

5

Personal Information: A New Currency of Exchange

Nicholas A. Lassow and Jamie Ourada

Introduction

Like any valuable thing, privacy has a price, and in the modern capitalist society there is no shortage of people who are willing to trade in the market of personal information. In some cases people have no choice in what kind of record is kept, but there just as many cases where personal data is volunteered. Every day, people trade a portion of their privacy for the promise of some return benefit. Benefits can range from a discount on groceries, gasoline, or even novelty items like iPods. Consumers strike this bargain in some of the most mundane moments of life, where the loss of privacy is barely noticed. People also give up their information to complete strangers who are never heard from again. Two of the biggest exchanges of privacy come in the form of grocery store loyalty cards and Internet marketing campaigns. The next two subtopics will touch on the specifics of the interactions between the corporate world and the personal world.

Loss of Privacy with Grocery Store Loyalty Cards

A simple trip to the grocery store offers people perhaps the most common opportunity to trade personal information for a perceived benefit. Today, nearly every large retail grocery store offers some kind of loyalty card based customer tracking system. These programs operate by recruiting customers to voluntarily provide the store with a way to track the intimate details of their shopping habits. In exchange, the stores promise huge discounts on products and wondrous gains in customer service.

To receive a loyalty card, customers must provide the store with detailed information about themselves. The application forms request name, address, phone number, and other demographic information. There are also blanks for e-mail address and cell phone numbers. Once the customer has the card they are eligible to use it at checkout to receive extra discounts not available to non-card-carrying shoppers. Often these discounts appear to be substantial and the consumer is usually given a print out listing the percent and dollar amounts that have been saved by using the card.

In exchange for discounting the price of products, the grocers keep track of the spending habits of their customers in a way that allows them to link a unique person to a particular purchase. Once the purchase is recorded it is stored in a massive database that tracks the customer over time. The grocers claim that this is a mutually beneficial arrangement that allows them to provide customized service to the consumer.

Despite the benefits the grocers attribute to these programs, there are several reasons to believe that shoppers who participate in these programs are getting far less than they bargained for. Consumers get very little in exchange for their sacrificed privacy. These loyalty card programs appear, on the surface at least, to be a boon for consumers, but the grocers would not be pushing these sales tactics so aggressively if they did not provide substantial advantages to the companies. There are several layers of benefit that these programs provide, few of which have anything to do with putting money back in the hands of shoppers.

The biggest promise dangled in front of consumers is that of lower prices on the groceries that they would be buying anyway. However, in many cases the claimed savings simply do not exist. There are a number of ways that grocers mislead their customers into believing that they are getting a bargain. In many documented cases, grocers have raised the "normal price" of items just in time to promote a special card savings opportunity. Albertsons has been caught in the act of deceptive pricing on more than one occasion, and there are examples of this happening at all of the large grocery chains that use a card system (Van Auken 2002).

In Waco, Texas, a local newspaper found that shortly after Albertsons implemented a card program, the price of a block of processed cheese rose from \$3.99 to \$5.99 for shoppers not using the card. Shoppers who chose to participate in the program were able to buy the cheese for the "low-low" price of \$3.99. When shoppers read their receipts they were told that they had saved 33%. In reality, there were no savings (Van Auken 2002). *The Waco Tribune* found that shoppers who paid the full, non-card price on products at Albertsons were paying 20% to 60% more than those who bought the same item at competing stores that lacked a loyalty card program. In fact, even when the card-related discounts were factored in, Albertsons' prices were still considerably higher than those at the four other grocers included in the study (Van Auken 2002).

The use of the cards is often extended to third party retailers that have partnered with the large grocery chains. Local restaurants and entertainment venues offer discounts to card wielding customers even though they did not originally issue the card. In Colorado, the Albertsons Preferred Shopper Card is accepted at over 150 restaurants,

many of them offering savings of 20% or more. Additionally, Albertsons has partnered with rental car agencies and hotel chains to offer discounts on a national basis (“Security and Privacy”).

Safeway has taken its card program even further by allowing people to link their Club Card to personal banking information. The program, dubbed “Safeway Safe Check” by the grocer, enables the shopper to use the card to automatically deduct funds from his or her checking account (“About Club Card”).

While this information seems personal, shoppers in the United States are required to give up relatively little personal information. Loyalty card programs in the United Kingdom require information about such things as corrective eyewear usage, employment status, and the customer’s family status. They even go so far as to as when a pregnant mother is due to give birth (Shabi, 2003).

Consumers don’t seem to mind giving this information out to grocers. In the U.S. over 60 percent of shoppers have two or more loyalty cards (Turcsik 2000). In England over 85% have signed up at least once (Shabi, 2003).

Despite the fact that most consumers use these cards, it’s interesting to note that few consider them to be a factor when deciding where to shop. In a 2004 study, researchers found that shoppers valued such things as a good deli department or a large selection of fresh produce over any particular loyalty card program (Bellizzi, 2004).

On the most basic level, loyalty card programs give retailers a highly effective way to track inventory and customer preferences. When a shopper buys a product, that transaction is linked to all of the purchases that that person has previously made. Not only can this be tracked at that particular store, it can be matched to any purchase made at any of the stores in the chain.

This type of tracking provides very valuable data about what was sold, and to whom. Time and date of purchases can be tracked as well as method of payment. All of these factors feed into a high-resolution profile of individual buyers and their habits. Does she buy cream cheese with her bagels, and if so, in what ratio? How many days pass between his milk purchases? How many different stores within the chain do they shop at? Any of these questions and countless others can be answered with a simple database search.

This information is made even more powerful when it is aggregated into an overall picture of shoppers in a particular region. Customer loyalty cards add a new dimension to traditional inventory management systems by linking individuals to their purchases over time and multiple locations. Trends can be identified and exploited much more rapidly and effectively than they have ever been in the past. Inventory can be re-allocated and realigned to match up with local preferences resulting in a new level of flexibility for retailer (Donegan, 2000).

One of the principal benefits that card programs offer grocers is that they lay the foundation of discriminatory pricing. This is the practice of charging different prices for a particular item depending on any number of identified criteria (Odlyzko, 2003).

Consumers experience discriminatory pricing at every turn. Companies in the air travel and insurance industries have used this

practice to maximize profits for decades. A plane ticket can vary in price depending on the day it's purchased or the length of time the buyer will be traveling. Insurance agents set the price of automotive coverage on such obscure facts as where their clients live and what is in their credit history.

Retailers have become very creative in their use of discriminatory pricing. Beverage companies have even experimented with vending machines that raise the price of cool drinks on hot days (Black, 2003).

To use these pricing tactics, businesses need to be able to track their customers and have a way of adjusting prices on the fly. Grocers have found a way to meet both of these requirements. By instituting a loyalty card program grocers have the tools they need to begin tailoring the cost of food to each individual shopper (Odlyzko, 2003).

There have already been cases where this idea has been put into practice. In an effort to reduce jammed checkout lines, some stores have used increased card related discounts to entice customers to shop at off-peak times. Grocers now are faced with the challenge of sifting through the mountains of information they are collecting to determine the best way to initiate further selective pricing initiatives (Turcsik 2000).

Establishing and maintaining loyalty card programs is an expensive proposition. A grocer can expect to pay as much as 30 million dollars to build a card system and spend 5 to 10 million a year maintaining it (Van Auken, 2002). For the large national chains like Kroger and Safeway the costs are much higher.

While these programs can be costly, the real challenge grocers face is learning how to harness the raw data and turn it into useful information. This is where the real value of loyalty cards is to be established. With the advancement of data mining technology these difficulties are being quickly over-come (Donegan, 2000). For grocers the strategic advantages these systems provide far outweigh the cost.

Consumers often fare poorly in the bargain. They receive very little of the promised benefits of these cards and sacrifice more than they realize. The vast databases that grocers build compromise customers' ability to maintain their personal privacy.

Most of the grocers that offer loyalty cards provide customers with at least a superficial privacy statement. These documents usually look like a formal policy statement where the grocers promise that the information that customers provide will be kept in the strictest of confidences and that the data is held securely in locked and encrypted databases. Despite all they promise, these documents provide no real protection and lead consumers to a false sense of security. The privacy statements themselves are chocked full of loopholes that grocers can, and have, exploited to make money at the cost of the customers' privacy.

Safeway's privacy statement tries to allay the fears of customers by assuring that "Safeway does not sell or lease personally identifying information" but that promise is qualified with the following "to non-affiliated companies or entities." Safeway has provided itself room to maneuver by claiming that they won't give up customers' information unless it is to companies that are Safeway's partners. At no point are those partners identified or enumerated. In effect, the so called privacy statement gives Safeway the right to sell shoppers' entire purchasing

history to anyone who wants to spend some money to become a "Safeway partner" ("About Club Card" 2004). There are already examples of this happening. In 1999, an Internet startup called SmartMouth.com "partnered" with a large chain of grocers. The idea of the business was to make a history of the purchases shoppers had made available to them online. Visitors to the site only had to enter their loyalty card number to be given a complete list of all their recent purchases. SmartMouth.com then offered to analyze the food that the shopper had bought for nutritional value (Van Auken 2002).

There was almost no protection of the data that the grocer had shared with its "partner." Anyone with access to a shopper's card number could review all the person's grocery purchases online (Van Auken 2002). Eventually, this business plan was scrapped due to customer backlash, but there is nothing in the current grocer's privacy statements to keep this from happening again at any time.

One thing not directly addressed in most of the grocers' privacy statements is that these databases can be subpoenaed in almost any court case. Information gathered at checkout counters has been used in divorce proceedings as well as criminal cases. Grocers have made no effort to stop courts from peering into the loyalty card databases (Van Auken 2002). Judges have consistently ruled that if the information is even remotely related to the case, it may be used and thereby become public information available to everyone. Even when stores try to protect the information that customers trust them with, there is no guarantee that a person's purchases will be kept private. This applies to civil as well as criminal cases.

Even with the modest protection that privacy statements provide, there are still instances where shoppers' privacy is in jeopardy. Any networked computer is inherently insecure, and the database servers that the grocers use are certainly no exception. Not only do outside hackers pose a risk, there is a precedent of theft of personal information by people who at one point had direct authorized access to the data. In May of 2004, InfoWeek reported that "Unisys chief security adviser Sunil Misra tells of a case where a member of the senior IT staff at a large supermarket chain created a secret backdoor so he could access and sell protected information" (Calaburn 2004). People who sign up for grocers' loyalty cards are led to believe that they will be saving money in exchange for their willingness to be tracked. They are also assured that the information that is gathered will be held securely and not given out to third parties without the shoppers explicit consent. Unfortunately, both of these promises are predicated by deception on the part of the grocers. There is little benefit to the shopper and their privacy is severely compromised. With nearly all of the large national grocery retailers offering a loyalty card program, it has become difficult for consumers to avoid them. These types of marketing practices have effectively put a real monetary premium on keeping one's buying habits private.

Ethical Analysis of Grocery Store Loyalty Card Programs

Users of grocery store loyalty cards have a choice to make. They are faced with the decision of sacrificing a portion of their privacy for the promise of lower food prices. It becomes a question of short-term

benefits versus long-term costs. In the short term, shoppers are baited with artificially inflated savings that in many cases never existed in the first place. In return, consumers are required to allow the detailed recording and tracking of some of the most intimate details of their life. With the documented abuses that grocers have taken part in, it is difficult to see how the short term gains could possibly outweigh the long term costs. This is an example of ends based thinking on the part of grocers. They are in business to maximize profits for their shareholders. Grocers will take any steps necessary to achieve this goal. In this situation, they are using the apathy and ignorance of their customers in that pursuit.

Online Marketing Ploys: freeiPods.com

Gratis Internet, one of *Inc. Magazine's* 500 fastest growing U.S. companies, specializes in affiliate marketing ("Gratis" 2004). Simply stated, this type of marketing is when one company refers users or customers to another. A common example of this is an advertisement that appears after a Google search. Google hosts this ad for one of their affiliate advertisers. The affiliate pays Google every time someone clicks on their ad. Gratis Internet's most famous venture has been their "free [insert trendy product] dot-com" websites, especially freeiPods.com. Similar to grocery stores, Gratis has developed a way to place a figurative price tag on personal privacy. For freeiPods.com, the price tag is an Apple iPod. Some of their other websites are freeFlatScreens.com, freeHandBags.com, and freeVideoGames.com to name a few ("Gratis" 2004). Gratis Internet will ship an iPod, free of charge, to any user who completely fulfills the requirements of their offer.

Before a web surfer on freeiPods.com creates an account, Gratis presents them with a decision: choose the color of your iPod. This builds the user's excitement and preps them to create an account. Each user sends Gratis their full name, address, date of birth, phone number, and creates a unique username and password. They claim the personal information is mainly used for shipping purposes, but can also be used on behalf of their affiliates. According to *Inc. Magazine*, over 10 million people have registered accounts with Gratis ("Gratis" 2004). Once a user creates an account, there is no way to cancel ("Privacy" 2004). Gratis recommends to simply stop using the campaign's website if the user wishes to cancel their account. The only recourses a user has to manage their personal information are updating it or falsifying it. Gratis retains your personal information, accurate or not, in a database regardless of whether or not you fulfill the remainder of the requirements. To Gratis Internet's credit, they claim any aggregate personal data is not linked with any other data that could positively identify a user ("Privacy" 2004). However, the privacy policy does not actually explain what this means.

The next step for a user to claim their iPod of choice is to complete a free offer from one of Gratis Internet's sponsors. Coincidentally, the sponsors are the same companies who provide Gratis with the majority of their revenue, which amounted to just under \$5 million. Not bad for a fledgling company with only nine employees. Once a user clicks on a free offer, they are forwarded to a third party webpage. Every time a user clicks an offer from one of their sponsors, Gratis gets credit for the

referral.

One of the more popular offers is the Blockbuster Online trial. Users can choose a free two-week trial of Blockbuster Online, which operates very similarly to the Netflix rental model. Blockbuster, as well as many of the other sponsors, requires the user to provide a credit card number before the free trial begins. If the user does not actively cancel the offer by the end of the free period, their card is automatically charged the standard monthly service fee. Since many users forget to cancel the offer before the end of the free trial, the affiliates earn a one-time, weekly, or monthly payment depending on the terms of the offer. Even if the user does cancel in time, the affiliate still has their personal information for use in future marketing attempts. At this point, the user must complete one more step to earn their free iPod.

Now that the user is even closer to getting a free \$300 portable music player, he or she needs to provide Gratis with the names and e-mail addresses of five other people. Not only has the user decided how much their own privacy is worth, but also that of the five referrals. These five referrals must complete the same process in order the original person to receive the iPod. How much is the privacy of your personal information worth? For every user that has managed to earn their free iPod, there are more users who have needlessly signed up for a credit card or purchased discount ink cartridges. Gratis has successfully created a database of personal information with users paying to get in.

Now that the user has given their personal information to Gratis, what makes it valuable to them? When a user clicks on one of ten potential free offers, it shows they are interested in a particular product or service, and the affiliate pays Gratis a small referral fee. Small referral fees add up to a large amounts of revenue when there are millions of people clicking links. Once a product or service interest is linked to a user's account, the data becomes useful to their affiliates, who in turn "bring selected retail opportunities to our members via direct mail, e-mail and telemarketing" ("Privacy" 2004). Out of this list of possible marketing mediums, the user will receive mostly, if not exclusively, e-mail because it is one of the cheapest and fastest methods to market (Richter 2004). The third party will be able to target potential customers they know will be more interested in their product or service than would a random selection. This type of marketing is far cheaper than and more effective than conventional TV or print ads. Although Gratis may not receive any revenue directly from users completing an offer, their current success in obtaining users keeps the heavy hitting clients paying.

Once the user is linked and signed up with a sponsor's offer, they are out of the jurisdiction of the Gratis Internet privacy policy. The user can easily opt-out of any offers sent directly from Gratis, but offers from third party affiliates will flow during the upcoming weeks and months. Each of these seemingly extraneous offers has an option to opt-out, but not before the web of affiliates has been spun. Every time Gratis sends user information to a third party, there is a whole new web of unknowns.

To advanced computer and Internet users, it is common knowledge that no information sent over the Internet is ever 100% secure. The best

Gratis can do is to ensure users their security is “commercially acceptable” (“Privacy” 2004). Gratis shares their users’ information with many third parties, each time increasing the chances of a security breach. Gratis Internet’s privacy policy has been reviewed by TRUSTe, a leader in developing strict online privacy standards (“TRUSTe” 2004). Although the privacy policy is supposed to add a sense of security to the user, there are loopholes. This is a large risk Gratis Internet must take on as a company dealing with millions of accounts holding commercially valuable personal information. They could face lawsuits from their users if the wrong people obtain access to their databases. The same can be applied to their affiliates’ databases as well.

What if the U.S. government decides they need information from a corporate database, which happens on a regular basis? If the government ever requests access from Gratis Internet, they are legally required to comply (“Gratis” 2004). Unfortunately, the government has been known to mishandle commandeered information. In the case of the Enron investigation, the Federal Energy Regulatory Commission made 1.6 million Enron e-mails available online in a searchable database (Swartz 2003). Many of these e-mails and documents contained sensitive personal and corporate information such as social security numbers and banks accounts. Not to say that mistakes this drastic happen every time the government obtains access to a database, but Gratis Internet could be caught in a catch 22. What if Gratis gave access to the government and in turn, the government leaked access to another malignant party? Gratis could get sued simply because they complied with their TRUSTe approved privacy policy.

Gratis Internet has proven their marketing campaigns to be very effective. They have shipped \$2 million worth of iPods to their customers, about 500 per week, and their websites receive about 200,000 hits per day (“Gratis” 2004). This amounts to 1.4 million hits per week. Gratis ships iPods to only a fraction of a percent of these visitors. The few users who do receive an iPod, flat screen TV, or handbag generate enough hype to keep people creating accounts and generating revenue. This marketing process has made Gratis Internet a stable affiliate marketing company in merely four years. As long as the users keep coming, corporate clients keep paying up.

Third party affiliates benefit from Gratis Internet’s campaigns slightly differently. The affiliates pay Gratis Internet every time a user clicks on one of their offers. However, this interest is noted in the user information database and will be used for future marketing. If the user completes the offer, there is a high likelihood of one or more months of revenue because they forget to cancel after the free trial period. If the user really enjoys the product or service, they can become a stable customer and generate even more revenue.

Some users of freeiPods.com benefit, but not in the same way as the corporate clients. In a best case scenario, a user will receive a free iPod. Alternatively, a user will sign up for an offer because they are under the impression they will easily get a free iPod. What the users almost never realize is that they gave their personal, highly marketable, information away and suddenly became a customer of a company they never expected to.

Ethical Analysis of Gratis Internet's freeiPods.com

Philosophers have given labels to many different kinds of ethical thinking: Ends-based, Rule-based, and Care-based to name a few (Kidder 1996, p. 15). While each philosophy appears morally correct in its own light, they cannot all be positively applied to all aspects of life at the same time.

Gratis Internet's application of affiliate marketing is ethically questionable. If all of the users completely understood the privacy policy, and the implications of each step to obtaining a free iPod, many users would abstain from the entire process. While a good business person would not want to be treated any differently than he or she would treat another, the people running Gratis Internet have full knowledge of the implications to their users. They have shined a spotlight on a free iPod, and this lures people into the marketing scheme for the life of whatever databases their personal information makes its way into. It simply takes too much time and understanding for the average user to figure out the importance of their personal information. People write down their name, address, phone number, and e-mail address so frequently that it is almost second nature to disclose these pieces of information to whoever may ask for them. The users of freeiPods.com have effectively agreed to accept months upon months of e-mails from affiliates of affiliates because they wanted a \$300 MP3 player. Not only will the vast majority never see their free iPod, but they have signed up as a customer for another company and are likely to have spent money as a result. People typically do not appreciate being misled. The people running freeiPods.com value money over their honesty.

On another note, out of 10 million user accounts, it is inevitable that some of these people recognize the implications of creating an account. These advanced users understand that they will forever be pinpointed marketing targets. Not everyone can afford to spend \$300 on a novelty item like an Apple iPod. People are willing to trade their personal information in exchange for the slim chance they could receive the free MP3 player. They have weighed the long-term consequences of giving their personal information to Gratis Internet and accounted for the short-term benefit of a free iPod.

Conclusion

With the growing popularity of Internet marketing and grocery store loyalty cards, companies are discovering new and unique ways of attracting customers, both corporate and consumers. As a result of these new marketing practices, consumers are offered high valued products in exchange for their personal information. So far, methods like the freeiPods.com marketing scheme have proven effective, but at some point the bubble of spam e-mails is going to burst. Web surfers are willing to give away their personal information and sign up for offers they never intended to. Shoppers have proven themselves willing to exchange their personal information for discounts at checkout. In both cases, the price of privacy is hardly being met in a way that benefits consumers in the long term or even in the short term.

Works Cited

- "About Club Card." *Safeway Corporate Website*. October 23, 2004. <http://www.safeway.com/club_card.asp>.
- Bellizzi, Joseph A. "An Assessment of Supermarket Loyalty Cards in One Major US Market." *The Journal of Consumer Marketing*. Santa Barbara: 2004: Vol. 21, Iss. 2/3. p. 144.
- Black, Jane. "Sharper Tools for Discriminatory Pricing." *Business Week Online*. July 31, 2003. <http://www.businessweek.com/technology/content/jul2003/tc20030731_6139_tc073.htm>.
- Claburn, Thomas. "Feds Want Tougher Penalties For Insider Identity Theft." *Information Week*. May 24, 2004. <<http://www.informationweek.com/showArticle.jhtml?articleID=20900519>>.
- Donegan, Pracilla. "Mining for knowledge." *Grocery Headquarters*, February 2000: p. 27-31.
- "Gratis Internet Garners #95 in Inc. Magazine's Prestigious Inc. 500 Ranking of 500 Fastest-Growing Companies in the U.S." *Business Wire*. October 26, 2004. <<http://www.proquest.com>>.
- Kidder, Rushworth M. "Overview: The Ethics of Right versus Right." *How Good People Make Tough Choices*. New York, NY: Fireside: 1996. p. 14-29.
- Miller, Jack. "How Companies Can Benefit by Addressing Privacy Issues." *The CPA Journal*. 2003: p. 14. <<http://www.proquest.com>>.
- Odlyzko, Andrew. "Privacy, Economics, and Price Discrimination on the Internet." *University of Minnesota*. July 2003.
- Parker, Robert G. "How to Profit by Safeguarding Privacy." *Journal of Accountancy*. 2003: p. 47-52. <<http://www.proquest.com>>.
- "Privacy Policy." *Privacy Policy*. Gratis Internet. October 13, 2004. <<http://www.freeiPods.com>>.
- Richter, Scott. E-mail interview. September 21, 2004.
- "Security and Privacy." *Albertsons Corporate Website*. October 23, 2004. <www.albertsons.com/privacy.asp>.
- Shabi, R. "The card up their sleeve." *The Guardian*. July 19, 2003. <<http://www.guardian.co.uk/Print/0,3858,4714196,00.html>>.
- Swartz, Nikki "The Electronic Records Conundrum." *Information Management Journal*. 2003. <<http://www.proquest.com>>.
- "TRUSTe Partners with NetCreations to Increase Consumer Confidence around Collection of Personal Information." *Business Wire*. October 18, 2004. <<http://www.proquest.com>>.
- Turcsik, Richard. "In the Cards." *Progressive Grocer*. New York: Jun 2000. Vol. 79, Iss. 6. p. 61-65.
- Van Auken, Cindy. "Consumers' Group Blasts Loyalty Cards; Grocery Stores Defend Programs." *Waco Tribune Herald*, 2002.
- "Want the CIA Director's Address? Get it for \$26 Online." *Information Management Journal*. 2003: p. 16. <<http://www.proquest.com>>.