The Economics of Peace and Security Journal, ISSN 1749-852X

Online supplement to Vol. 5, No. 1 (2010)

Online supplementary materials for

Stowe, C. Jill, Kate Krause, and Janie M. Chermak. "Preferences for privacy and security: an empirical investigation." *Economics of Peace and Security Journal*. Vol. 5, No. 1 (2010).

1. Table S1: Results of rankings of surveillance measures
2. Table S2: Participant characteristics: demographics and attitude, n = 85
3. Table S3: Experimental variables descriptive statistics
4. Supplementary material: detailed version of the theoretical model with proofs
5. Figure S1: Optimal level of privacy invasions without and with probabilistic resolution of a catastrophic event ($p^*_{certain}$ and p^*_{risk}).
6. Stage one survey instrument
7. Stage two survey
8. Narrative instructions for stage two and reporting form

Preferences for privacy and security: an experimental investigation

Supplementary Tables

Table S1: Results of Rankings of Surveillance Measures

	Stage One Participants		Stage Two Participants	
	Mean (Std Dev)	Median (Mode)	Mean (Std Dev)	Median (Mode)
Body search	3.13 (1.28)	3 (3)	2.69 (1.16)	3 (3)
Property search	3.91 (1.01)	4 (5)	3.60 (1.23)	4 (5)
Wiretapping	4.52 (0.98)	5 (5)	4.25 (1.28)	5 (5)
E-mail/internet monitoring	3.78 (1.26)	4 (4)	3.94 (1.22)	4 (5)
Security camera	1.87 (1.17)	1 (1)	1.63 (1.09)	1 (1)
Racial/ethnic profiling	3.30 (1.33)	4 (4)	3.52 (1.43)	4 (5)
Background check	2.22 (1.11)	2 (2)	2.45 (1.26)	2 (2)
Drug test (urine)	2.41 (1.39)	2 (1)	2.39 (1.28)	2 (1)
Field sobriety test	1.87 (1.15)	1 (1)	2.01 (1.23)	2 (1)
Financial records disclosure	3.04 (1.26)	3 (2)	2.93 (1.28)	3 (3)
Academic records disclosure	2.43 (1.19)	2 (1)	2.44 (1.41)	2 (1)
Library records disclosure	2.30 (1.24)	2 (1)	2.45 (1.34)	2 (1)
Medical records disclosure	3.65 (1.29)	4 (4)	3.36 (1.39)	4 (5)

Table S2: Participant Characteristics: Demographics and Attitude, N = 85

Quantitative Characteristic	**Average**	**S.D.**	**Min**	**Max**	**Mode**	**Median**
Age (in years)	21.7	5.21	17	48	19	20
College (in years)	2.65	1.36	1	5	2	2
Attitude (between 1 & 5)	3	1.16	1	5	3	3
Average Rank (between 1 & 5)	2.88	0.74	1	5	3	3
Percent Yes	0.40	0.19	0	0.85	0.38	0.38

Qualitative Characteristic		**Percent**	**Count**
Female		60%	51
U.S. Citizen		95%	81
New Mexican		68%	55
Freshman/Sophomore Status		59%	50
Junior/Senior Status		25%	21
Graduate Student		16%	14
Race or Ethnicity	Caucasian	42%	36
	Hispanic	32%	27
	Native American	6%	5
	African American	2%	2
	Asian	10%	8
	Other	6%	5
	Did Not Answer	2%	2
Attitude	1: *Reduced privacy doesn't bother me*	13%	11
	2	16%	14
	3	40%	34
	4	19%	16
	5: *Reduced privacy bothers me*	12%	10

Table S3: Experimental Variables Descriptive statistics

Variable	Mean	s.d.	min	max	N
Choice (R1)	0.929	0.507	0	2	85
Choice (R2-4)	0.924	0.521	0	2	210
Outcome Last	0.238	0.427	0	1	210
Percent Incident Last	0.238	0.329	0	1	210
Group Last	2.595	0.903	0	4	210

Supplementary Material: Detailed version of the theoretical model with proofs

Suppose that individual i has preferences over net wealth, m_i, and these preferences are represented by utility function u_i; as usual, $u_i' > 0$, $u_i'' < 0$, and $u_i(0) = 0$. Individual i is endowed with wealth w_i and is part of a group which decides the level of security for society. The level of security s depends on the number of privacy invasions the group chooses to allow, with the idea that as more privacy is sacrificed, the less likely a catastrophic event will be. Denote the allowable privacy invasion level as p, and let $s = f(p)$, with $f' > 0$ and $f'' < 0$, be a function which translates privacy invasions into security levels. Furthermore, let the function v_i translate the provided level of security into monetary terms, with $v_i' > 0$, $v_i'' < 0$, and $v_i(0) = 0$. Of course, privacy invasions are costly; for example, waiting in line to be searched or having phones wiretapped may result in time costs and embarrassment costs. Accordingly, let $c_i(p)$ represent the dollar equivalent of the loss due to privacy invasion p, with $c_i' > 0$ and $c_i'' > 0$. Hence, $u_i(m_i) = u_i(w_i - c_i(p) + v_i(f(p)))$.

Individual i chooses an acceptable privacy invasion level, denoted p_i, to maximize expected utility. However, the prevailing privacy invasion level $\mathbf{p}$ is not solely determined by individual i; it depends on individual i's choice p_i as well as all other individuals' choices (denoted $\mathbf{p}_{-i}$) and the voting rule. Clearly, $\mathbf{p}$ is unknown until all votes are counted; let the expected prevailing privacy invasion prior to revelation of the vote be represented by $E[\mathbf{p}|p_i,\mathbf{p}_{-i}] = z$. For convenience, suppose that z is continuous in p_i; for example, the privacy invasion could be determined by the mean vote of the group. (The majority voting rule used in our experiment is not continuous in p_i, but we expect that our results should still apply when a voting rule is not continuous.) The corresponding expected level of security provided is then $f(z)$.

Next, let q represent the probability of complete loss. The probability of loss depends on the level of security provided, so $q = q(f(z))$. We assume that q is continuous in z and that $q' < 0$; the more security provided, the smaller chance of a complete loss. Finally, individual i chooses p_i to maximize expected utility subject to the budget constraint, $c_i(z) \leq w_i$:

$$\max_{p_i \in P} \left(1 - q(f(z))\right)\left(u_i(w_i - c_i(z)) + v_i(f(z))\right) + q\left(f(z)\right)u_i(0).$$

The first term is the utility from no loss, which occurs with probability $1 - q$, and the second term is the utility from a complete loss, which occurs with probability q. Since $u_i(0) = 0$, the objective function reduces to

$$\max_{p_i \in P} \left(1 - q(f(z))\right)\left(u_i(w_i - c_i(z)) + v_i(f(z))\right). \tag{1}$$

Differentiating (1) with respect to p_i and rearranging indicates that p_i^* solves

$$c_i'(z) = v_i'\left(f(z)\right) f'(z) + \lambda \frac{m_i}{\varepsilon_u}, \tag{2}$$

where $\lambda = -(q'(f(z))f'(z)/(1 - q(f(z))) > 0$ is a hazard function, $m_i = w_i - c_i(z) + v_i(f(z))$ is net wealth, and $\varepsilon_u = \left(\frac{\partial u(m_i)}{\partial m_i}\right)\left(\frac{m_i}{u(m_i)}\right)$ is the income elasticity of utility, which is assumed positive.

So, given the assumptions of the model, the optimal privacy invasion equates the marginal cost of the privacy invasion to the marginal benefit of increased security, plus a term incorporating the inherent riskiness of providing security as well as the income elasticity of utility. Both the LHS and RHS of (2) are greater than zero. Moreover, the LHS of (2) is increasing in p_i, and the RHS is decreasing in p_i, ensuring that a unique interior maximum exists (proof below). The SOC is less than zero, ensuring that p_i^* is a maximum.

Consider (2), and suppose for the moment that there is no risk ($q = 0$); in other words, once a given level of privacy loss is reached, catastrophic events are avoided with certainty. In this case, the optimal allowable privacy invasion simple equates the marginal cost of privacy loss to the marginal benefit in terms of increased security. Adding risk, however, changes this outcome. Figure S1 shows the optimal level of allowable privacy invasions in the setting described in this model (p^*_{risk}) as well as in the case where there is no risk $(p^*_{certain})$. According to (2), individuals choose to submit to more privacy invasions when there is a probabilistic resolution to disastrous events.

Proof:

Equation (2) provides the condition for the optimal privacy invasion choice for individual *i*:

$$c_i'(z) = v_i'\left(f(z)\right) f'(z) + \lambda \frac{m_i}{\varepsilon_u},$$

To see that the LHS is increasing in p_i, note that $\partial c_i'/\partial p_i = c_i''(z)\cdot \partial z/\partial p_i$ and by assumption, both c_i'' and $\partial z / \partial p_i > 0$.

For the RHS of (2), let $A = v_i'\left(f(z)\right) f'(z)$ and let $B = \lambda \frac{m_i}{\varepsilon_u}$. We have

$$\frac{\partial A}{\partial p} = v_i''\left(f(z)\right)\left[f'(z)\right]^2 \cdot \frac{\partial z}{\partial p_i} < 0$$

since $v_i'' < 0$ and f', $\partial z / \partial p_i > 0$. Also,

$$\frac{\partial B}{\partial p_i} = \frac{\partial \lambda}{\partial p_i} \cdot \frac{m_i}{\varepsilon_u} + \lambda \cdot \frac{\partial\left(\frac{m_i}{\varepsilon_u}\right)}{\partial p_i}.$$

Now, assuming $q''(f(z)) > 0$,

$$\frac{\partial \lambda}{\partial p_i} = -\left[\frac{\left(1 - q\left(f(z)\right)\right)\left[q''\left(f(z)\right)\left(f'(z)\right)^2 + q'\left(f(z)\right) f''(z) \right] \frac{\partial z}{\partial p_i} + \left(q'\left(f(z)\right)\right)^2 \left(f''(z)\right)^2 \cdot \frac{\partial z}{\partial p_i}}{\left(1 - q\left(f(z)\right)\right)^2} \right] < 0$$

and noting that $m_i / \varepsilon_u = u_i(m_i) / u_i'(m_i)$, we have

$$\frac{\partial \left(u_i(m_i) / u_i'(m_i) \right)}{\partial p_i} = \frac{u_i'(m_i)\left(-c_i'(z) + v_i'\left(f(z)\right) f'(z) \right) - u_i(m_i) u_i''(m_i)\left(-c_i'(z) + v_i'\left(f(z)\right) f'(z) \right)}{\left(u_i'(m_i)\right)^2}.$$

The term $c_i'(z) + v_i'(f(z))f'(z) < 0$ from the FOC, and since $u_i''(m_i) < 0$, it is the case that $\partial(m_i/\varepsilon_u)/\partial p_i < 0$. Hence, $\partial B/\partial p_i < 0$; this shows that the RHS of (2) is decreasing in p_i.

Figure S1

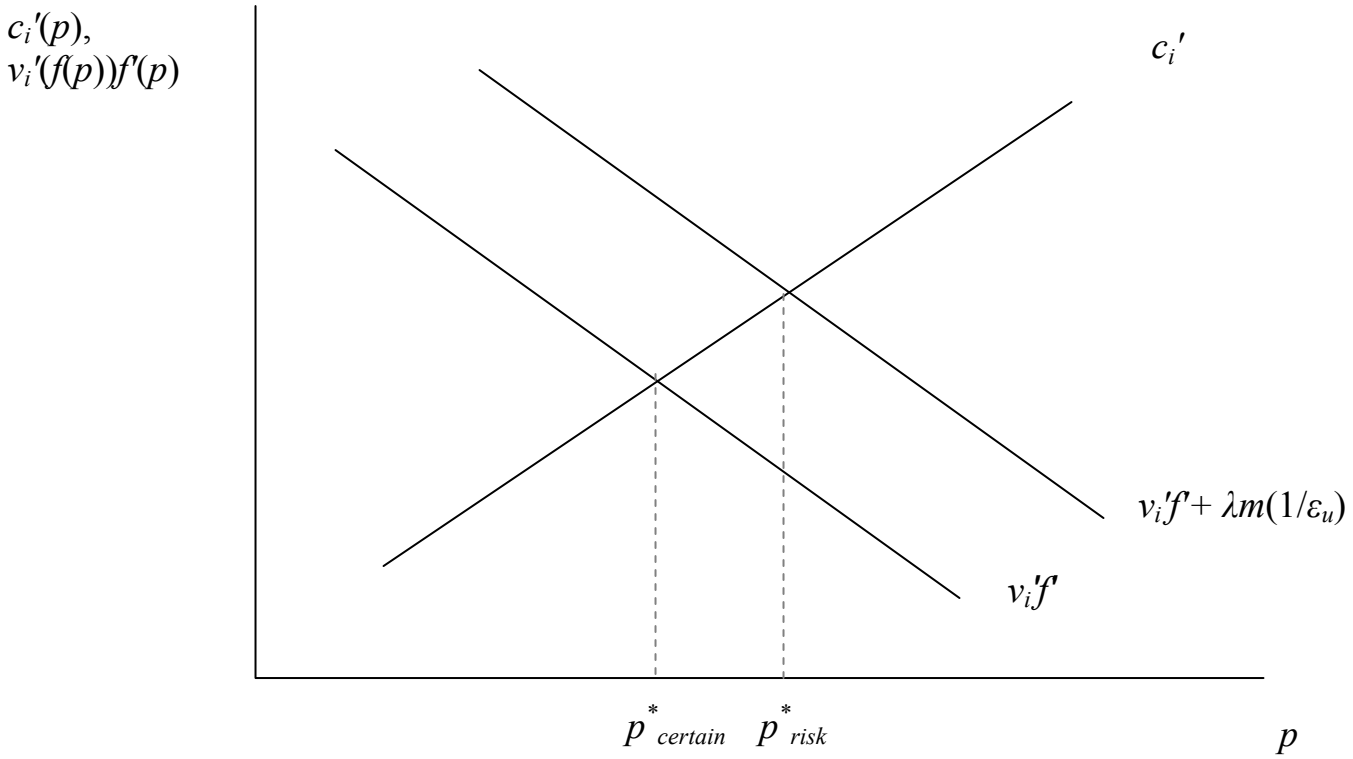

Figure S1: Optimal level of privacy invasions without and with probabilistic resolution of a catastrophic event ($p^*_{certain}$ and p^*_{risk}).

Stage One Survey Instrument

Privacy Issue	**Description (In all cases, the information is obtained by a Federal, State or Local Agency)**	Please check the appropriate box to indicate the extent to which each item is an *invasion of your privacy*					Has this happened to you? Please check appropriate box.			If yes, how many times?			
		1 Least	**2**	**3**	**4**	**5 Most**	**Yes**	**No**	**Don't Know**	**1**	**2-5**	**>5**	**Don't Know**
Body Search	An over-the-clothing pat-down search of your body												
Property Search	Includes backpacks, vehicles, dorm rooms, or apartments												
Wiretap	Monitoring of your phone conversations without your knowledge												
Monitoring of E-mail or Internet use	Makes content of e-mails sent or internet sites visited available, but does not include interception of e-mail prior to sending												
Security Camera Monitoring	Monitoring of crowds in public areas												
Racial or Ethnic Profiling	The use of racial or ethnic characteristics in determining whether a person is considered likely to commit a particular type of crime												
Background Check	Includes checking places of residence, arrests, website ownership, or interviewing acquaintances for things such as a job or firearm purchase												
Mandatory Drug Test	Testing of urine for illegal substances												
Sobriety Test	A field sobriety test, which is used to help determine one's motor and mental dexterity												
Disclosure of Financial Records	Includes debt and payment records, credit scores, ownership of property, and default on loans												
Disclosure of Academic Records	Includes GPA, course schedule, or other academic information, such as content of academic work												
Disclosure of Library Records	Makes available titles of books that have been checked out on your library record												
Disclosure of Medical Records	Makes available physical and mental health records												

Stage Two Survey

[This survey included the Likert instrument included in Appendix B plus the following questions.]

The following information will help us in our research. All information is voluntary and anonymous. For any questions you choose not to answer, please write NA in the blank. Thank you for participating in this survey.

1. How old are you? _____ years

2. What year in college are you?

   ___Freshman ___Sophomore ___Junior

   ___Senior ___Other (please specify)_____

3. What is your Ethnicity? _____

4. What is your gender? _____Male _____ Female

5. Are you an International student? _____Yes _____ No

   If yes, what is your home country? _____

   If no, what is your home state? _____

6. 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."

☐ ☐ ☐ ☐ ☐

1 2 3 4 5

Narrative Instructions for Stage Two

Welcome to this study and thank you for participating.

You have been given 30 tokens. Each token represents 40 cents, so your total token value is 30 times 40 cents, or $12. This money is yours, but depending on choices that you and others make during this study, you may lose some or all of that money. Today you will participate in several rounds of the study. When the session is over, one of those rounds will be chosen, at random, to be the round for which you will be paid. We will pay you, in cash, the value of the tokens you had at the end of the round chosen for payment. This payment will be in addition to the $5 fee you will be paid for participating in this experiment.

In this study we will ask you to imagine yourself in the scenarios that we describe.

Think about situations in which a crime has occurred that resulted in significant loss to people. In many cases, these events might be prevented if people sacrificed some degree of privacy. For example, searching everyone as they enter a public place reduces the risk that someone will enter with a weapon or an explosive device.

In this study, we will ask you to think about how much privacy you are willing to give up to reduce the risk of a devastating loss.

We have listed six steps that could be taken to reduce the risk of a complete loss. You may think that some of those steps would not be very offensive for you, but some may seem to violate your privacy in a significant way. It will be up to you to decide which you would tolerate and which you would not.

Because we can't actually take these security measures, we will assign a token, or monetary, value to the "cost" you would feel if you were to experience them.

The more invasive the security step, the more tokens, or money, you will lose. But, the more invasive the security step, the lower your risk of complete loss.

We can't actually cause a devastating loss either. In this experiment, that loss is a complete loss of all of your tokens.

In this experiment, a privacy violation causes you to lose some tokens. However, as more privacy is given up, the risk of complete loss of all of your tokens is reduced.

The decision to give up privacy in exchange for risk reduction must affect everyone. For example, if most people in this country thought it was acceptable to wiretap telephones, and voted to allow it, then everyone would be governed by the rule, not just those who voted for it.

In this study, the decision to take security measures will be by majority vote.

For each measure, we will ask you to decide whether you would vote to give up your privacy, and the privacy of others in your group, in exchange for the reduced risk of a complete loss. We will ask you to read down the list of security measures. The first ones on the list are ones that surveyed college students thought would bother them the least. But, as you read down the list, the steps become more invasive. Your task is to decide how far down the list you are willing to allow authorities to go in order to reduce the risk that all of your tokens will be lost. **Agreement must be in the order presented on the list: Agreeing to any measure means you have also agreed to all measures closer to the top of the list.**

For each security measure, we will count the number of participants who chose to give up that degree of privacy. If half or more of the participants in your group choose to accept that step, ALL members of your group will lose the specified number of tokens and the probability of risk will fall. We will continue this way, down the list, until we reach the point at which fewer than half of the group members voted to tolerate the privacy violation in exchange for reduced risk.

You have been randomly assigned to a group of five participants. We will not tell you who is in your group. We will ask you to make this decision several times, and we will change groups each time you make a decision. At the end of the session, we will pay you based on the outcome of just one of those decisions. The round that is used for payment will be determined by a random draw from this bingo cage.

On the reporting form we will be asking you how much privacy, or tokens, you would vote to give up in order to reduce risk.

You may refer to these instructions at any time during your session.

Now please look at the list on the reporting form.

If no steps are taken to increase security there is an 80% chance that you will lose all of your tokens. In other words, there is a four in five chance that you will lose all of your tokens. But if most of the people in your group agree to some of the security measures, the chance of losing all of your tokens falls.

If loss occurs, all of the wealth that you have earned in this round of the experiment will be lost. If the loss is avoided you will keep the thirty tokens that you started with minus any that you have "spent" in lost privacy. Regardless of the outcome of any round, you will begin each new round with 30 tokens, or $12.

Once everyone has made their decisions we will collect the forms and determine the highest level of security measures that is acceptable to the majority of people in your group of five. We will then use this bingo cage to determine whether the loss actually occurs or not.

Reporting Form

Round: _____ ID#_____

Privacy Item	**Description (In all cases, the information is obtained by a legal authority)**	**If everyone experiences this and all previous measures, risk of complete loss is:**	**Value of lost privacy for this and all previous security measures (tokens you will lose if your group agrees to this level of security)**	**Would you agree to have this done? (circle one)**	
Security Camera Monitoring	Monitoring of crowds in public areas	0.50	2	Yes	No
Drug Test	Testing of urine for illegal substances	0.35	5 (includes 2 from above plus 3)	Yes	No
Body Search	An over-the-clothing pat-down search of your body	0.22	9 (5 from above plus 4)	Yes	No
Monitoring of e-mail or internet use	Makes content of e-mails sent or internet sites visited available, but does not include interception of e-mail prior to sending	0.12	14	Yes	No
Property Search	Includes backpacks, vehicles, dorm rooms, or apartments	0.05	20	Yes	No
Wiretap	Monitoring of your phone conversations without your knowledge	0.02	27	Yes	No