The Economics of Peace and Security Journal, ISSN 1749-852X
© www.epsjournal.org.uk – Vol. 5, No. 1 (2010)

Preferences for privacy and security: an experimental investigation

C. Jill Stowe, *Kate Krause*, and *Janie M. Chermak*

In the United States, the events of 11 September 2001 led to increased efforts to reduce the risk of another terrorist attack. One way to reduce such a risk is to increase surveillance and other security measures. Increasing surveillance, however, reduces privacy. In determining optimal policy, policymakers must weigh the value of a reduced risk of a catastrophic event against the value of privacy. While the debate is not new, interest in the tradeoffs between security measures and individual privacy has grown.[1] We conducted experiments in which participants chose between these two commodities. We use participants' choices, as well as demographic and other information, to analyze the relative importance of privacy and security across a heterogeneous group of university students.

We assume that there exists a tradeoff between privacy and security: giving up some degree of privacy improves security.[2, 3] While the decision as to the appropriate balance is collective, our focus is on the privacy loss to the individual. We do not account for the governing authority's costs and benefits due to increased security.[4]

We asked undergraduate and graduate students to choose among various levels of surveillance in return for reduced risk of loss. Our participants are heterogeneous both in demographics and response, ranging from 19 to 41 years of age, with an average age of almost 22. About 40 percent identified themselves as Caucasian, 32 percent as Hispanic, 6 percent as Native American, 10 percent as Asian, and 2 percent as African American. Like most convenience samples, this pool is younger than the general population and differs from both the typical sample of largely Caucasian, 18-22 year-old college students and the U.S. population generally.[5] Most choose to give up some privacy in exchange for reduced risk but are unwilling to submit to the most invasive measures in return for a very low risk of loss. A nonnegligible percentage of the participants' decisions reflect preferences that are either high privacy (HP) or high security (HS). Participants whose decisions take relatively extreme values are distinguishable from the participants with more moderate preferences both in the ways they respond to feedback and in some of their demographic characteristics.

We begin with a theoretical model explaining the choice of optimal levels of surveillance and privacy and then describe the experimental design. Then, we present regression models and results, and a summary concludes the article.

Theoretical model

We model individuals as voting on allowable surveillance levels. Higher surveillance levels reduce the risk of a catastrophic event, like a terrorist attack; however, to reduce that risk, individuals bear a loss of utility due to invasion of personal privacy.[6] In our model, individuals have preferences over net wealth. Net wealth is determined by the original wealth endowment, utility gained from the provided level of security, disutility from the corresponding privacy invasions, and the probabilistic occurrence of a catastrophic event. Individuals vote for optimal levels of surveillance and hence the corresponding optimal levels of privacy loss. The prevailing surveillance level is determined by a specified voting rule, such as majority vote. We assume that individuals do not know the choices of other members of society. Consequently, each person selects the surveillance level that maximizes his or her expected utility over net wealth, conditional on what they expect others to do. Thus, there are two types of uncertainty: first, there is uncertainty regarding the votes of other members of society; second, there is uncertainty regarding the occurrence of a catastrophic event.

We conducted experiments in which participants chose between privacy and security. A nonnegligible percentage of the participants' decisions reflect preferences that are either high privacy (HP) or high security (HS). Participants whose decisions take relatively extreme values are distinguishable from the participants with more moderate preferences both in the ways they respond to feedback and in some of their demographic characteristics.

Each individual's optimal surveillance level choice equates the marginal cost of that privacy invasion level to the marginal benefit of increased security, plus a term incorporating income elasticity of utility as well as the inherent riskiness of providing security. Security, even if provided at high levels, cannot fully protect against a catastrophic event; as a result, individuals choose higher levels of surveillance and submit to more privacy invasions when there is a probabilistic resolution of a disastrous event.[7]

Individual differences in preferences over money and security and in sensitivity to privacy invasions yield different optimal choices. High privacy decisions are consistent with high marginal costs of additional privacy invasions, whereas high security decisions are consistent with greater marginal utility from higher levels of security relative to the cost of privacy invasions. Differences in the individual cost and benefit functions explain why high privacy participants optimally vote for fewer privacy invasions and high security participants allow more privacy invasions.

If preferences change over time, optimal decisions will likewise change. For example, a person may not have well-formed preferences over risks not personally experienced. If the risky event were to occur, that person may adjust his or her preferences between security and privacy. In our experiment, we observe some participants choosing different privacy loss levels after observing a negative outcome,

suggesting that people do adjust their decisions based on experience.

Experimental design

Our participants were asked to imagine themselves in a hypothetical scenario. We presented participants with choices between sacrificing some degree of privacy in return for increased security. Because we could not subject participants to realistic privacy invasions, nor could we subject our participants to acts of crime or terror, we used financial loss and gain to give saliency to their choices. Thus, a violation of privacy cost the participant a specified amount of experimental earnings, while realization of the threat resulted in a complete loss of all earnings. In this sense, the investigation resembled an insurance market. Participants could sacrifice a specified amount of earnings in exchange for a reduced probability of complete loss.

Other features of the experiment distinguish it from an insurance market. Ex ante payment did not secure compensation in the event of loss; it only reduced the chance of loss. In addition, decisions about the appropriate tradeoff between security and privacy are necessarily collective. A policy that subjects citizens to various security-enhancing methods must apply to all. Therefore in this investigation, groups of participants voted on the degree to which they were willing to accept privacy invasions in return for more security.

Because we characterized privacy invasions as a cost, a necessary first step was to determine dollar values of various privacy invasions so that those values, in an ordinal sense, were aligned with participants' perceptions of those invasions. Thus, our design has two parts. In the first stage, we asked 46 undergraduate students recruited from three lower-division undergraduate economics courses to rate several privacy invasions by the degree to which that invasion was perceived as intrusive. That first stage of our design informed the second stage. In the second stage, a different group of students, randomly and anonymously assigned to groups of five, voted on the level of surveillance their group would tolerate in exchange for different levels of security.

Stage one

We investigated students' reactions to a number of possible steps that a governing authority might take by asking students to complete a Likert-scale survey. Students were presented with a list of thirteen different surveillance practices and a brief explanation of each practice. They then rated those practices on a scale from one to five, where five indicated a practice perceived as most intrusive.[8]

We used Stage One results to rank each security measure by the extent to which most students would be offended and to identify those practices for which the perception of invasiveness was most uniform. In the second stage, we included those invasions for which student responses were most consistent and allowed the greatest degree of spread between the least invasive measure and the most. Stage Two participants completed the same instrument after completing the experiment. Their responses are similar to the responses of the Stage One participants as shown in the last column of Table S1 (online supplemental material).

Table 1: Costs and benefits of each choice

Step	*Cumulative cost (in tokens)*	*Probability of complete loss*	*Expected value*
No measures taken	0	0.80	6.00
Security camera	2	0.50	14.00
Drug test	5	0.35	16.25
Body search	9	0.22	16.38
Email, internet monitoring	14	0.12	14.08
Property search	20	0.05	9.50
Wiretap	27	0.02	2.94

From least intrusive to most, the six practices that we selected were security camera monitoring, drug test, body search, email or internet monitoring, property search, and wiretapping. Both the initial Stage One participants and the Stage Two participants were drawn from a university student body, a population whose experiences with these measures may be quite different from the experiences of the adult population generally.

Stage two

The second stage of our investigation addresses our primary interest. We recruited 85 undergraduate and graduate students, none of whom participated in the first stage. After they completed the experiment, Stage Two participants provided demographic information, completed the Stage One instrument, and responded to the following question: "On a scale of one (1) to five (5), which number best describes your attitude?" One (1) is equivalent to: "Reduced privacy doesn't bother me: I am not doing anything wrong so I don't have anything to hide." Five (5) is equivalent to: "Reduced privacy bothers me. It imposes on my rights and allows governmental agencies too much access to my personal information." Responses were fairly symmetric: 40 percent of our sample chose the middle ranking, a 3, in response to this question, 13 percent chose 1, the lowest ranking, and 12 percent chose 5, the highest. Sixteen percent leaned toward not being bothered, choosing 2, and 19 percent leaned toward being bothered, choosing 4.[9]

Second stage participants were asked to imagine themselves in a hypothetical

Table 2: Absolute and relative frequencies of privacy choices

Privacy choice (up through and including)	*R1 Freq. n=85*	*R2 Freq. n=85*	*R3 Freq. n=85*	*R4 Freq. n=40*	*All Freq. n=295*
0: None	1 (1.2)	4 (4.7)	5 (5.9)	3 (7.5)	13 (4.4)
1: Security cam.	13 (15.3)	9 (10.6)	11 (12.9)	5 (12.5)	38 (12.9)
2: Drug test	20 (23.6)	20 (23.6)	15 (17.6)	5 (12.5)	60 (20.3)
3: Body search	36 (42.4)	36 (42.4)	35 (41.2)	15 (37.5)	122 (41.4)
4: E-mail monit.	7 (8.2)	10 (11.8)	9 (11.6)	7 (17.5)	33 (11.2)
5: Property search	4 (4.7)	3 (3.5)	4 (4.7)	5 (12.5)	16 (5.4)
6: Wiretapping	4 (4.7)	3 (3.5)	6 (7.1)	0 (0)	13 (4.4)
Average (s.d.)	**2.7 (1.3)**	**2.7 (1.3)**	**2.8 (1.5)**	**2.8 (1.4)**	**2.8 (1.3)**

Group divisions (see text for explanation):
- 0 and 1 => HP (high privacy)
- 0 through 4 => Base
- 0 through 6 => HS (high security)

situation that would lead to a complete loss of all earnings with an 80 percent probability if no security-enhancing steps were taken. That probability would be reduced with increasingly invasive security measures. Participants were asked to vote on the proposed security measures that their group would endure. Security measures were constrained to be cumulative in the order presented, so that a participant who voted to accept one security measure was accepting all lower-cost measures as well. Participants were given an endowment of 30 tokens at the beginning of each round. Each token was worth 40 cents, so that the participants' starting endowment was USD12. Table 1 summarizes the cumulative cost of taking each step and the reduction in the probability of loss associated with each level of security.[10] While it can be clearly seen from Table 1 that accepting security measures through the level of a body search maximizes expected return, this information was not explicitly provided to participants.

Once all members of a group made their decisions, the experimenters determined the highest level of security accepted by at least three members of the group. A draw from a bingo cage, done in full view of all participants, determined whether or not the loss occurred. Rounds were repeated with no rollover of earnings. Group membership changed with each round and the number of rounds was not pre-announced. In five separate administrations of the experiment, three groups completed three rounds and two groups completed four rounds.

Earnings

Only one round of the hypothetical scenario was chosen for payment. In addition to earnings from the decisions and outcomes, participants were given a USD5 participation fee. Earnings ranged from USD5 to USD15 and averaged USD12.60.

Model and results

The frequency of participants' choices among the seven security/privacy tradeoff levels is presented in Table 2. Body Search (which includes the lower-ranked surveillance methods of Security Camera and Drug Test) is the mode across all rounds. Assigning a numerical value from zero (none) to six (wiretapping) for the seven choices, respectively, the mean response is 2.8 across all rounds (between Drug Test and Body Search), with a standard deviation of 1.3.

We assume that each participant chooses the level of surveillance which he or she is willing to tolerate in order to approximately maximize utility according to

$$(1) \qquad U(\text{alternative } j) = \beta_j \mathbf{x}_j + \epsilon_j \qquad (j = 0, 1, ..., m)$$

where β_j is a vector of coefficients and $\mathbf{x}_j$ is a vector of characteristics that capture participants' perceptions of the benefits and costs of increased surveillance. The observed choice = j if U (alternative j) > U (alternative k) $\forall\, j \neq k$. The probability a participant makes choice j then is

$$(2) \qquad \text{Prob}[\text{choice } j] = \frac{\exp(\beta_j' \mathbf{x}_i)}{\sum_{k=1}^{m} \exp(\beta_k' \mathbf{x}_i)}.$$

Incorporating survey and experimental data into equation (2) allows us to consider the following questions:

1. Are observable characteristics correlated with participants' privacy/security preferences?
2. What distinguishes participants who prefer high security from those who prefer high privacy?
3. How do participants' choices respond to a loss event, either to the participant or to others in the experiment?
4. Do participants who had made high security decisions in the first round respond to loss events in the same way as those whose early decisions had reflected high privacy preferences?

The size of the data set prevents modeling the probability of each of the seven

Table 3A: Round one results

Model 1	*High privacy*			*High security*			*Mean*
Variable	*Coeff.*	*s.e.*	*p-value*	*Coeff.*	*s.e.*	*p-value*	*value*
Experience and attitude							
Attitude	0.91[a]	0.40	0.02	-0.28	0.44	0.53	3.00
Average rank	0.94[c]	0.61	0.12	-1.96[a]	0.84	0.02	2.88
Percentage yes	5.61[a]	2.89	0.05	5.11	3.73	0.17	0.40
Financial check	-0.83	1.10	0.44	-0.48	1.40	0.73	0.27
Sobriety test	-1.65[b]	0.97	0.09	-1.23	1.23	0.31	0.31
Demographics							
Age	—	—	—	—	—	—	21.46
Female	—	—	—	—	—	—	0.60
International	—	—	—	—	—	—	0.05
Non-Anglo	—	—	—	—	—	—	0.61
Junior/senior	—	—	—	—	—	—	0.25
Graduate	—	—	—	—	—	—	0.16
Constant	-9.26[a]	2.47	0.00	1.69	2.34	0.47	

Notes: LL = -44.8; restricted LL = -63.0; chi-sq. = 36.3; pseudo-R^2 = 0.29
[a] = stat. sign. at 5%; [b] = at 10%; [c] = at 15%.

	Actual			
Predicted	*Base*	*HP*	*HS*	*Total*
Base	60	3	0	63
HP	8	6	0	14
HS	5	0	3	8
Total	73	9	3	85

individual security choice levels, so we aggregate responses into three groups: High Privacy (HP), Base, and High Security (HS). A Base choice is the mean plus or minus one standard deviation, rounded to the nearest whole number. Based on this criterion, we categorize decisions to accept None or surveillance by Security Camera only as reflecting HP preferences. Approximately 17 percent of all decisions made in the experiment meet this criterion. The Base group includes choices to accept surveillance practices up to and including Drug Test, the Body Search or Email/internet Monitoring, which accounts for more than 75 percent of the responses. The remaining responses reflect HS preferences and include the most costly levels of security in terms of privacy loss. These three designations are the dependent variables in our analysis.

Explanatory variables fall into three categories: (1) experience and attitudinal; (2) demographic, and (3) experimental (which reflect choices and outcomes of previous rounds). Experience and attitudinal variables capture pre-experiment attitudes and experiences. PERCENT YES is the percentage of security events that a participant had experienced. AVERAGE RANK is the participant's average ranking of invasiveness of the thirteen survey items. ATTITUDE is the participant's ranking of the extent to which reduced privacy bothered them (where a 5 indicated that reduced privacy "bothers me"). Thus higher scores on AVERAGE RANK and on ATTITUDE indicate a relative preference for privacy. Finally, we considered experience with each of the 13 privacy issue variables, but include only those two variables which were statistically significantly (at 15 percent) associated with either HS or HP decisions in our initial model.[11]

Demographic variables include AGE, education (binary variables for JR/SR and GRAD), ethnicity (NON-ANGLO), gender (FEMALE), and international student status (INTERNATIONAL). These capture cultural and other systematic differences (if any) that might influence participants' tastes for privacy and security.

Experimental variables allow us to test a participant's response to prior round outcomes. A participant's choice in round one provides a baseline, pre-feedback prior about security and privacy (R1 CHOICE). We investigate whether a good or bad outcome in one round influences a participant's choice in the next round by including the following variables: the participant's outcome in the previous round (OUTCOME LAST), the percentage of groups that experienced a loss in the previous round (PERCENT INCIDENT LAG), the sum over all previous rounds of losses that happened to the participant (SUM INCIDENT), and the participant's group security level from the previous round (GROUP LAST).[12]

Round one models

To distinguish the influence of pre-experiment experience, attitudes, and demographics from experience in the experiment, we estimate two separate sets of multinomial logit models. Models 1 and 2 employ only round one data (n=85). This provides a baseline to which we can compare the impact of experiment outcomes. In Model 1, we include only experience and attitudinal variables. Model 2 adds the demographic variables. The results are presented in Tables 3A and 3B (statistically significant variables are indicated with a superscript), with the actual versus predicted values provided in the last row of the tables.[13]

Table 3B: Round one results

Model 2	*High privacy*			*High security*		
Variable	*Coeff.*	*s.e.*	*p-value*	*Coeff.*	*s.e.*	*p-value*
Experience and attitude						
Attitude	0.95[a]	0.56	0.00	-1.70[a]	0.88	0.05
Average rank	0.90	0.79	0.25	-2.33[b]	1.33	0.08
Percentage yes	7.13[a]	3.34	0.03	11.22[b]	6.30	0.07
Financial check	-2.11	1.51	0.16	-6.12[c]	3.84	0.11
Sobriety test	-1.28	1.01	0.20	-3.62[c]	2.43	0.14
Demographics						
Age	0.20[c]	0.13	0.11	0.22	0.26	0.39
Female	0.43	0.89	0.63	-3.72[a]	1.89	0.05
International	-25.30	>100	1.00	6.39[b]	3.64	0.07
Non-Anglo	-1.24[c]	0.86	0.15	-1.68	1.21	0.17
Junior/senior	-0.32	0.98	0.75	-1.94	1.66	0.24
Graduate	-1.24	1.79	0.49	2.28	3.06	0.46
Constant	-13.56[a]	4.50	0.00	2.68	6.10	0.66

Notes: LL = -33.2; restricted LL = -63.0; chi-sq. = 59.5; pseudo-R^2 = 0.47
[a] = stat. sign. at 5%; [b] = at 10%; [c] = at 15%.

	Actual			
Predicted	*Base*	*HP*	*HS*	*Total*
Base	62	1	0	63
HP	8	6	0	14
HS	2	0	6	8
Total	72	7	6	85

Participants who indicated on their surveys that reduced privacy bothers them generally (ATTITUDE), as well as specifically in the context of the thirteen surveillance practices (AVERAGE RANK), and who had relatively more experiences with those practices (PERCENT YES), were more likely to make an HP choice than the Base choice. Participants who had experienced a sobriety test were less likely to make an HP choice. Participants whose decisions reflected an HP preference assigned higher invasiveness scores to the thirteen surveillance practices and those whose decisions reflected an HS preference assigned lower invasiveness scores to the items.

Adding demographic variables in Model 2 only moderately changed the results for the attitude and experience variables. Frequency of experience with the named surveillance practices continues to explain HP decisions, but, somewhat puzzling, is also positively associated with HS decisions. However, specific experience with financial record disclosure and sobriety tests was negatively associated with a HS decision. It appears that for some, having experienced a privacy violation made them more tolerant of violations in the future (HS) while for others the experience made them less tolerant (HP), indicating different people will respond to the same stimulus in different ways.

Table 4: Round one model marginal effects (evaluated at the mean)

	Model 1		*Model 2*	
Variable	*HP*	*HS*	*HP*	*HS*
Experience and attitude				
Attitude	0.07	—	0.02	-0.01
Average rank	0.08	-0.01	—	-0.01
Percentage yes	0.43	—	0.15	0.04
Financial check	—	—	—	-0.02
Sobriety test	-0.13	—	—	-0.01
Demographics				
Age	—	—	0.01	—
Female	—	—	—	-0.01
Non-Anglo	—	—	-0.03	—
International	—	—	—	0.02

Of the demographic variables, older participants were more likely to choose HP and non-Anglo participants were less likely to choose HP. Women were less likely to choose HS while international students were more likely to choose HS, but this result must be interpreted with caution given the relatively small number of international students in this data set.

Table 4 presents the marginal effects, estimated at the sample means of the RHS variables. The marginal effects provide the changes in the probability that an individual will choose HP (or HS) over Base, for a one-unit change in the variable.

In Round 1, participants tended to make choices that were generally consistent with their pre-experiment attitude toward privacy. Experience with security measures cuts both ways, perhaps because of differences in how those measures were executed.

Feedback models

We now turn to the models that incorporate immediate feedback from the

Table 5: Immediate feedback model marginal effects

	Model 3		*Model 4*		*Model 5*	
Variable	*HP*	*HS*	*HP*	*HS*	*HP*	*HS*
Experience and attitude						
Attitude	—	-0.01	—	-0.01	-0.04	—
Average rank	—	-0.07	—	-0.04	—	-0.01
Percentage yes	0.43	—	-0.44	—	-0.42	—
Financial check	—	—	—	-0.07	—	-0.01
Demographics						
Age	—	—	0.02	—	0.02	—
Female	—	—	—	-0.02	—	-0.01
Non-Anglo	—	—	-0.09	-0.01	-0.04	—
Junior/senior	—	—	-0.32	—	-0.28	—
Graduate	—	—	—	0.07	—	0.01
Experimental						
R1 choice	—	—	—	—	-0.66	0.001
Outcome last	—	—	—	—	—	0.002
Sum incident	—	—	—	—	0.16	—
Group last	—	—	—	—	—	0.001
Constant and time						
Constant	-0.74	0.08	-0.43	0.15	—	—
Round 4	—	—	—	0.02	—	—

experiments. We lose all first round observations when we lag variables, leaving us with 210 observations. Model 3 replicates Model 1, but with data from later rounds of the experiment and binary round variables. Similarly, Model 4 replicates Model 2 with this data and binary round variables. While the magnitudes of the coefficients have changed, we observe many of the same patterns. Older participants continue to choose HP, and women continue to avoid choosing HS. In the new data, though, pre-experiment attitude no longer predicts HP choices, and experience with the thirteen security measures is negatively associated with HP choices. Model 5 incorporates the experimental variables (feedback) and suggests that pre-experiment attitudes and experience may be supplanted by the outcomes of earlier experimental rounds. Results are provided in Table A1, appended to this article.[14]

The number of statistically significant experience and attitude variables related to HS declines when immediate feedback is included: attitude and experience are partially supplanted by immediate experience. Relative to Model 2, fewer demographic variables explain HS choices, but having experienced a loss in a prior round and having higher security imposed in a prior round are associated with an increased likelihood of a HS choice. Thus, current events appear to influence privacy/security tradeoff preferences. The tendency to make HP choices appears less sensitive to inclusion of feedback variables. Only the cumulative count of losses in prior rounds is statistically significantly associated with the likelihood of choosing HP, and its influence is to increase HP choices.

First round choices strongly predict choices in subsequent rounds. The likelihood that a participant will display HP preferences increases as the overall faring of the experimental group in the last periods worsens (SUM INCIDENT), while the likelihood of displaying HS preferences is positively associated with a loss that is personally experienced by the participant, as well as with the level of security chosen by his or her group in the previous period (OUTCOME LAG and GROUP LAST).

The marginal effects for statistically significant variables from Models 3, 4, and 5 are presented in Table 5. The marginal effects for HP are larger than those in Models 1 and 2, while the magnitude of marginal effects for HS are relatively small in magnitude. Current events affect participants' choices, and there is a distinct difference in how those events lead to HP or HS choices. Pre-experiment experience and a pro-privacy attitude, when immediate experimental feedback is included in the model, reduce the probability of making an HP choice in the later rounds. Regardless of the specification, older participants tend toward HP preferences. The decision to make an HP choice is impacted by the community-centric variable—what happened to the entire experimental group last period—rather than by the individual-centric variables. In this case, a one-percent increase in loss in the last period increased the probability of a HP choice by 16 percent. This counter-intuitive result may reflect the tendency for participants to apply a heuristic assessment of risk: if a terrorist attack happens on a given day, another incident may seem highly unlikely on the following day.

HS participants appear much different from their HP counterparts. As in every other specification, being female reduces the probability of HS. This may at first seem at odds with other studies that find women are more risk averse than men, but in this context, there is more than one risk domain that must be considered. Other researchers have found that women's risk attitudes differ depending on the domain.[15] There is the security (and hence financial) risk, but there is also a personal risk associated with being subjected to invasive actions.

In contrast to the case for HP choices, the immediate feedback variables that impact the probability of HS are the individual-centric variables. What happened to me? What did my group do? An adverse own-group event increases the probability of HS.

Switching behavior after a loss

There were 50 instances in which a subject experienced a loss in a round prior to the last round of play.[16] Of those who experienced a loss, 21 switched their choice from the previous round. Among these switchers, the average privacy invasion chosen in the round leading to the loss was 2.81, whereas the average privacy invasion selected after the loss was 3.38. Thus, these individuals increased their tolerance for privacy invasions after suffering a loss.[17]

Switchers differed attitudinally and demographically. Switchers' response to the overall attitude question (where 5 indicated that privacy violations bothered the person) averaged 2.95, while non-switchers entered the experiment with more strongly-held preferences for privacy; their average ATTITUDE rank was 3.69.[18] Switchers are less sensitive to reduced privacy and so are more willing to submit to increasing privacy violations in exchange for risk reduction. Switchers also tended to be younger. The average age of the switchers is 21.2, while the average age of non-switchers is 23.0.[19] This is consistent with the positive correlation between age and pro-privacy attitude.

Summary and conclusions

We sought insight into people's preferences for privacy and security when an explicit tradeoff exists between the two. While most participants chose a moderate level of privacy in exchange for a moderate level of security, some made choices that were consistent with a very strong preference for security, and others made choices that were consistent with a very strong preference for privacy.

In response to the first two questions we pose, we find that older participants tended to make high privacy choices and women were less likely than men to choose high security measures. Non-Anglo participants were less likely to make high privacy choices; international students tended to make higher security choices. These suggest that policies intended to enhance security, at the expense of privacy, must be sensitive to the relative values that citizens of diverse backgrounds place on privacy and security.

We answer our third and fourth questions by investigating choices over multiple rounds, observing how choices change when a participant experiences a loss or when a participant observes others' loss. Other participants' losses were associated with high privacy choices, while high security choices were more likely after participants experienced a loss themselves. However, a participant's first round decision remained predictive even when controlling for loss experience.

We find evidence for diversity of preferences for security and privacy, and we find that this diversity is correlated with observable characteristics and pre-experiment experience with surveillance. But those preferences are not immutable. Experimental experience led some participants to change their decisions, although not in uniform ways. This suggests that the relative value that citizens place on security and privacy will change as circumstances change and as events unfold.

Notes

C. Jill Stowe, the corresponding author, is an Assistant Professor of Agricultural Economics, with a joint appointment to the Department of Economics, at the University of Kentucky, Lexington, KY, U.S.A. She may be reached at jill.stowe@uky.edu. **Kate Krause** is an Associate Professor of Economics at the University of New Mexico in Albuquerque, NM, U.S.A. She may be reached at kkrause@unm.edu. **Janie M. Chermak** is a Professor of Economics at the University of New Mexico in Albuquerque, NM, U.S.A. She may be reached at jchermak@unm.edu.

1. A search on LexisNexus Academic finds 121 references to "privacy security debate" in major U.S. and world publications between 16 September 2008 and 16 December 2008, of which 86 were in newspapers. In the prior 3 months, there were 134 references, with 100 of them in newspapers. See www.lexisnexis.com [last accessed 16 December 2008].

2. Both privacy and security are broad concepts, so it is important to clarify their definitions in the context of this article. The most accurate description of privacy for our purposes comes from Schoeman (1984), who described privacy as one's right to determine what information about oneself is communicated to others, one's degree of control over personal information, and who has sensory access to oneself, and a state or condition of limited access to oneself. These ideas are related to those found in Hirshleifer (1980), Stigler (1980), and Posner (1981). These authors consider privacy in both narrow and broad terms. Narrowly, privacy is the restriction or concealment of information (secrecy); broadly, privacy is freedom and autonomy from society, or the right to manage information about oneself. We adopt Baldwin's (1997) notion that security is a "low probability of damage to acquired values."

3. See Chandler (2009).

4. Lenard and Rubin (2006).

5. Compared to U.S. Census Statistics, our sample is younger and under-represents Caucasians and African Americans, while it over-represents Hispanics and Native Americans.

6. The formal model, including definitions and proofs, is available online as supplementary material. See www.epsjournal.org.uk, vol. 5, no. 1.

7. Figure S1 in the online supplementary materials illustrates this result.

8. The Stage One survey instrument is available in the online supplementary materials. Summary statistics of the results of this stage of the investigation are presented in Table S1.

9. Demographic detail and the distribution of responses to this attitude question are given in Table S2.

10. This information was presented to the participants in an expanded narrative. All experiment forms and instructions are available in the online supplementary materials.

11. The privacy issue variables were added one at a time to Model 1. If the additional variable was significant for either or both HP and HS it was kept; otherwise, it was dropped. In the case where the addition of a new privacy issue variable resulted in making an already included privacy issue variable insignificant, the variable which had the higher explanatory power was kept and the other was dropped.

12. Table S3 provides descriptive statistics for these prior-round variables.

13. The log-likelihood ratios indicate both models are a better fit than a restricted model with only a constant. Further, including demographic information in Model 2 provides better explanatory power than Model 1, as indicated by the log-likelihood ratio, as well as by the pseudo R-squared. Finally, the Wald statistic for the demographic variables is 11.11, implying rejecting the null of joint insignificance at the usual levels.

14. Again, Wald tests indicate the additional variables in Models 4 and 5 are jointly significant at the usual levels.

15. For example, Weber, Blais, and Betz (2002) find that women are more risk averse than men in four domains: financial decisions, health/safety, recreational, and ethical; however, women are not more risk averse than men in the domain of social risk. Fellner and Maciejovsky (2007) find that women are more risk averse than men when choosing between binary lotteries.

16. Three subjects experienced two losses, in rounds 2 and 3.

17. These means are different at about a 91% level of significance.

18. These averages are significantly different at a 97% level.

19. These values are significantly different at the 85% level.

References

Baldwin, D.A. 1997. "The Concept of Security." *Review of International Studies*. Vol. 23, pp. 5-26.

Chandler, J. 2009. "Privacy Versus National Security: Clarifying the Trade-Off," pp. 122-138 in I. Kerr, V. Steeves, and C. Lucock, eds. *Lessons from the Identity Trail: Anonymity, Privacy and Identification in a Networked Society*. New York: Oxford University Press.

Fellner, G. and B. Maciejovsky. 2007. "Risk Attitude and Market Behavior: Evidence from Experimental Asset Markets." *Journal of Economic Psychology*. Vol. 28, pp. 338-350.

Hirshleifer, J. 1980. "Privacy: Its Origin, Function, and Future." *Journal of Legal Studies*. Vol. 9, No. 4, pp. 649-664.

Lenard, T.M. and P.H. Rubin. 2006. "Much Ado About Notification." *Regulation*. Spring, pp. 44-50.

Posner, R.A. 1981. "The Economics of Privacy." *American Economic Review*. Vol. 71, No. 2, pp. 405-409.

Schoeman, F. 1984. "Privacy: Philosophical Dimensions of the Literature," pp. 1-33 in F. Schoeman, ed. *Philosophical Dimensions of Privacy: An Anthology*. New York: Cambridge University Press.

Stigler, G.J. 1980. "An Introduction to Privacy in Economics and Politics." *Journal of Legal Studies*. Vol. 9, No. 4, pp. 623-644.

Weber, E.U., A. Blais, and N.E. Betz. 2002. "A Domain-Specific Risk-Attitude Scale: Measuring Risk Perceptions and Risk Behaviors." *Journal of Behavioral Decision Making*. Vol. 15, Iss. 4, pp. 263-290.

Table A1: Immediate feedback results

Variable	*Model 3 High privacy Coeff*	*s.e.*	*p-value*	*Model 3 High security Coeff*	*s.e.*	*p-value*	*Model 4 High privacy Coeff*	*s.e.*	*p-value*	*Model 4 High security Coeff*	*s.e.*	*p-value*	*Model 5 High privacy Coeff*	*s.e.*	*p-value*	*Model 5 High security Coeff*	*s.e.*	*p-value*	*Mean*
—Experience and attitude—																			
Attitude	0.09	0.19	0.64	-0.43c	0.29	0.14	-0.22	0.24	0.35	-0.95a	0.42	0.02	-0.43c	0.28	0.12	-0.60	0.62	0.33	2.97
Average rank	0.27	0.31	0.39	-2.26a	0.55	0.00	0.27	0.37	0.46	-2.89a	0.77	0.00	0.30	0.41	0.46	-4.96a	1.70	0.01	2.87
Percent yes	-2.89a	1.39	0.04	0.03	2.36	0.99	-3.78a	1.56	0.02	1.29	2.97	0.66	-4.56a	1.76	0.01	4.50	4.46	0.31	0.40
Financial check	0.11	0.60	0.86	-1.39	1.05	0.18	-0.19	0.83	0.81	-4.96a	2.02	0.01	0.05	0.87	0.95	-9.48a	4.54	0.04	0.26
Sobriety test	0.10	0.44	0.82	0.36	0.63	0.57	0.26	0.52	0.62	0.34	0.85	0.69	0.67	0.59	0.26	-0.30	0.99	0.76	0.31
—Demographics—																			
Age	—	—	—	—	—	—	0.21a	0.09	0.02	-0.08	0.18	0.65	0.21a	0.11	0.05	-0.25	0.26	0.33	21.15
Female	—	—	—	—	—	—	=0.42	0.48	0.38	-1.32b	0.77	0.08	-0.47	0.51	0.36	-1.95b	1.05	0.07	0.60
International	—	—	—	—	—	—	-0.53	1.28	0.68	1.99	1.72	0.25	0.43	1.50	0.78	-0.77	2.81	0.78	0.05
Non-Anglo	—	—	—	—	—	—	-0.79a	0.38	0.04	-1.09a	0.54	0.04	-0.81b	0.42	0.06	-0.58	0.60	0.33	0.63
Junior/senior	—	—	—	—	—	—	-2.81b	0.85	0.04	-0.37	0.88	0.68	-3.02a	0.91	0.00	0.13	1.18	0.91	0.25
Graduate	—	—	—	—	—	—	-1.52	1.17	0.19	4.41a	1.71	0.01	-1.71	1.54	0.27	8.15a	3.52	0.02	0.13
—Experimental—																			
R1 choice	—	—	—	—	—	—	—	—	—	—	—	—	-0.66a	0.28	0.02	1.35a	0.62	0.03	2.75
Outcome last	—	—	—	—	—	—	—	—	—	—	—	—	-0.46	0.67	0.49	2.01b	1.10	0.07	0.24
Percent incident last	—	—	—	—	—	—	—	—	—	—	—	—	-1.07	0.76	0.16	-0.60	1.47	0.68	0.45
Sum incident	—	—	—	—	—	—	—	—	—	—	—	—	1.75a	0.87	0.04	1.77	1.83	0.34	0.81
Group last	—	—	—	—	—	—	—	—	—	—	—	—	-0.43	0.30	0.16	0.98b	0.59	0.09	2.60
—Constant and time periods—																			
Constant	-1.70c	1.09	0.12	4.38a	1.64	0.01	-3.58b	2.14	0.09	9.69a	4.3	0.02	-0.44	2.65	0.87	7.85	5.93	0.18	
Round 3	0.32	0.42	0.45	0.84	0.65	0.19	0.38	0.46	0.40	1.03	0.72	0.16	-0.32	0.61	0.59	-0.17	1.33	0.90	0.40
Round 4	0.43	0.52	0.41	0.93	0.75	0.21	0.69	0.56	0.22	140b	0.84	0.09	-0.72	0.94	0.44	0.55	1.94	0.77	0.19

LL = -135.5; restricted LL = -161.7
chi-sq. = 52.5; pseudo-R^2 = 0.162

	Actual			
Predicted	Base	HP	HS	Total
Base	147	2	3	152
HP	35	0	2	37
HS	14	0	7	21
Total	196	2	12	210

LL = - 115; restricted LL = -161.7
chi-sq. = 93.38; pseudo-R^2 = 0.29

	Actual			
Predicted	Base	HP	HS	Total
Base	148	1	3	152
HP	26	10	1	37
HS	11	0	10	21
Total	185	11	14	210

LL = -101; restricted LL = -161.7
chi-sq. = 120.6; pseudo-R^2 = 0.37

	Actual			
Predicted	Base	HP	HS	Total
Base	146	5	1	152
HP	24	13	0	37
HS	8	1	12	21
Total	178	19	13	210

Notes: a = stat. sign. at the 5% level; b = at the 10% level; c = at the 15% level.