Quantifying Privacy Choices with Experimental Economics

David L. Baumer[1], Julia B. Earp[2] and J.C. Poindexter[3]

College of Management, North Carolina State University, Raleigh, NC 27695-7229
[1] David_Baumer@ncsu.edu [2]Julia_Earp@ncsu.edu [3]JC_Poindexter@ncsu.edu

Submitted to: Law and Economics category of the 2005 Workshop on the Economics of Information Security (WEIS'05)

An earlier and abbreviated version of this paper was presented at the Workshop on Privacy in the Electronic Society (WPES), October 2004

Abstract

The importance of personal privacy to Internet users has been extensively researched using a variety of survey techniques. The limitations of survey research are well-known and exist in part because there are no positive or negative consequences to responses provided by survey participants. Experimental economics is widely accepted by economists and others as an investigative technique that can provide measures of economic choice-making that are substantially more accurate than those provided by surveys. This paper describes our preliminary efforts at applying the techniques of experimental economics to provide a foundation for estimating the values that consumers place on privacy and various forms of security, such as encryption and HIPAA. In the activities described, experiment participants are graduate and undergraduate students currently seeking jobs. Preliminary results from two pilot experiments suggest that a complete set of experimental measures of choice-making will provide valuable quantification of behavior in Internet privacy/security space. These results also show that online job seekers place great value on security measures, both legislative and technical, that make identity theft much less likely.

1 Introduction

Information privacy has been recognized as an important concern in a wide variety of settings, ranging across the disciplines of computer science, management, law, and consumer behavior. A 1999 survey revealed that 87% of Internet users are concerned with threats to their privacy when using the Internet [CRA99]. Since that time, a number of other credible studies have reached similar conclusions [EB03, EAA05]. It is apparent that Internet users' concerns about privacy and security are realistic as the FTC reports that, for the fifth year in a row, "identity theft topped the Federal Trade Commission's list of most-reported frauds, …" [SU05]. Dissatisfaction with the privacy/security status quo is likely to increase as computerization of personally identifying information (PII) continues to lower the costs of acquiring, storing and transferring such information [MSB00, Rau02].

In addition to computerization, there has been a proliferation of other technologies used to acquire and transfer PII. All of the following are responsible for making inroads on personal privacy: widespread use of the Internet, networked systems, radio frequency identification (RFID) tags, surveillance cameras, location-tracking wireless devices, cards that track buying patterns and electronic storage technology that allows organizations to store an abundance of personal information. These technologies all provide opportunities to collect and store large amounts of personal information about online users, potentially violating those users' personal privacy wishes [Bel97, Cla99]. No doubt, additional technologies and mechanisms for capturing and storing personally identifying information will be developed and utilized.

Even though it is evident that there is growing dissatisfaction with the inroads to personal privacy carved out by new information-collecting technologies, the designs of technologies often leave privacy as a concern that is considered and addressed as an afterthought [AE01]. Some organizations are now considering privacy earlier in the product design process and are struggling with the tradeoff between maximizing the benefits from collecting customer information while adhering to user privacy preferences. Simultaneously, government actions in the form of legislation requiring a focus on privacy and security measures, in conjunction with enforcement actions by administrative agencies, particularly the FTC, are increasingly a part of the legal environment (with attendant compliance costs) [BEP04a].

Quite clearly, improvements in the accuracy of measurement of the true *value* of privacy to Internet users is a high priority as the design of privacy-preserving technologies and practices has become an important focus for organizations, both for-profit businesses and policy makers. The possession of accurate privacy/security valuation has become increasingly important for organizations as they invest time and resources into privacy policy development and enforcement, access control, and general privacy management technologies.

Among scholars in information technology, a commonly used and accepted approach to assessing user privacy values involves the application of survey methodologies. Although survey measures can be useful in identifying user concerns and, to some degree, in rank ordering those concerns, they still suffer a number of shortcomings, mainly due to the fact that no consequences flow directly from the choices "reported" by respondents [SMI03]. "Polls record unmotivated, representative, average opinion, while markets record motivated marginal opinion that cannot be described as 'representative'" [FHSS94]. Forsythe, et al., report that when voters are given a monetary stake in outcomes, as in the Iowa Electronic Market (IEM), participants' predictions are superior to those gathered via exit polls and that there is less forecasting error in the periods leading up to elections relative to nationally prominent polls [FHSS94].

Another reason to be skeptical of poll results is that self-described behavior is influenced by idealistic myths respondents have about their actions in a given setting. In fact, there are often sizeable disparities between what people say (survey answers) and the actions they take [EB03]. Repeated surveys reveal that consumers sometimes appear irrational which is at variance with economic theory [BEC62], though some investigators have other explanations for seemingly irrational individual behavior [Smi03]. Even though some of our prior work involves reporting the results of surveys we designed and administered, we recognize the limitations of that work and believe that using economic experiments will allow us to enhance the accuracy of our measurement of user valuations of privacy and security.[1]

This paper reports the insights gained by a preliminary application of experimental economics methodology. As is standard in this field, we have relied on the provision of real interests (rewards and penalties) for participants and have tightly controlled the experimental test situations employed to prevent outside influences from affecting choices made by participants [FV04]. Our current interest was primarily in testing the applicability of experimental economic techniques in a research program aimed at going beyond the metrics that survey methodologies are able to provide in order to better estimate and quantify user choices and responses to changes in the Internet environment. The results of our preliminary work, presented in this paper, are unique as to our knowledge they reflect the first application of experimental economics methods to the search for an understanding of consumer privacy demands.[2]

We present the results of our first pilot study and some of the highlights of a second pilot study. In these preliminary investigations, we have examined the privacy/access tradeoff choices made by job seekers as they make use of online resources to initiate job searches. The job-seekers in these experiments make decisions that impact both their privacy status and their prospects for finding ideal jobs. The remainder of this paper is organized as follows. Section 2 provides an overview of the survey methodology applied to privacy studies, and of experimental economics and the ways in which experimental economics methods can benefit privacy researchers. Section 3 describes the methodology applied in our pilot experiments and Section 4 presents the empirical results of our preliminary efforts. Finally, a summary and discussion of future work is provided in Section 5.

2 Relevant Literature

2.1 IT Survey Methodology for Individual Privacy

An extensive literature has been created by researchers who have used surveys to investigate user privacy opinions. Privacy surveys typically use one of two common approaches. The first approach simply asks respondents to rate the respondent's agreement (strongly agree, agree, etc.) to various privacy practices by asking questions such as, "are you willing to supply your social security number to this website?" [EP03]. Although a valid approach, this methodology does not provide the individual with an *environment* that necessarily requires a realistic and accurate response. The manner in which people think they would "act" in a specific situation may be different from the manner in which they act when they actually have to make choices and bear the consequences of those choices. The second approach provides respondents with a scenario narrative and then asks them about their corresponding privacy concerns [ACR00]. The scenario approach can provide more "environment" for participant responses, but it is based on text rather

[1] The Privacy Place™ contains an extensive collection of paper and published works about Internet user privacy and security (http://theprivacyplace.org/).

[2] This statement is made after searching both the information technology (IT) and experimental economic literature.

that visual stimuli. Of course, this second approach, as is the case with all surveys, requires researchers to assume that respondents' answers are the same that they would be if there are real consequences to their decisions.

In an early study, a 15-item survey instrument based on extant literature was designed to measure individuals' concerns regarding organizational information practices [SMB96]. This widely cited privacy survey named four categories of abuses of personally identifying information:

- *Collection* measures concerns about the collection and storage of large amounts of information.
- *Errors* addresses concerns regarding errors in data collected about individuals.
- *Unauthorized secondary use* involves concerns about data being collected for one purpose, and subsequently used for another purpose without the individual's consent.
- The fourth subscale, *improper access,* refers to concerns about individuals' data being available to unauthorized viewers.

The Smith et al. survey [SBM96], as frequently described in the information systems literature [AJB98, SS02], focuses on determining which of the four categories of abuse are of most concern to users. Like all privacy *surveys,* it relies on the self-described behavior of the respondent and, hence, likely represents users' idealistic behaviors rather than the users' actual online behavior.

Another important survey conducted several years ago asked 381 United States Internet users about their online privacy concerns in specific online scenarios [ACR99]. These Internet users were then categorized according to off line privacy user categories of [HW91, 94, 96, 98]. In this study, *Privacy Fundamentalists* are individuals who are extremely concerned about their privacy, so they rarely reveal any private information about themselves, even when privacy protection measures are in place. The *Pragmatic Majority* represents the bulk of Internet users; these individuals are concerned about privacy, but less so than Privacy Fundamentalists. The Pragmatic Majority often has specific concerns that can be addressed by making privacy policies/mechanisms available to them. Finally, the *Marginally Concerned* refers to those individuals who are willing to provide personal information to websites under almost any circumstances.

In an extension of [ACR99], [SGB01] determined that the Pragmatic Majority category could be divided into two specific clusters: the Identity Concerned and the Profiling Averse. *Identity Concerned* individuals are most worried about revealing personally identifiable information such as name, address, email address, etc., whereas the *Profiling Averse* are more concerned about revealing information about their hobbies, interests, health, etc. A slight population shift towards the Privacy Fundamentalist side was also observed in this later study [SGB01], suggesting increased privacy threat awareness among Internet users. These studies accurately portray the kind of behavior users think they exhibit, but once again these ideas may not accurately portray the users' true behaviors.

Few privacy surveys have used a visual layout to enhance the typical textual design of a survey instrument. [EB03] describes a survey design that used the flexibility of the web to offer respondents a realistic visual to emphasize survey items. Respondents in this online survey were exposed to screen shots of actual websites and asked about their willingness to reveal PII to that website or do business with that website. By providing actual screen shots of various websites,

the survey brought respondents closer to the settings they face on line when deciding whether to reveal personal information to a specific actual website.

The realism of asking consumers to respond on line to actual screen captures likely enhances the reliability of survey results relative to asking consumers, in the abstract, about their willingness to reveal information on line. Such an approach is a step in the right direction, but it still requires users to provide self-descriptions of on line behavior, which may differ markedly from actual behavior. Illustratively, fifty-four percent of respondents surveyed in this study [EB03] said they would read a website's privacy policy on the first visit. That number is grossly inconsistent with website privacy policy log data from several organizations, which regularly reveal that fewer than two percent of Internet users review an organization's privacy policy in their first visit and that fewer still examine website privacy policies for changes in subsequent visits.[3]

A survey of users and businesses found that 87.5% of surveyed users expect to see comprehensive information regarding privacy practices when visiting a commercial website [FK99]. Similarly, another poll found that 59% of users have read privacy notices while 91% thought it important to post privacy notices [HW91, 94, 96, 98]. Although it is obvious that Internet users and customers think the presence of privacy policies is important, it is less obvious how this information aids managers and IT staff charged with responding to customer and user demands for privacy and security. A recent survey of more than 1000 Internet users revealed that there is a notable discrepancy between what privacy policies are currently stating and what Internet users say are their strongest privacy concerns [EAA05]. Managers and computer scientists can use the results of various privacy surveys such as these to justify spending resources in protecting data collection and storage, but the contours of efficient expenditures on privacy and security remain elusive.

It is hoped that creating an accurate economic model of user privacy will provide privacy/security valuations free of the idealistic notions self-reported in earlier surveys, assisting computer scientists and managers in making more accurate and productive decisions regarding privacy management and security technology choices. To date, there have been no studies that apply experimental economics as a means to model user privacy values.

2.2 Using Experimental Economics

There are three main areas of application of experimental economics: testing and quantifying theories of individual choice, testing game-theoretic hypotheses, and investigating industrial organization issues. The commonality of these areas is that decision-makers' choices determine how much benefit they (or their organization) will enjoy, with that benefit often measured in monetary terms. Quite typically, economic experiments address decisions that are made in a probabilistic setting; one where outcomes are not known with certainty. Experimental economics is, then, well suited for examining individual choice settings in which experiment subjects are confronted with opportunities to take or refuse certain gambles or risks where payoffs (or losses) have real value – monetary or otherwise. The exercises we describe follow this pattern.

The methods of experimental economics are well suited to modeling decision-making on privacy and security issues, in this case applicable to Internet activities. A large number of applications have involved decision-making under uncertainty (e.g., [Sav71], [Sho91], [Sip97]),

[3] Numerous discussions with industry CIO's who collect such data report tiny percentages actually visit website privacy policies.

which is precisely the plight of Internet users. Ideally, experimental economic exercises allow for the "repetitive testing" study of a process or behavioral response, allowing the testing of expected responses in lifelike settings. As indicated earlier, potential payoffs from this approach include a deeper understanding of the principles at work prompting observed responses and measurements that inform us regarding the strength of responses.

Economic experiments are typically governed by rules, which can be explicit or implicit. Explicit rules are defined either by the experimenter, or by events, occurring in the game, that have a specified payoff to the subject. For example, these rules may be those at an auction where motivated people buy or sell abstract rights (to consume or produce) information and services. Implicit rules are the norms, traditions and habits that people possess as part of their cultural or biological self. Hence, they are not controlled by the experimenter [Smi02]. This illuminates the natural fit between the core concept described and the everyday experience of Internet users. Internet users come to this modern electronic marvel with habits, beliefs, expectations, tastes and behavioral standards that are the result of their cultural, social, vocational and biological heritage. They are then confronted with opportunities for interactions – information dominated – that expose them to hidden rules, charges, and payoffs, positive or negative, that are dictated to them through the medium they have chosen to enter. They enter this medium with pre-existing beliefs, but adapt those beliefs to experience. Replacing the actual Internet (and Internet experience) with an "experimental" Internet experience that closely parallels reality offers the opportunity to closely track choices made with pre-existing beliefs, adjustments in choices with learning, and subsequent adjustments with learning to alterations in the structure they confront [Bro95].

2.3 Prior Economic Experiments that Deal with Privacy

A search of the experimental economics literature does not reveal prior use of it to uncover Internet privacy valuation and preferences [Holt99]. Similarly, there are no published studies in the information technology privacy and security literature that make use of experimental economics to estimate Internet user behavior with regard to privacy and security [EPB04]. Given the substantial reported deviations between survey results and actual behavior, it is clear that there is substantial room for improvement in the quantification of Internet users' valuations of privacy and security and their responses to changing risks in Internet usage.

3 Methodology

The Internet confronts users with numerous opportunities for decision making that affects both the benefits enjoyed and the risks experienced from usage. As a consequence of the richness of interaction opportunities, we anticipate a research process that requires multiple phases that, in the end, will provide a model of consumer behavior in the making of privacy/security decisions along multiple dimensions. Interfaces that deserve attention include those associated with healthcare, financial transactions, job searches, and general Internet usage. Our initial experiments have focused on job searches using students, graduate and undergraduate, as subjects. The research activities have been conducted at a large university in the southeastern U.S.

The core assumption of our experiment is that people will attempt to maximize the net benefits of using the Internet for various purposes while recognizing that Internet connections

result in both positive outcomes (e.g. easy communication, rich and efficient sources of information) and negative outcomes (e.g. SPAM, spy-ware, viruses, identity theft). We assume that more intensive Internet usage brings increased benefits, but that it also is likely to bring additional risks. To parallel their assumed "real world" behavior, we provide "real interest" motivation through a course grade incentive. Experiment performance is monitored in "counting money" terms, with subjects provided with an initial money allocation. Their money balances are used for tracking the net benefit from Internet usage choices made by the students.

The purpose of the pilot study described herein is to guide us in preparing additional experiments that will use an electronically simulated Internet environment. This section provides a detailed description of the economic methodology that we followed in our pilot experiment. Such detail is warranted since this is the first application of experimental economics to the privacy domain.

3.1 Participants and Incentives

The pilot study was divided into two groups; group A was comprised of undergraduate students enrolled in a single section of a law class and group B was comprised of graduate students enrolled in an Internet law class. A course requirement for the students in group A was a term project, accounting for 25 percent of their total grade. As an option, these students were able to forego the term project and participate in this economic experiment. Students were told that by participating in the economic experiment, 25% of their grade would depend on the amount of money they had at the end of the economic experiment. Students were told that the top one-third of them would earn a "95" for the term project, the middle third an "85" and the bottom third a "75". Twenty-seven of thirty-five students enrolled in the course chose to participate in the economic experiments described below. Casual observation of the students suggests that given the impact on final grade, these students were very motivated to "optimize" their net benefits from Internet activities so as to finish in the top one third or avoid the bottom third. Unlike survey research where there are no beneficial or adverse consequences to making the wrong choices, it is clear that the participants were very aware of the consequences of their choices in a cyberspace is an environment characterized by a good deal of uncertainty.

Students in group B were given a different, but appropriate, incentive structure. These students were allowed to increase their class participation grade by up to 100 percent (those finishing in the top one-third received a "100" for participating, the next group was promised a "90" for their class participation grade if they finished in the middle third and an "80" if they finished in the bottom third). Class participation for this group comprises ten percent of their final grade. Students were told that their class participation grade could exceed "100" by participating in the economic experiment. Unlike Group A, Group B students could not hurt their grade by participating, but at the margin their performance could be the difference between letter grades. Reflecting the value of this opportunity, all 32 students in the graduate course elected to participate.

3.2 Choices and Outcomes

Group A was provided with the following information before making choices:

Table 1: Information for Subjects in Group A

You are in your final semester at the University and you are looking for a job. In order to get a job you have to prepare a resume. On your resume, you list your education, age, gender, and job objectives.

Among the means you have for advertising your talents and job interests are three types of websites:
1) General employment websites (GEW) such as Monster.com, which is known for its volume of job seekers and the number of employers who survey it.
2) Employer websites (EW) that allow you to apply online. The employer websites generally require you to submit more information about yourself than GEWs. Often, EWs require you to reveal your social security number and other information that typically does not appear on resumes so that the employer can check your credit history.
3) Headhunter websites (HW) are selective but they are also the websites where the best jobs are often found. HWs require much more information, including detailed health information about you and your family. HWs also require your social security number.
4) Family and friend contacts (see below).

By revealing your resume to websites, there is a small probability that your personally identifying information (PII) could be obtained by non-employers who could harmfully exploit that information. Among the negative consequences of your resume ending up in the "wrong" hands, is the possibility of identity theft. Statistics compiled by the Federal Trade Commission (FTC) reveal that the typical victim of identity theft loses an average of $5,000 when the damages attributable to ruined credit, the hassles associated with clearing up misinformation, and legal fees are totaled. Also according to the FTC, the chances that you will be a victim of identity theft are 10 times as great when you reveal your social security number to a source. Note further that all of these websites rely on electronic submissions and identity thieves specialize in intercepting electronic transmissions. The chances of interception by identity thieves can be reduced to near zero if the information you send to websites is encrypted and some, but not all, websites advertise that they use encryption to make transmissions secure.

Headhunters make money when they send reliable, healthy job candidates to companies who are expected to stay with the company for an indefinite period. Although companies are not allowed to discriminate because of disabilities, companies are allowed to take health data into account when making hiring decisions for those who are not protected by the Americans with Disabilities Act. Using DNA analysis and family health histories, companies are now able to predict, with some accuracy, which job applicants will later cost the company considerable money because of long term health problems.

Assume the following probabilities are present:

If you submit your resume to a GEW, your have a 50% chance of being hired in the first three months of submission. According to statistics supplied by the GEW, the average starting salary of job seekers is $30,000.

Also during the period you have a 1/1000 chance of being a victim of identity theft. Some of the "employers" who have access to GEWs are not authentic employers, but in fact are scam artists and identity thieves.
For a fee of $25.00 you can request that the GEW encrypt your resume data. If your data is encrypted, your chances of becoming a victim of identity theft are reduced to 1/10000.
At the end of the three-month period, you can resubmit your resume to the GEW, in which case you again have a 50% chance of being hired, but you also endure the same probabilities of being a victim of identity theft.

If you submit your resume to EW, you have a 50% probability of being hired in the first 3 months. The job you are applying for has an advertised starting salary of $40,000.

Many of the EWs do not have the security precautions that are undertaken by GEWs. The probability of being a victim of identity theft is much higher because applicants are required to submit social security numbers and security measures undertaken by employers are less able to deter identity thieves. Also, some "employer" sites are fronts for identity thieves to get your information. Assume that the probability of identity theft if you submit your resume to an EW is 1/100.
For $100 you can hire a detective website (DW) that specializes in identifying EWs that do not take adequate security measures or are fronts for scam artists. If you hire a DW, your chance of being a victim of identity theft is 1/1000.
By submitting your social security number of an EW, you have a 1/500 chance of being identified as a **health risk** based on pooled health data that some employers are able to access. If you are classified as a health risk, it will cost you $1,000 more to sign up for health insurance and you will not be hired by this employer. Unless you are living at home, you must obtain health insurance.

If you submit your resume to a HW, your chances of being hired are 25% in the first 3 months at an average starting salary of $60,000.

Using DNA analysis and other medical information you are required by HW websites to submit, you have a 1/10 chance that you will be rejected by prospective employers as a **health risk**.
If you are classified as a health risk, it will cost you $1,000 more to sign up for health insurance and you are precluded from reapplying for a job at a HW because headhunters share their data.
If you are rejected for health reasons, your chances of obtaining another job at a GEW or EW are reduced by one-half.

Of course, you do not have to reveal any information about yourself to any websites; you can try to get a job based on contact from family and friends. If you choose not to submit your resume to any of the websites listed above, your chance of being a victim of identity theft is 1/10000. On the other hand, if you only look to your family and friends for a job, your expected starting salary is $20,000 per year, and you have to live at home with your parents.

The four choices (above), made available to Group A participants, are reasonably indicative of the choices that current college graduates face. Soon-to-be graduates know that the Internet is a very efficient mechanism for advertising that they are seeking employment and the skills they bring to the job market. For recent business management graduates of this University the starting salaries are reasonably accurate. Group A participants have never known a time when computers and the Internet were not an important fact of life. They are very aware of the dangers of identity theft and they are aware that medical records are computerized and can be used in ways that are adverse to their interests.

A few plausible adjustments were made to the choices facing Group B (see Table 2). First, all of the expected starting salaries were doubled. Second, the costs of obtaining "protection" from identity theft and being labeled a health risk were adjusted so that it would cost the participant $500 to encrypt his data (assuming he or she selected option 1.) and $1,000 to hire a detective website that would investigate whether employer websites were authentic (assuming he or she selected option 2.). In general, Groups A and B were subjected to the same options except that the starting salaries were different so that the choices the participants faced corresponded to what they probably faced in the current job market given their respective educations.

A payoff matrix establishes the possible outcomes from each experimental choice made and the probabilities of each outcome. The instructions provided by the payoff matrix for our initial pre-test exercises are given immediately below. Note that the payoffs are not linear. The choices and payoffs we provide should be familiar to many students, whose net worth are often less than $10,000, use Monster.com to get a job, and know that there are consequences to identity theft etc.

Table 2: The Payoff Matrix for Group A

The payoff matrix is constructed so that you can calculate your money at the end of the four periods. Note that you can "quit" participating at any time. You can always decide to live at home and earn the salary and net income that corresponds to option 4. below.

Assume that your initial endowment (or net monetary worth) is $5,000. As stated above, you have four choices:

1) If you submit your resume to a GEW and you are hired, add $7,500 ($30,000/4) to your income for each period that you are employed, minus $5,000 in living expenses. Your net gain for three months of a starting salary of $30,000 after three months is **$2,500**. If you are victim of identity theft, you are "busted" and have a net worth of zero. If you are hired to a $30,000 per year job in the first period, in subsequent periods, you can apply to other websites. If you are hired at an EW or a HW, you increase your money accordingly, but of course you also endure the risks listed in those websites.

2) If you submit your resume to an EW and you are hired, add $10,000 ($40,000/4) to your income, but subtract $6,000 for living expenses, making your net worth **$9,000** after three months, ceteris paribus. Even if you are a victim of identity theft you could still be hired, but your net worth is $5,000 lower. However, if you are identified as a health risk, you will not be hired by that employer and have to wait until the next period to reapply at another EW or try your luck at a GEW or HW. Also, lower your net worth by $1,000 if you are identified as a health risk.

3) If you submit your resume to a HW and you are hired, add $15,000 to your income, and your net worth increased by **$7,000** because your living expenses are assumed to be $8,000 during the three-month period. If you are successful in the first period and are hired at $60,000, you can resubmit your resume to another HW. If you already have a $60,000 per year job and resubmit to a HW and are successful in getting hired, increase your salary by 50% to $90,000 year and your net worth by $20,000 in the next three-month period. Of course, if you resubmit your resume to a HW, you also assume the same risks as discussed above associated with HW websites. If you have a $90,000 a year job, you can resubmit your resume to another HW. If you are successful in obtaining another job, increase your income to $135,000 per year and your net worth by $50,000 for the three-month period. As before, by resubmitting your resume to a HW website, you endure the risks inherent in such sites.

4) If you choose not to submit your resume online, instead restrict your submissions to family and friends, then you can assume that your family will pay for your health insurance. Your parents have decided that you are old enough to pay rent and so your net income after three months of living at home and earning $20,000 per year is **$1,000.**

The main differences between the Payoff Matrices for Group B relative to Group A are that the payoffs are higher but the differences are non-linear. Briefly, if the participant was hired and selected choices 1-4 as described above, the payoffs (additions to net income) to Group B participants were:

1. $5,000
2. $8,000
3. $22,000
4. $2,000.

3.3 Final Instructions and Location

Both Groups were told before participation that their net worth would be affected by whether the job they are offered corresponds to their location preferences. Before making their selections, participants were instructed that:

There are ten cities listed below, next to letters, A through E. Please select your preferred locations from the two lists below. If you are successful in getting a job and your location matches one of the cities in the two lists below, add $2,000 to your net worth. If you are successful in getting a job but your job location is different from the two cities you select, subtract $1,000 from your net worth. Please select from the list of cities below, your most preferred job location and your second most preferred. New York, Boston, Chicago, Raleigh-Durham area, Atlanta. Miami, New Orleans, Los Angeles, Seattle, Denver.

As we know, an important job satisfaction factor is location. The importance of location is influenced by proximity to relatives and to temperature. Participants who listed a city from the lists below that turned out to be where their job was located had their net income raised $2,000 for the three-month period. For those who jobs turned out to be in a city that was not listed among their top two choices, their net worth for the three-month period was reduced $1,000. Those who elected not to submit their information on the Internet but instead restricted their search to family and friends were assumed to have selected their abode (their parents) and thus there were no location adjustments. The same salary increments and decrements were used for both Groups A and B.

4 Empirical Results

4.1 Results of the First Experiment: Groups A and B

All of the results are shown in Table 3. For the first trial, random number generator simulacrums were used to create the results, which were posted next to student ID numbers (not their social security numbers). After each experiment students could not only see how they fared, but they could also see how others fared. For each group at least one participant became a victim of identity theft and one was a victim of being identified as a health risk. The participants from both groups made their choices from the list of websites above and the results were as follows:

Table 3: Website and Protection Choice Frequencies

		GEW	EW	HW	HOME		Totals
Experiment 1							
	Group A	2	21	1	3		27
	Protection	2	19	n/a	n/a		21
	Group B	2	22	6	2		32
	Protection	1	14	n/a	n/a		15
Experiment 2							
	Group A	1	22	2	2		27
	Protection	1	22	n/a	n/a		23
	Group B	0	15	10	2		27
	Protection	0	11	n/a	n/a		11
Experiment 3							
	Group A	0	17	8	1		26
	Protection	0	14	n/a	n/a		14
	Group B	1	10	15	1		27
	Protection	1	6	n/a	n/a		7
Experiment 4							
	Group A	3	10	3	11		27
	Protection	2	10	n/a	n/a		12
	Group B	1	13	9	7		30
	Protection	0	11	n/a	n/a		11

For Group A, 21 of 27 participants elected to submit their resumes to option 2, which is an employer website. This choice is not surprising since it has the highest expected value, ignoring risks. Of the 21 participants who selected option 2, 19 opted to pay for protection in the form of a $100 payment to a detective website to investigate whether the employer website they submitted their resume to was indeed authentic. Of the two participants who selected General Employment websites, both selected to encrypt their data, so when given a choice in a risky environment, 20 of 22 participants elected to pay money for protection against identity theft.

Similar results were recorded for the Group B participants. Of the 32 participants, 22 selected option 2 (EW) and of those, 14 were willing to pay for protection in the form of a detective website. A possible reason for the decreased willingness to pay for detective websites by Group B participants is the increased cost of this protection. We set the cost of identity theft protection for Group B participants at $1,000 whereas the same protection cost Group A participants $100. We were interested in some measure of the demand elasticity for protection from identity theft. The reduced quantity selecting this protection reflects the law of demand.

4.2 Results of the Second Experiment: Groups A and B

In the second experiment, both Groups were presented with the same options, but the results of the first round were made visible to them. As in the "real world", we assume that job seekers are influenced by news broadcasts as well as word of mouth communications among fellow job applicants. For the second economic experiment, there were no "pseudo" news announcement that participants were able to take into account before making their selections as to websites visited and protection purchased. Participants of each Group were able to see the results of the first experiment and in viewing those results they would have found that:

- one participant was a victim of identity theft and thus had a net wealth decrease of $5,000; and
- one participant was identified as a health risk and as a result suffered a net wealth decrease of $1,000.

In lieu of repeated experiments in this set of pilot exercises, we have assumed that the results of the second experiment would be (1) not dissimilar to those for the first experiment and (2) would therefore represent an equilibrium condition, with the differences among participants reflecting differing risk preferences. In fact, 22 of the 27 participants in Group A selected option 2. (employer websites) and each selected protection in form of paying $100 for a detective website. For Group B, of the 27 participants for the second experiment, 15 selected option 2 and of those 11 elected to pay $1,000 for detective website protection.

As before, Group B participants were more adventuresome than those in Group A, which is plausible and illustrates a major shortcoming of survey research. With 25 percent of their final grade at stake, Group A participants were clearly motivated and, not surprisingly, their participation rate for four weeks was nearly 100 percent. Those who teach undergraduates on a regular basis know that undergraduate attendance during the late spring often falls well below perfect. For Group B participants, their performance in these economic experiments only minimally affected their final grade and the direction of the impact was always positive. Ten of the participants from Group B selected option 3, which has a starting annual salary of $120,000, but also involves more risk and a lower probability of being hired. Option 3 is the option that would appeal to those who have a positive preference for risk. For each group in the second experiment, two participants elected not to submit their resume information online and instead restricted their exposure to option 4, family and friends.

4.3 Results of the Third Experiment: Passage of HIPAA

Before making their selections for the third economic experiment participants in both groups were advised that the Health Insurance and Privacy Accountability Act (HIPAA) had been passed by Congress and therefore nonconsensual distribution of medical records was made illegal.[4] In earlier work, survey research revealed that those entrusted with health records regarded nonconsensual distribution of medical records as the greatest threat patients' privacy [BEP00]. In this round, participants were told to regard the probability of them being termed a "health risk" as is discussed in options 2 and 3 above are radically reduced as a result of the pseudo news event, the promulgation of HIPAA regulations. As with other changes in risks mentioned in these experiments, students were not told that the risk was eliminated, but only that the probability of being labeled a health risk was substantially changed.

[4] 26 USCS § 9802 (2004).

4.4 Results of the Fourth Experiment: The Frequency and Cost of Identity Theft Increases

For the fourth and final experiment, participants were told to assume that,

> "*The consequences of identity theft were doubled to $10,000 and its prevalence was substantially increased*."

Examining Table 1 above, the most apparent effect of this pseudo change was a far greater number of participants electing not to submit their resumes online but instead restricted the distribution of their identifying information to family and friends. Eleven Group A participants selected option 4 thereby refusing to submit their resumes online where they would have much higher expected values, but of course there were now much greater risks. All but one of Group A's participants who selected options 1 or 2, where identity theft protection could be purchased, did so. Among Group B participants, 7 participants refused to submit their resumes online and risk identity theft. Eleven of 13 Group B participants who selected an employer website were willing to pay $1,000 to a detective website to make sure the employer website was authentic. In the fourth experiment the number of Group B participants willing to submit their resumes to option 3 (Headhunter Websites) declined significantly from 15 to 9. Overall, these results suggest that an uncertain environment in cyberspace where identity theft is a significant factor can cause major shifts in behavior. These results also suggest that efforts by the FTC to go after identity thieves are worthwhile, though nothing presented here is offered as an approximation of a complete cost-benefit analysis [BEP04a].

4.5 Fall 2004 Experiments

Following the pilot experiments during the spring of 2004, we administered experiments to two additional test groups in the fall of 2004. The instructions for both groups were the same. Table 4 below shows the pooled results for fall 2004.

The main instructional difference is that we made the probability of being hired the same for all websites at 50% and thus the highest expected value was for participants to choose HW, ignoring the probabilities of being a victim of identity theft or being identified as a health risk. Compared with the results reported in Table 3, more participants in the fall experiments selected Headhunter Websites (HWs). The opportunity to purchase encryption protection was not present in the first week so most participants choose GEWs or EWs. In the second week, participants were allowed to purchase protection from identity theft and for their health records. Given the availability of protection, there was a pronounced shift away from GEWs towards EWs and HWs websites. Forty-five out of fifty participants in the second week chose to encrypt their resumes and 15 of 29 participants chose to encrypt their health information. In the third week, the pseudo news event was the passage of HIPAA, which correlated with a shift towards HWs at the expense of EWs and only 8 of 38 participants elected to pay money to protect their health records. In the last week, the pseudo news event was that the frequency and cost of identity theft were decreased because of (1) increased criminal penalties for identity thieves and (2) that the FTC had developed tracking software that increased the probability of catching the identity thieves. The impact of a safer environment for submitting PII was a virtual abandonment of websites other than those for HWs, which offered the highest expected values of positive payoffs. Of the 51 participants in the fourth week, 46 selected HWs. The data suggest that

online choices made by job seekers were significantly affected by the risk of identity theft and unauthorized use of health information.

Table 4: Website and Protection Choice Frequencies

		GEW	EW	HW	HOME		Totals
Experiment 1							
	Group	15	27	10	0		52
	Protection Encrypt Resume	n/a	n/a	n/a	n/a		21
	Protection Encrypt Health Info.	n/a	n/a	n/a	n/a		
Experiment 2							
	Group	1	21	29	0		50
	Protection Encrypt Resume	1	19	26	n/a		45
	Protection Encrypt Health Info.	n/a	n/a	15	n/a		
Experiment 3							
	Group	0	13	38	0		51
	Protection	0	12	37	n/a		49
	Protection Encrypt Health Info.			8			
Experiment 4							
	Group	0	5	46	0		51
	Protection Encrypt Resume	0	3	39	n/a		n.a.
	Protection Encrypt Health Info.			6			

5 Summary and Future Work

In this paper we approached the exploration of consumer privacy concerns in a unique and innovative manner. We applied experimental economics methods to a scenario of job seekers using the Internet to search for employment. In the process, the job seekers made decisions that affected both their privacy and their hiring potential. We discovered that game participants reacted in expected ways when confronted with realistic combinations of benefits on the one hand and risks and uncertainties on the other that are characteristic of the Internet. Repetitive experiments of this kind would permit the detailed quantification of user responses to changes in Internet risks (resulting from any source, including government policies and/or commercially provided technology). This methodology provides the opportunity for construction of "consumer demand" schedules for privacy enhancing technology and policies and can allow detailed cost-benefit analyses of various recently passed legislation such as the Gramm-Leach-Bliley Act,

HIPAA regulations, and FTC initiatives. The results of our preliminary experiments indicate that Internet users are willing to pay hefty sums to increase security. In like fashion, when the environment becomes more risky (Experiment 4), pronounced changes in behavior occurred. Our experiment involved job search, but experimental economic methodology may be applied to purchasing decisions, online banking, marketing research, and many other scenarios.

The results and observations of the pilot experiment described herein will be considered as we design the final set of experiments that will be electronically automated. These future experiments will rely on a simulated Internet environment that consists of several websites with which the participants will interact. Participants will surf the simulated web environment as they try and fulfill a particular task. Similar to the actual Internet, the simulated Internet environment will cause the participant to be vulnerable to computer viruses, identity theft, hackers, etc. As a result, the participants will make decisions that will impact their privacy as well as their success in fulfilling the websurfing tasks. Monetary incentives will be used to ensure that participants are dedicated to trying to succeed in their task.

6 References

[ACR99]M.S. Ackerman, L.F. Cranor and J. Reagle, "Privacy in e-commerce: examining user scenarios and privacy preferences," *Proceedings of the First ACM Conference on Electronic Commerce,* pp.1–8, 1999.

[AE01]A.I. Antón and J.B. Earp, "Strategies for developing policies and requirements for secure electronic commerce systems," in *E-Commerce Security and Privacy*, edited by Anup K. Ghosh, Kluwer Academic Publishers, pp. 29-46, 2001.

[AJB98] P.S. Alexander, T.M. Jones and S.R. Brown, "Attitudes toward information privacy: differences among and between faculty and students," *Proceedings of the Association for Information Systems Conference*, pp. 48-50, 1998.

[BEP00] D.L. Baumer, J.B. Earp, F.C. Payton, "Privacy of Medical Records: IT Implications of HIPAA." Vol. 30(4), pp.40-47, 2000.

[BEP04] D.L. Baumer, J.B. Earp, and J.C. Poindexter, "Internet Privacy Law: A Comparison between the United States and the European Union." Forthcoming *Computers and Security*.

[BEP04a] D.L. Baumer, J.B. Earp, and J.C. Poindexter, "Meaningful and Meaningless Choices in Cyberspace." Forthcoming, *Journal of Internet Law*.

[BE62] G.B. Becker, "Irrational Behavior and Economic Theory." *Journal of Political Economy*. Vol. 70, pp. 1-13, 1962.

[Bel97]V. Bellotti, "Design for privacy in multimedia computing and communications environments," in *Technology and Privacy: The New Landscape*, Philip E. Agre and Marc Rotenberg (Eds). Cambridge: MIT Press, pp.63-98, 1997.

[Bro95] Brown, Paul M. (1995) "Learning from Experience, Reference Points, and decision Costs," Journal of Economic Behavior and Organization, 27:3.

[CA99] M. Culnan and P. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation," *Organization Science*, vol. 10, pp.104-115, 1999.

[Cla99] R. Clarke, "Internet privacy concerns confirm the case for intervention," *Communications of the ACM*, (42), pp.60-67, 1999.

[EAA05] J.B. Earp, A.I. Antón, L. Aiman-Smith and W. Stufflebeam "Examining Internet privacy policies in the context of user privacy values," *IEEE Transactions on Engineering Management*, forthcoming in 2005.

[EB03] J.B. Earp and D. Baumer, "Innovative web use to learn about user behavior and online privacy." *Communications of the ACM*, vol. 46, no. 4, pp.81-83, April 2003.

[EPB04] J.B. Earp, J.C. Poindexter, and D.L. Baumer, "Modeling Privacy Values with Experimental Economics," paper presented to the Workshop for Privacy in an Electronic Society, Oct. 2004.

[FV04] P. Fevrier and M. Visser, "A Study of Consumer Behavior Using Laboratory Data." Vol. 7, pp. 93-114, 2004.

[FTC00]Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress, 2000.

[FHSS94] Forsythe, R., J.L. Horowitz, N.E. Savin, and M. Sefton, "Fairness in Simple Bargaining Experiments," Games and Bargaining Behavior, 6, pp. 347-369, 1994.

[FK99] S. Furnell and T. Karweni, "Security implications of electronic commerce: a survey of users and businesses," Internet Research, vol. 9, pp. 372 – 382, 1999

[MSB00]S.J. Milberg, J.H. Smith and S.J. Burke, "Information privacy: corporate management and national regulation," *Organization Science*, vol.11, no.1, pp.35-37, 2000.

[Nash51] J. Nash, Jr., "Noncooperative Games," *Annals of Mathematics,* Vol. 54, pp. 286-295, 1951.

[Rau02] A.P. Raul, Privacy and the Digital State: Balancing Public Information and Personal Privacy, Boston, MA: Kluwer, 2002.

[Sav71]Savage, Leonard J. -1971-"Elicitation of Personal Probabilities and Expectations," JASA 46:4.

[SGB01]S. Spiekermann, J. Grossklags and B. Berendt, "E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior," *Proceedings of the 3rd ACM Conference on Electronic Commerce*, pp.38–47, 2001.

[Sho91] Shoemaker, Paul -1991- "Choices Involving Uncertain Probabilities: Tests of Generalized Utility Models," Journal of Economic Behavior and Organization, 16:3.

[Sip97] Sippel, R. – 1997 – An Experiment on the Pure Theory of Consumer's Behavior," Economic Journal, 107:444.

[SMB96] J. Smith, S. Milberg and S. Burke, "Information privacy: measuring individuals'concerns about organizational practices," *MIS Quarterly*, vol. 20, pp.167–196, 1996.

[Smi02] Vernon Smith, "What is Experimental Economics?" ICES, http://www.ices-gmu.org/article.php?id=368.

[Smi03] Smith, Vernon, "Constructivist and Ecological Rationality in Economics," a version of Smith's address to the Nobel Committee in 2002, http://www.law.gmu.edu/////////currnews/smith-lecture.html.

[SS02] K.A. Stewart and A.H. Segars, "An empirical examination of the concern for information privacy instrument," *Information Systems Research*, vol. 13, pp.36-49, 2002.

[SU05] Sullivan, Bob, ID Theft again Tops List of the FTC Complaints, http://www.msnbc.msn.com/id/6891556/, Feb., 2005.

[HW91, 94, 96, 98]]Louis Harris and Associates and A. F. Westin. *Harris-Equifax User Privacy Surveys*. Atlanta, Ga. Equifax Inc. 1991, 1994, 1996, 1998.