THE ECONOMICS OF PRIVACY

Privacy: People, Policy and Technology

Justin Zhan and Vaidyanathan Rajamani

Carnegie Mellon University
{justinzh,vrajaman}@andrew.cmu.edu

Abstract

Privacy of personal information is an area of growing concern and importance. The heart of the conflict is between commercial value and respect for an individual's right to privacy. This tradeoff is of economic value and the issue of privacy is an economic problem that justifies the emergence of the economics of privacy as an important discipline, combining efforts of regulation, technology, and business efficiency. In this survey paper, we look into work done by eminent researchers on the economic aspects of privacy and privacy's relationship with people, technology, and regulation.

1. Introduction

The revolution in the ability to capture, store and process information, enabled by advancement in technology and cost efficiency, has spawned a trend among organizations to chase more data about individuals in an effort to better know their customers and serve them appropriately. Also, customers have come to expect personalized services and simple access to information systems. The move from mass marketing to targeted one-on-one marketing certainly warrants increased sharing of personal information. This also raises numerous concerns and questions for consumers, businesses, and policy-makers. Researchers from different backgrounds have put forward their opinions and possible solutions to the nebulous issues of privacy. The following is a digest of some of the most important work done in this area.

2. Privacy and People

George Stigler defines privacy as the concealment of useful information assuming an economic value in transactions [Stigler 1980]. Privacy involves the protection or revelation of information of commercial value, like purchasing power, and noncommercial value, like age or weight. It has been found that people tend to reveal information that will help the other party provide the desired benefits to the person revealing (e.g.: the kind of books one prefers to read) and conceal information that would be counterproductive (e.g.: their maximum willingness to pay). [Posner, 1978,

Posner, 1981 and Varian, 1996] talk about the types of information people like and dislike to reveal.

The way people do business has been changed by advancement in information technology. We are in an era of information overload. Forced by consumer demands and market competition, businesses feel the need to collect more and more information. This helps them achieve efficiency by better understanding the needs of existing and prospective consumers and effectively assigning services and products to cater to their requirements in a cost and time-efficient way. The incentive driving businesses to collect more personal information is that it enables them to implement price discrimination based on consumer willingness to spend and thus generate consumer surplus [Odlyzko, 2003]. The need of the people for personalization of services and the need of businesses for efficiency has warranted and led to increased exchange of information between the private and public space than ever before.

On the other hand, the concern for privacy is a primary reason for people not to trade online who are otherwise willing to do so if their privacy is assured. Privacy, as an economic problem, saw its attention and importance from this aspect by the work of [Posner 1978, Posner, 1981], and [Stigler, 1980].

In this context, information is seen as an economic good. There is an element of uncertainty associated with the value of information as the importance of the information being exchanged is valued differently by different people. Though people value the protection of the privacy of their information, their attitudes and behaviors have been found to be paradoxical. People exhibit contradicting behavior when it comes to "willingness to pay" to protect information and "willingness to accept" compensation for revealing information. [Grossklags, 2007] conducted an experiment on the hypothesis that people care deeply about their privacy, except in practice, and found that, on average, there exists a preference for "willingness to accept" over "willing to protect". Based on the science of behavioral economics, [Acquisti, 2004] seeks to explain that the tendency for immediate gratification and enjoyment, as opposed to the expected rational thought process, tends to govern behavior when it comes to revealing personal information. This behavior applies even in the case of people who value privacy and understand the risk involved in such a transaction, which indicates that ignorance of the risk involved is not a cause for this behavior.

People expect personalization of their transaction experience and at the same time show concern in doing business online for privacy reasons. [Taylor, 2005] explores the incentives of information acquisition by firms to understand the conditions under which these firms discriminate the amount of information they collect in a competitive market with homogenous products considering its relevance to the profit and welfare of its business. The work also compares its conclusion with the work of [Hermalin and Katz, 2004] which is about the effect of privacy on efficiency in a marketplace and is considered complementary to [Taylor, 2005].

According to [Hirshleifer,1980, Stigler, 1980, and Posner,1981], the forces of competition will ensure an equilibrium of marginal cost of information acquisition and the marginal cost of service or products and hence discounts the risk of privacy in such a scenario ultimately resulting in no social value for information. [Taylor, 2004] claims that when information acquisition is not observable, a firm has incentives for information acquisition, particularly negative information about individuals, and the competitive pressure on a firm doing this will lead to a divergence between the marginal private benefit of information acquisition and the marginal social benefit and shifting away from equilibrium. The incentives of the firms to collect the information they need depends on the technology they have.

3. Privacy and Technology

While discussion on the issue of privacy have been around for a while, growth in information technology has taken it to a level where it is a significant problem of concern today. With increasing spread of Internet adoption, increases in storage and data mining capability have given firms the ability to gather and process huge amounts of information to derive customer information. This would otherwise be difficult and expensive if done manually. This information is of great value to businesses because by studying the buying patterns and willingness of the customers to pay they can implement price discrimination. Price discrimination generates consumer surplus and economic efficiency. Economic incentives to price discrimination has been discussed in [Odlyzko, 2003]. These economic incentives promote the development of new technologies for privacy violation.

While economic incentives is the reason behind the adoption of technologies for undermining privacy, the lack of the same economic incentives for consumers stalls the adoption of privacy enhancing technologies. The economic and legal elements of privacy need to be incorporated in the design of privacy enhancing technologies so that the stakeholders have the right incentive and are governed by regulation in their operations [Acquisti, 2004]. Privacy technologies can be privacy preventive, avoiding, and detecting technologies, the discussion is covered in detail by [Jiang, Hong, and Landay, 2002].

Let us briefly look at the basics of information tracking on the Internet. To map the various transactions of an individual and build a profile, the HTTP protocol enables the server to deposit a cookie in the hard drive of the user's system. Cookies are unique identifiers about a transaction. They reside in the user's system after a transaction session has ended. During the next session with the same computer, the web server reads the cookie and identifies the user.

Encryption technology has seen considerable adoption and gives the parties involved control over access to information. Privacy is seen as the right of an

individual over personal information, and, as explained in the *Privacy and People* section, rationality does not always guide decision making in this area.
The difference encryption as made is that it allows consumers to get paid by the buyer for revealing information that was otherwise freely available to them [Noam, 1997]. We could extend this to say that even privacy-enhancing technology could provide bargaining power to the consumer to reveal information over which the consumer has increased control. However, according to [Varian and Acquisti, 2004], such anonymity technologies are not found to be beneficial to consumer welfare. On the other hand, cookie technology is considered to have a social benefit as it allows the firm to offer personalized services to the consumer [Acquisti and Varian, 2001]

Privacy is a major obstacle for the success of e-commerce. Emerging ways of communication, like wired-mobile convergence, raises questions of privacy protection. The need for privacy protection, incidents of identity thefts, and the associated economic concerns are driving the adoption of privacy enhancing technologies, such as identity management systems that give user the control on the type and level of information they can reveal. By using pseudonyms and anonymity technologies, privacy of an individual is protected. The importance for such technologies is elaborated by [Hansen, 2004].

Despite the ability of firms to track down and build profiles of the users and consumers from isolated transactions, the adoption of privacy preserving technology is not quite encouraging. Consumers' lack of foresight of the possible uses of their information involved in using anonymity technology explain the failure of large scale adoption of privacy enhancing technology. The problem is that it is difficult to quantify the cost, benefits, and risks involved in information disclosure as most of the evaluation boils down to a subjective nature. Also, the unpredictability of the consequences of information asymmetry is a big challenge in evaluating the economic impact of information disclosure and in developing a proper mechanism of incentives for the stakeholders. [Acquisti, 2002] explains, with a simple mathematical method, the cause of the failure of privacy enhancing technologies from an economic perspective. The work also explains the factors that influence an individual in using privacy enhancing technology and states that the bigger problem is that the highly complex networked world makes marketing and adoption of privacy technologies difficult compared to the actual ability of these technologies to provide privacy protection.

4. Privacy and Policy

In the previous two sections we saw privacy from the perspectives of people and technology, but the issue of privacy is also one of who should own and control the flow of information. This takes us to privacy from the point of view of regulatory controls. From the work of [Kahn et al, 2000] we can understand how it is not easy to build flexibility in transaction contracts. The model explains the costs and benefits to the stakeholders from the assignment of rights and how to create efficiency in

transactions under the considerations of constraints in contract flexibility and Coasian logic.

Privacy policies play a crucial role in allowing a firm to collect and use sensitive customer information. There are varying degrees of flexibility in the adoption of privacy policies. For example, in the US, the Gramm-Leach-Bliley Act of 1999 prohibits financial institutions from disclosing customer information to a third party to be used in telemarketing or direct mail marketing, but the regulation also requires that the financial institution share customer information with public credit bureaus.

We can understand that optimal design of privacy policies acceptable to the stakeholders and promoting efficiency is a welcome solution. Often, consumers deal with multiple vendors at the same time. The work of [Calzolari and Pavan, 2004] addresses the question of ensuring optimal privacy and incentives in a sequential contracting environment by studying the factors determining disclosure and their impact on individual and collective welfare.

The current privacy policy provides three provisions. The opt-out provision requires that firms give customer an option to refuse permission to share information with a third party. An opt-in, on the other hand, allows the use of personal information within the firm but requires the consent of consumer to sign up for this before disclosing their information to a third party. Finally, there is the anonymity aspect of the privacy policy by which the firm would not be able to use the information for any decision making or planning. The work of [Bouckaert and Degryse, 2006] provides an economic analysis of these privacy policy provisions to understand their implications on the abilities of firms to collect and use customer information in regard to pricing strategies and other decisions. Considering the cost of adopting a privacy policy [Litan, 1999], in his analysis of the cost and benefits of privacy regulations, says the cost is marginal compared to the greater benefits of providing privacy assurance to customers and gaining consumer trust.

Information privacy is seen as a major problem and its growing importance warrants the formulation of models for privacy to address the issues. This saw the evolution of privacy regulations in the United States and in Europe. Relevance and implications to the privacy to consumers and firms are discussed by [Zwick and Dholakia, 1999] while exploring the definitions of privacy and the evolution of these models based on the *EU Directive of Privacy Protection* and the *Federal Trade Commission 'Online Privacy' Report to Congress*.

Many firms adopt the Fair Information Practices (FIP) of the Federal Trade Commission that stipulates guidelines [FTC Report, 2004] on the type and amount of data to be collected. The effect of the FIP on the risk for consumers is assessed by [Culnan and Bies, 2003]. Privacy assurance thus is expected to assist people in evaluating the risk involved and encourage people to go online and disclose information by virtue of trust. Work along these lines was done by [Milne and Culnan, 2004]. To assess the actual value consumers place in privacy assurance practices [Hui, Teo and Lee, 2006] conducted a field experiment. Besides analyzing

customer trust in privacy assurance the work also evaluates the behavior of consumers towards information disclosure under the conditions of monetary incentives and requests for information.

The need for a remedial course of action for privacy concerns is crucial. The organization, firm, or market players are expected to play a responsible role by formulating privacy policies in the interest of the public. [Merold, 1997] stresses the importance for an organization to develop a framework for protecting the privacy of its users by working with its partners and vendors to identify the weaknesses of the system and challenges posed by technological trends and the impact on existing policy and enforce it effectively with consumer education. This kind of self-regulation promotes the value of information and privacy in society. On the other hand, the passivity of organizations in this regard will affect their ability to collect useful information by forcing the emergence of legislation or by the prevalent consumer apprehension for information disclosure.

Though traditionally, self-regulation of the industry has produced policies and best practices that served as the basis for drafting federal regulations, doubts and concerns on the adequacy of self-regulation to effectively address privacy issues prevail. [Mulligan and Goldman, 1997] examine the need and limitations of self-regulation and suggest a collaborative or an interactive model involving stakeholders of privacy in solving privacy problems. The limitations are the lack of oversight, enforcement, and the absence of legal recourse of affected individuals. [Mulligan and Goldman, 1997] are of the opinion that the promise of privacy assurance can be realized only through the concerted efforts of policy makers, the community, and the communications and computer industries in building a framework that depends upon privacy policies and privacy enhancing technologies. A collaborative model involving the Internet Privacy Working Group (IPWG), World Wide Web Consortium (W3C) and other stakeholders representing public and private interest currently exists for addressing privacy issues.

With some skepticism in the issue of privacy, [Noam, 1997] suggests that while the market alone cannot provide a solution to privacy problems, it can be engaged in seeking a solution. It seeks to convey that privacy problems arise over the right of ownership and use of information by those involved in a transaction. It is an area of intricate problems and it might not be effective to see privacy as a larger problem of an individual and state or individual and a firm. An interactive mechanism would help in protecting privacy in a conducive environment.

Much focus has been given to the importance of protecting privacy, but this does not discount the value of information sharing. Responsible sharing of personal information lays a stable foundation for a productive and successful economy. It enhances customer satisfaction, generates surplus, and efficiency for the businesses and reduces fraudulent practices. Discussing the importance of responsible information sharing and its social benefits, [Staten and Cate, 2003] state that a regulation or legislation designed to protect privacy should not be counter-productive to the benefits of information sharing, but rather should balance out its effect on the

protection of privacy and the good of information sharing. The timing of this study assumes importance in the light of legislations that were being drafted to adopt stringent information sharing practices with third parties through the opt-in system rather than the opt-out method.

Along the same lines, financial institutions and their customers benefit from sharing information. Customers save about 17 billion USD and 320 million hours annually from sharing of information by financial institutions with their affiliates and third parties [Ernst & Young, 2000]. Another similar report by [Turner, 2001] discusses the impact of restrictions on the free flow of information through online shopping.

5. Conclusion

In the competitive market we live in today, personal information is of commercial value. It is needed to generate consumer surplus, customer satisfaction, business efficiency, and due diligence in decision-making. The issue is who has the right and ownership over the information to use to ones advantage.

Advancement in information and communication technology has made it difficult to evaluate the risks of privacy intrusions. With no regulations effectively controlling privacy and misaligned incentives, there could be competition to develop both privacy enhancing and privacy invasive technologies to serve the interest of each player in privacy. We may conclude that effective privacy rights policies can provide a solution to this race for contradicting technologies. Some might argue for the need for increased consumer education on Internet trade.

Efforts are being made by academics, scientists, businesses, task forces, and government agencies to catch pace with the issue of information privacy and find an agreeable solution. All these efforts cannot be done in isolation of each other and hope to be effective.

Any solution to protect privacy should not be counterproductive to the benefits of information sharing but rather should balance out its effect on the protection of privacy and the good of information sharing. The need for a remedial course of action for privacy concerns is crucial. Businesses, consumers, governments, developers, policy makers, and other market players are expected to play a responsible role by developing a combined framework involving all aspects of privacy concerns in the best interest of all those involved.

6. Reference

1. A. Acquisti and H. Varian. Conditioning prices on purchase history. Forthcoming, Marketing Science, 2005. (Technical report, University of California, Berkeley, 2001.)

A. Acquisti. Protecting Privacy with Economics: Economic Incentives for Preventive Technologies in Ubiquitous
2. Computing Environments. Workshop on Socially-informed Design of Privacy-enhancing Solutions, 4th International Conference on Ubiquitous Computing (UBICOMP 02), Goteborg, Sweden, September 2002.
3. A. Acquisti. Privacy in Electronic Commerce and the Economics of Immediate Gratification. Proceedings of ACM Electronic Commerce Conference (EC 04). New York, NY: ACM Press, 21-29, 2004
4. A. Acquisti. Security of Personal Information and Privacy: Technological Solutions and Economic Incentives. In J. Camp and R. Lewis (eds), The Economics of Information Security, Kluwer, 2004.

G. Calzolari & A. Pavan. "On the Optimality of Privacy in Sequential Contracting," Discussion Papers 1394, Northwestern University, 2004
5. M. Culnan and J. Bies. Consumer Privacy: Balancing Economic and Justice Considerations, Journal of Social Issues (59:2), 2003, pp.323-342.
6. Ernst & Young LLP. Customer Benefits from Current Information Sharing by Financial Services Companies, December 2000.
7. K. Hui, H. Teo, and T. Lee, "The Value of Privacy Assurance: An Exploratory Field Experiment," MIS Quarterly, 2006.
8. M. Hansen, P. Berlich, J. Camenisch, S. Clauß, A. Pfitzmann and M. Waidner. Privacy-enhancing identity management, Information Security Technical Report, Pages 35-44, Volume 9, Issue 1, January-March 2004.
9. J. Hirshleifer. 1980, Privacy, Its origin, Function, and Future, Journal of Legal Studies, 9, 649–66, 1980.
10. X. Jiang, J. Hong, and J. Landay. Approximate Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing. In Proceedings of Ubicomp 2002. Goteborg, Sweden 2002. pp. 176-193.
11. C. Kahn, J. McAndrews, and W. Roberds. A Theory of Transactions Privacy. Federal Reserve Bank of Atlanta, Working Paper 2000-22, November 2000.
12. R. Litan. Balancing Costs And Benefits Of New Privacy Mandates (May 1999). AEI-Brookings Working Paper 99-03. Available at SSRN: http://ssrn.com/abstract=179074.
13. N. Mundorf, D. Zwick, and N. Dholakia. Die Web-Präsenz führender deutscher Industrieunternehmen (Presence on the Web of Leading German Industrial Enterprises). In Fritz, W. (Ed.). Internet Marketing. Schaeffer-Poeschel Verlag, 81-106, 1999.
14. D. Mulligan and J. Goldman. The Limits and the Necessity of Self-Regulation: The Case for Both. U.S. Dept. of Commerce, Privacy and Self-Regulation in the Information Age, 1997.
15. R. Merold. The Necessary Elements Of Self-Regulatory Privacy Regimes And The Role Of Consumer Education In A Self-Regulatory Privacy Regime, U.S. Dept. of Commerce, Privacy and Self-Regulation in the Information Age, 1997.
16. G. Milne and M. Culnan. Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices, Journal of Interactive Marketing (18:3), pp. 15-29, summer 2004.
17. E. Noam. Privacy and Self-Regulation: Markets for Electronic Privacy. In U.S. Dept. of Commerce, Privacy and Self-Regulation in the Information Age, 1997.
18. A. Odlyzko. Privacy, economics, and price discrimination on the internet. In ACM Fifth International Conference on Electronic Commerce, 2003.
19. R. Posner. "Privacy, Secrecy, and Reputation". University of Chicago - George G. Stigler Center for Study of Economy and State 4, Chicago - Center for Study of Economy and State, 1978.
20. R. Posner. The economics of privacy. American Economic Review, 71 (2): 405-409, 1981.
21.G. Stigler. An Introduction to Privacy in Economics and Politics, Journal of Legal Studies, 9, 623–44, 1980.
22. C. Taylor. Consumer Privacy and the Market for Customer Information, RAND 35, 631–51, 2004.
23. M. Turner. The Impact of Data Restrictions on Consumer Distance Shopping. Information Services Executive Council, 2001.
24. H. Varian. Economic Aspects of Personal Privacy. In U.S. Dept. of Commerce, Privacy and Self-Regulation in the Information Age, 1996.
25. D. Zwick and N. Dholaki, Models of Privacy in the Digital Age: Implications for Marketing and E-Commerce, 1999.
26.J. Grossklags. Experimental Economics and Experimental Computer Science: A Survey. In Workshop on Experimental Computer Science, ACM Federated Computer Research Conference, San Diego, CA, June 13-14, 2007. ISBN: 978-1-59593-7