence that people are willing to trade off their personal detail in exchange for incentives. One particular case explored is the growth of online sweepstakes. People began providing their data in exchange for a chance to win a sweepstakes in 1963 via Reader's Digest. Later in 1967 Publishers Clearing House launched its own sweepstakes in order to sell more magazines in its direct mailing campaigns. Two modern companies worth analyzing are Adsalsa and Planet49. Both started off as the same company then due to a disagreement among the founders they split into two separate operating companies. The basic idea is that the people will be willing to fill out personal information including name, address, phone number, age gender etc. in exchange for a chance to win several prizes. The prizes have been well researched including at the minimum level iPads and at a maximum level Audi's and BMWs. Interestingly the maximum prizes which are the cars do not need to be provided in Asia to get sufficient responses to the sweepstakes. The global growth of Planet49 has just been phenomenal. The business started in Germany and then expanded to other countries in Western Europe including Spain, Portugal, Italy and Sweden and now even Asia with Singapore, Korea, Hong Kong and Taiwan. There has been little research to date on incentives leading consumers to provide private information which makes this research particularly important.

GMAIL launched by Google is a more modern example of the willingness of consumers to give up their privacy for incentives in this case being free email. Facebook is also another great example of how people were willing share a great deal of personal information for compensation. For the benefit of efficient communication with friends and family Facebook is granted by subscribers a "non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any intellectual property content (photos, videos, etc) that you post on or in connection with Facebook". What does this suggest? Also consider this one "We share your information with third parties when we believe the sharing is permitted by you, reasonably necessary to offer our services, or when legally required to do so". We believe is an interesting statement the result of which is that many users grant data rights to Facebook either willingly or unknowingly.

Consumer perceptions of the real privacy of their data appear to be mixed. Evidence of this can be found in readers comments every time a "BIG DATA" application article is published in the popular media such as the *New York Times* or the *Economist*. However, retailers and vendors on the internet must pay close attention to this as studies demonstrate trust in terms of data privacy is related to purchase intention and greater customer loyalty (Jahankhani, 2009). This makes a further case as to the importance of conducting research on data privacy and incentives

Facebook advertisers spent over \$1.5 billion a year to get access to this data. Facebook sets up the terms from which you can expect privacy. If you don't agree with the terms then you will not be granted access. Studies demonstrate that the gratifications consumers receive from using Facebook outweigh their perceived threats to privacy (Debatin et al., 2009).

In my research classes students are very active in discussing Facebook and its dangers. Some focus on the fear of a job interview requesting to see their Facebook pages. Others discuss the fact that logging into to Facebook remotely and showing pictures from your vacation can advertise to potential criminals who are embedded in one's network that you are away and they can burglarize your home. However, studies show that most consumers have a false sense of security around the existing privacy features offered by Facebook (Debatin et al., 2009).

Daniel Solove (2007) discusses the privacy is not one-faceted and that people choose which aspects of their lives they want to remain private and which one's should be open to certain people. This discussion he brings forth is in the context of how privacy is usually treated as all-encompassing or ubiquitous meaning if one thing needs to be protected then everything needs to be protected. On the government side people knowingly give up the privacy for protection under the US Patriot Act. People also give up their privacy at their place of work in exchange for employment (Flaherty, 1999, Innis, 1992 Schneier, 2006, Solove, 2006a,b, 2007). Of course there is also an ownership issue associated with using equipment which is owned by the employer but incremental cost of using computing and telecommunication assets



is a minor issue these days especially when many employers will allow employees responsible personal usage of the phone and internet during off duty times at lunch. If this was not occurring in the workplace we would never have the CyberMonday phenomenon.

### 3. METHODOLOGY

203 consumers were sampled for this study. In order to make sure issues regarding data privacy were front and center the consumers were given a pre-exposure to the ACLU website on data privacy and then asked in a brief survey if they would be willing to give up their privacy if they were compensated fairly and significant measures could be taken to protect their information. The link for the ACLU website can be found below:

<http://www.aclu.org/pizza/images/screen.swf>

### 4. RESULTS

From a qualitative perspective of the consumers who did respond positively to the willingness to share private information in exchange for compensation the majority felt that their data was being used already by firms without compensation so they might as well get some form of compensation for the use of this data. One consumer indicated he would sell his personal information (excluding his national identity number) since he felt that if companies wanted it bad enough they would be able to obtain it anyway without compensation in the absence of laws to prevent such a theft. Another positive responder indicated that since we put our personal information online almost every day, through Billpay, FaceBook, PayPal or other similar sites we have already made it easy enough for companies to delve into our personal lives and therefore she didn't think that anything that is put on the internet is private anymore. One specific consumer said the compensation required would depend on the size of the firm and the type of business they were engaged in and that the said firm would not be able to use his personal information if the specific compensation requirements were not being met. Another consumer indicated that he would sell his personal information since he felt that companies were doing well despite the fact that there was still high unemployment in certain countries. Therefore, these companies have a societal obligation to give compensation to individuals for the use of personal data. Many positive responders also indicated they would need to do the proper due diligence on a firm before the transaction can take place. Finally, one consumer indicated that any company which takes his personal information for compensation would need to sign an agreement stating clear liability and agreeing to compensation if his personal privacy is breached in any way.

From a qualitative perspective of the consumers who didn't respond positively to the survey the key reason was that they indicated that they needed the assurance that their data was truly being protected. Or else it depended on the type of data which was being collected usually the less personal was considered acceptable to sell. Many consumers were skeptical that any firms would pay given the fact that they have access to the data already. Some consumers had a true belief that their data should not be shared under any circumstances yet realized in reality their data was being used regardless of their individual opinions. Some would want to talk it over with their significant others as they felt this was a shared decision since it would affect both parties. Some expressed that they would certainly take money for their personal data but wouldn't give out any additional information than the data they are already giving away for free. Some consumers felt that they would first want to know more about the business entity collecting the data before they could release their data for compensation. Many questioned the ability of firms to ever be able to predict an individual's privacy. People feel strongly about this issue. Few consumers would outright share all their personal information without exceptions for adequate compensation. Some have stated that personal data is categorized into many different types and there were certain types which they would accept compensation and certain types in which they wouldn't. Some have said that private being a relative term, that individuals have to determine what they are willing to share versus not. For example, some people may not want anyone to know their size in clothing whereas some do not care. One consumer stated they would not sell any of their medical information to a vendor unless it was being used in a study to cure some type of



disease. Another consumer indicated that they have no problem giving up their privacy if the information would be used to catch terrorists.

There were definite trends toward privacy at all reward levels if consumers have ever experienced any personal issues with identity theft in the past. This experience seems like a switch in which people who have been through this become extremely conservative over who has access to their personal data. This is an interesting finding for companies who may need to convert these people in the future. Not having them participate in the data economy could be a real issue from both a research and commercial perspective.

Almost all had some opinions on this and it seemed like they were thinking about this issue previously.

From a quantitative perspective the Pearson Chi-Squared Goodness of Fit was used to evaluate the main effect of whether consumers were more likely to allow their personal information to be used if they were adequately compensated. These were the appropriate tests considering the data collected was at the nominal level of measurement.

Of the 203 consumers the overall percentage from the counts of whether they would give up their private data if properly compensated is demonstrated (Table 1) below. It is interesting that we see that a larger percentage of consumers were willing to give up privacy in exchange for compensation. A Chi-square goodness of fit test shows that we can reject the null hypothesis that there is no relationship between consumers' willingness to give up data privacy in exchange for adequate compensation.

**Table 1.** Overall Percentage of Consumers Willing to Give up Personal Data Privacy in Exchange for Incentives

Observed % Willing to Give up Personal Data Privacy if Properly Compensated	Observed % Not Willing to Give up Personal Data Privacy if Properly Compensated
57	43

Chi-Square Goodness of Fit Test = 4.131 d.f.=1 p. < .05

Next, we examine if the number of consumers willing to give up personal data privacy in exchange for adequate compensation are related to gender using the chi-square test of independence. The results of this analysis shown below:

**Table 2.** Results of Pearson's Chi Square Test of Association Between "Gender" and "Incentive"

p value: 0.422 <sup>1</sup>

Pearson's Chi Square statistic: 0.644

Degrees of Freedom (df): 1

	Incentive
--	-----------

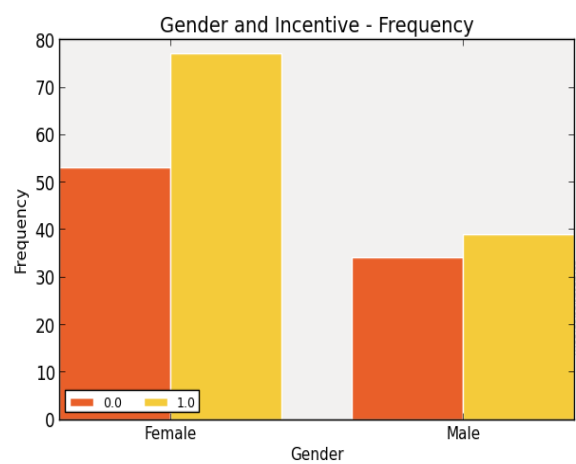
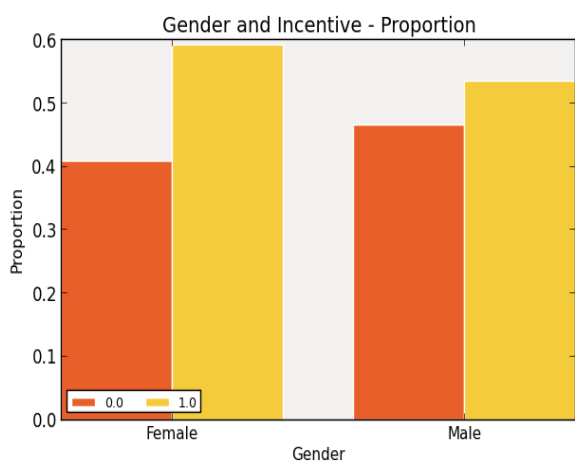


		0.0		1.0		TOTAL	
		Obs	Exp	Obs	Exp	Obs	Exp
Gender	Female	53	55.7	77	74.3	130	130.0
	Male	34	31.3	39	41.7	73	73.0
	TOTAL	87	87.0	116	116.0	203	203.0

Minimum expected cell count: 31.286

% cells with expected count < 5: 0.0

<sup>1</sup> If p is small, e.g. less than 0.01, or 0.001, you can assume the result is statistically significant i.e. there is a relationship.



**Figures 1 and 2.** Frequencies and Proportions of Gender and Incentives

The results demonstrate that we fail to reject the null hypothesis that gender is related to the number of consumers willing to give up personal data privacy in exchange for adequate compensation.

## 5. CONCLUSIONS

This study shows evidence of the fact that incentives are related to whether or not consumers are willing to give up their personal data privacy. These findings hold true irrespective of gender. The findings from this study should be useful for all companies engaging in electronic commerce and/or those which use customer data as a core part of their business operations or for marketing purposes. This is especially true given the current legal and regulatory environment focused on putting rules in place to protect consumer’s privacy. Therefore, the only unrestricted way in the future to use consumer data may be to get consumers to opt-in to be able to use their data.

One of the limitations of this study is the small sample size and limited sample frame. Therefore, further research in this area is necessary to insure that the findings hold true in subsequent tests and also using a larger variety of incentives.

Another area of further research is educating consumers that in reality their personal data can be housed securely and it’s their non-personalized data which is only necessary for detailed statistical analysis. Many consumers don’t realize this fact and believe it is the personal data which is most useful for data mining purposes when in reality it is really the



correlations between the data which are important. Implementing any insights or algorithms created from the analysis then would require personalized information. However, this could be conducted in a secure production environment.

Another interesting topic for further exploration is in the ability of consumers to provide personal information in exchange for content rather than financial rewards. One could imagine useful content like healthcare information could be very valuable to consumers in the future especially with aging baby-boomer populations across the globe. This would be especially important in the US with strict HIPAA laws governing how healthcare data can be used. Having consumers opt-in would provide the much needed flexibility. In addition, content bringing health and wellness advice and information on how to navigate the healthcare system in a particular country could be tested. Moreover, content on financial services such as advice on retirement or personal finance could also be tested in exchange for personal information. In summary, this research has shed the light on an important option for firms to be able to deal in both the present and future with the paradox of the growth of “BIG DATA” and expanding data privacy regulations.

## 6. REFERENCES

- [1] ACLU Data Privacy Website: <http://www.aclu.org/pizza/images/screen.swf>
- [2] Debatin, B., Horn, A., K., Hughes, B., N., Lovejoy, J., B. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences *Journal of Computer-Mediated Communication*. vol. 15 pp. 83–108.
- [3] Flaherty, D., H. (1999) *Visions of Privacy: Past, Present, and Future*, in *Visions of Privacy: Policy Choices for the Digital Age* 19, 31 (Colin J. Bennett & Rebecca Grant eds.).
- [4] Inness, J., C. (1992), *Privacy, Intimacy, and Isolation*, Oxford University Press.
- [5] Jahankhani, H. (2009). The Behaviour and Perceptions of On-Line Consumers: Risk, Risk Perception and Trust. *International Journal of Information Science and Management*, Vol. 7, No. 1. pp. 24-36.
- [6] Schneier, B., Commentary, *The Eternal Value of Privacy*, *Wired*, May 18, 2006, <http://www.wired.com/news/columns/1,70886-0.html>.
- [7] Solove, D., (2006). *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477.
- [8] Solove, D., (2002). *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1095–99.
- [9] Solove, D., (2007) “I’ve Got Nothing to Hide” and Other Misunderstandings of Privacy. *San Diego Law Review*, vol. 44 pp. 745.