# Price Discrimination, Privacy Technologies, and User Acceptance

**Alessandro Acquisti**
H. John Heinz III School of Public Policy and Management
Carnegie Mellon University
acquisti@andrew.cmu.edu

**ABSTRACT**
We discuss the relations between welfare enhancing price discrimination and privacy enhancing technologies, and the possible drivers of consumers' and merchants' acceptance of those technologies.

**Author Keywords**
Privacy, Price Discrimination, Economics of Privacy, PET, Position Paper.

## PRICE DISCRIMINATION AND ECONOMIC WELFARE

Price discrimination (or differential pricing) refers to the sale of the same commodity or service at different prices to different consumers. In its first degree, prices are based on individual preferences; in its second degree, customers self-select into buying different versions or quantities of the good; in its third degree, differential prices are assigned to different consumer segments based on some observable group characteristics.

Price discrimination is regarded favorably by economists, since it can be welfare enhancing (see, e.g., [13], and, in the context of privacy research, [6] and [11]). Aggregate welfare is enhanced by price discrimination, for instance, when a good would not have been sold unless its producer could target a segment of consumers willing to pay high prices for it. Price discrimination can also increase the welfare of consumers with lower evaluations, who otherwise may not have been offered the good at prices matching their willingness to pay. In addition, as recently hinted by [12], customers' reaction to price discrimination is not always adversarial - consumers judge its fairness depending on the degree of price discrimination (the first being the least liked, the second one being the most accepted), and the proposed rationale for its implementation.

Since price discrimination often relies on consumer identification, it may appear incompatible with privacy protection. This, in turn, would imply that the adoption of privacy enhancing technologies would come at the cost of the welfare enhancements that price discriminative strategies can otherwise provide. In fact, [11] implies that the current privacy debate is fuelled by the fight between consumers and merchants around the use personal information for price discrimination.

In reality, whether privacy enhancing technologies can or cannot be compatible with price discriminative strategies depend on what type of information they shield, and therefore on the scope of their privacy protection. In fact, we show below that the mingling of different types of privacy technologies and different degrees of price discrimination can lead to outcomes in which certain consumer data is actually protected, while welfare is enhanced through differential pricing.

## PRIVACY AND ECONOMIC WELFARE

Intended broadly, privacy is affected by differential pricing strategies, as they depend on merchants knowing, recognizing, and making use of individual consumers' data. However, previous works by [2] (based on [1]), [4] (based on [3]), [9], and [8], have hinted at using privacy technologies in a way that they protect certain types of consumer information but allow other individual data to be exchanged.[1]

In the rest of this paper we extend these analyses by discussing the relation between specific degrees of price discrimination and specific privacy technologies.

## PRICE DISCRIMINATION AND PRIVACY

We need to differentiate between privacy enhancing technologies that aim at anonymity and those that aim at pseudonymity. In *anonymous* technologies, any transaction (a payment, an email, an `http` request) from a certain agent is not linkable by an adversary to other transactions by the same agent, and is not traceable to her "real" identity either. In *pseudonymous* technologies, various transactions by the same agent are all linkable to the same pseudonyms identity, although they are still not traceable to her actual identity.

[1]Specifically, [4] and [2] discuss the economic implications of separating "online" and "offline" consumer information through anonymizing technologies; later, [9] and [8] introduce a number of additional technologies - such as an anonymous authentication protocol and a ring signature protocol - that can also implement that separation.

### First degree

First degree price discrimination takes place when differential prices are targeted to individual consumers. This strategy depends on estimating individual reservation prices more than recognizing actual individual identities.

Reservation prices depend on consumers' preferences and tastes, and are predictable - for instance - from observation of consumers' behavior or purchase histories. This information can be linked to individual pseudonymous, or "online"[2] identities [2]. It may even be traced to persistent identifiers (such as an email address used repeatedly to login to an account with a merchant; or a loyalty card used for multiple purchases from a chain of super markets). But such identifiers can be pseudonymous: while, logistically, a buyer's identity is often revealed in electronic transactions,[3] there is no theoretical requirement for information useful to link an agent's purchases to also be traceable to data that will identify her actual identity in another context - such as her real name, her address, her credit card number, and so on: what we define as her "offline" identity.

The separation of offline and online identities can avoid the consumer additional and possibly more serious costs than adverse price discrimination: credit frauds and identity thefts, discrimination by other entities and in forms other than price, or the creation of a personal digital dossier, shared by third parties on which the consumer has no control.

First, such separation can be enforced through pseudonymous payment technologies in which individual transactions by the same subject are linkable to each other through persistent pseudonymous, but not traceable back to the offline identity of the purchaser. An example of such technologies is the anonymous credit card protocol by [10]. The linkages between the transactions allow the merchant to recognize the consumer and offer targeted services and prices, while the offline identity is never revealed to the merchant.[4]

Second, consumer tracking can also be enforced through *anonymous* payment technologies, even though in principle such technologies make transactions both untraceable to the originating identity and unlinkable to each other. An example of such technologies are ecash payment systems based on [7]. In principle, this anonymous payment system, when used in the context of other anonymizing strategies (for example, in an ecommerce scenario, anonymous browsing that shields the consumers' IP address), would not allow a merchant to track that consumer's purchases over time. However, anonymous payment technologies can be made pseudonymous whenever (by design or oversight) the buyer provides information that allows the seller to track her transactions. For instance, using persistent email addresses, online accounts, or cookies in combination with anonymous technologies may shield the real identity of the buyer, while allowing repeated interactions with the seller.

[2]Although our arguments do not only apply to Internet commerce, the technology for consumer tracking - and certain forms of differential pricing - has improved particularly in the context of online transactions.

[3]As noted in [2], traditional payment systems naturally combine different types of consumer's information: email accounts are gathered together with the credit cards used to purchase from online stores; brick and mortar loyalty cards are combined with the personal information the consumer provided when signing up for the card.

[4]Given enough complementary information, traffic and trails analysis often can allow an organized and determined adversary to break pseudonymous and anonymous shields and re-identify the actual identity of the buyer. A realistic goal of such protective technologies is simply to make such attacks not cost effective.

### Second degree

Second degree price discrimination implies that customers willingly choose to pay differential prices for different versions or quantities of a good or service. This form of differential pricing therefore does not rely on individual information or on any form of traceability across different transactions or identities to be enforced. It can be implemented even when customers adopt untraceable, unlinkable anonymous payment strategies that shield any personal information (including online information, such as email accounts or IP addresses).

Price discrimination of this form is compatible with anonymous transactions - although the consumer's choice and selection may provide information that could be used for her re-identification.

### Third degree

In its third degree, differential prices are assigned to different consumer segments based on some observable group characteristics. The combination of privacy technologies and prices targeted to customer segments has been discussed by [9], who suggested the use of ring signature protocols for anonymous purchases. However, even the combination of existing anonymous payments protocols and anonymous credentials (that can prove the ownership of certain group attributes, such as age, employment status, and so on: see [5]) meets the requirements for this form of price discrimination. The anonymous payment protocol makes the transaction not traceable to the actual identity of the consumer, while the anonymous credentials allow her and the merchant to converge on a price set for a particular segment of the consumer population.

## CONSUMERS' AND MERCHANTS' ACCEPTANCE

Established anonymous payment technologies are compatible with various forms of differential pricing. The ensuing combination is a desirable middle path whenever unlinkable transactions would end up decreasing social welfare or traceable transactions would expose consumers to potential costs by revealing their identities.

For consumers, the advantages of adopting privacy technologies that allow for some individual tracking lie in the combination of the protection of sensitive information and the ability to receive personalized and targeted services (as well as, possibly, lower prices for low-evaluation customers). The disadvantages lie, for high value customers, in adverse price discrimination; and, for all customers, in the risk that the

combined study of various data trails could allow an adversary to trace back a purchase to the actual identity of the purchaser.

For merchants, the combination of privacy enhancing technologies and price discrimination strategies could permit the targeting of privacy sensitive consumers, without the loss of the ability to implement creative pricing and marketing strategies.

The fight between privacy technologies and tracking technologies that [11] imagines is really an interplay between the acceptance of specific types of privacy technologies and specific forms of personalization and price discrimination, with their varying welfare enhancing properties.

## REFERENCES


1. A. Acquisti. Privacy and security of personal information: Economic incentives and technological solutions. In *Workshop on Economics and Information Security (WEIS '02)*, 2002.

2. A. Acquisti. Privacy and security of personal information: Economic incentives and technological solutions. In J. Camp and S. Lewis, editors, *The Economics of Information Security*, 2004.

3. A. Acquisti and H. R. Varian. Conditioning prices on purchase history, 2001. Presented at the European Economic Association Conference, Venice, IT, August 2002.

4. A. Acquisti and H. R. Varian. Conditioning prices on purchase history. *Marketing Science*, 24(3):1–15, 2005.

5. S. Brands. *Rethinking Public Key Infrastructure and Digital Certificates - Building in Privacy*. MIT Press, Cambridge, MA, 2000.

6. G. Calzolari and A. Pavan. Optimal design of privacy policies. Technical report, Gremaq, University of Toulouse, 2001.

7. D. Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology (CRYPTO '82)*, pages 199–203. Plenum Press, 1983.

8. P. Das Chowdhury. *Anonymity and Trust in the Electronic World*. PhD thesis, University of Hertfordshire, 2005.

9. P. Das Chowdhury, B. Christianson, and J. Malcolm. Privacy systems with incentives, 2004. Mimeo, University of Hertfordshire.

10. S. Low, N. F. Maxemchuk, and S. Paul. Anonymous credit cards. In *2nd ACM Conference on Computer and Communications Security*, pages 108–117, 1994.

11. A. Odlyzko. Privacy, economics, and price discrimination on the Internet. In *Fifth International Conference on Electronic Commerce*, pages 355–366. ACM, 2003.

12. S. Spiekermann. Individual price discrimination an impossibility?, 2006. Mimeo, University of Berlin.

13. H. R. Varian. Price discrimination and social welfare. *American Economic Review*, 75(4):870–875, 1985.