Cars, Condoms, and Facebook

Vaibhav Garg
Drexel University
and L. Jean Camp
Indiana University

No Institute Given

Abstract. Participation on Online Social Networks (OSNs) inherently requires information sharing and thus exposes individuals to privacy risks. Risk mitigation then has been encouraged through adoption of usable privacy controls. However, stronger privacy enhancing technologies (PETs) decrease both risk and perceptions of risk. Thus, individuals feel safer and may in fact respond by accepting more risk. Such perverse results have been observed offline, e.g. automobile safety, HIV prevention. Risk perception offline has been understood to be a function of characteristics of the risks involved rather than as a calculus grounded only in the probability of the risk and the magnitude of harm. In this work we use nine characteristics of risk from a classic and proven offline model of perceived risk to conduct a survey based evaluation of perceptions of privacy risks on Facebook. We find that these dimensions of risk provide a statistically significant explanation of the perceived risk of information sharing on Facebook. Our results indicate that more knowledge about privacy violations may lower risk perceptions; thus, we argue for public campaigns grounded in risk communication with a focus on severity of consequences of information sharing.

Keywords: Privacy, Facebook, Risk Perception, Control

1 Introduction

There were approximately 50,000 fatalities due to car crashes in United States in the the 70's. Since then public policy mandates, such as car safety belts, airbags, and private sector offers (e.g. Anti Lock Brakes (ABS)) have been put in place to address concerns. Today the fatality rate is lower (≈40,000). Overall, it is unclear if this reduction in harm can be attributed to the safety interventions. Arguably, external factors, such as reduction in drunken driving, have had more influence; drunken driving accounts for more than ≈30% of such fatal accidents. The inability of car safety initiatives to significantly impinge harm is attributed to risk compensation [**?**], i.e. as technologies become safer individuals engage in more risk taking behaviors. Individuals who wear safety belts drive at faster speeds; when cars are enabled with ABS, drivers stay closer to the vehicle in front. Thus, mandates on technical solutions that should in theory reduce overall harm, are in practice rendered less effective (even impotent). Don't drive and

drive campaigns, however, have been found to be effective at reducing overall fatality rates as well as individual likelihood of harm [**?**,**?**].

The high-modernity of new technology exposes individuals to (novel) risks [**?**]. Information sharing on Online Social Networks (OSNs), e.g. Facebook, exposes individuals to privacy risks. These risks often manifest as tractable losses, e.g. Facebook fired. Yet participation in Facebook is continent upon sharing information. It is then not surprising that although individuals express privacy concerns, they willingly post potentially harmful information online. This disconnect between the expressed preference for privacy and observed behavior of willful disclosure has been called the privacy paradox [**?**]. To alleviate the harm from this information sharing, the foremost proposal has been that of Privacy Enhancing Technologies (PETs); for Facebook specifically these manifest as privacy controls. These controls have been bemoaned for the lack of usability [**?**]. However, assuming that usable controls are available corresponding reduction in harm is not given. As in the case of cars and seat belts, individuals may compensate for better privacy controls with risk seeking behavior. Brandimarte et al. [**?**] note that when individuals perceive a higher control in the publication of information, they tend to share more. Thus, similar to case of automobile safety the protection provided by stronger PETs may be mitigated by increase in information sharing.

The presence of strong technical solutions that are usable is necessary to enable privacy online. However, it is not sufficient as individuals do not engage in a economically rational calculus, optimizing the cost-benefit tradeoff, when sharing/protecting information [**?**]. Instead privacy behaviors, akin to behaviors offline, are boundedly rational [**?**]. Thus, the acceptability of (privacy) risks is driven by the perceived risk vs. the perceived benefit of an activity. Slovic argues that the differences in perceived risk is a key determinant of the distinct risk mitigation strategies employed by experts vs. non-experts [**?**]. Perceived risk offline is driven by nine characteristics of the hazard [**?**]: 1) voluntariness, 2) immediacy, 3) knowledge to the exposed, 4) knowledge to experts, 5) control, 6) newness, 7) common-dread, 8) chronic-catastrophic, and 9) severity. Offline, this framework informed four decades of research in risk perception and public policy in a diversity of risk domains, e.g. environmental risk [**?**], health risk [**?**]. Online, this framework has been used to explain perceptions of technical security risks [**?**] and insider threats [**?**].

In this paper, we will conduct a first examination of this framework for privacy risks of information sharing on OSNs using the psychometric paradigm of expressed preferences. In the process we adapt and translate Fischhoff's canonical nine dimensional model for privacy risks on Facebook. By grounding our analysis in a framework that has been used to examine perceived risk across domains and cultures we allow for a systematic comparative across risk perception studies, both online and offline. We detail the related work in section 2. Section 3 outlines the methodology including the survey instrument design and deployment procedure. We present our findings in section 4. Section 5 discusses

the implications of our findings. We conclude in section 6 with a description of future work.

2 Background & Related Work

Information disclosure on Facebook is to a large extent voluntary. Individuals, however, share more information when disclosure is voluntary [**?**]. Thus, individuals who perceive information sharing on Facebook to be voluntary should share more than others.

H_{0_1} : There is no correlation between the perceived risk of sharing an information item and its perceived voluntariness.

Perceived risk of an activity appears lower when the consequences are delayed. Smoking, for example, in the immediate term provides stress-relief, but the long term may lead to cancer. Information sharing, similarly, provides gratification, e.g. social recognition, in the short term. The regret of sharing may, however, be delayed and felt only after the information has been shared [**?**].

H_{0_2} : There is no correlation between the perceived risk of sharing an information item and the perceived immediacy of consequences.

As individuals better understand the underpinnings of an activity their perceptions of risk are similarly informed. Rationally informed individuals should make better decisions. In fact when privacy risks are communicated effectively, individuals share information in a manner aligned with their preferences [**?**]. Counterintuitively, informed individuals may feel more empowered to manage the consequences of sharing and thus share more.

H_{0_3} : There is no correlation between the perceived risk of sharing an information item and perceived knowledge to exposed.

The perceived knowledge to experts, or in this case the effectiveness of expert systems also informs risk perceptions and therefore behaviors. Inaccurate understanding of expert systems may mislead non-experts into assuming protections that are not provided by the technical solution. For example, non-experts assume comprehensive anonymous communication when running Tor, even though the protection is only available selectively [**?**].

H_{0_4} : There is no correlation between the perceived risk of sharing an information item and perceived knowledge to experts.

Perceived control over the consequences can also impinge the perceived acceptance of risk taking. Intuitively, as individuals feel more control over the consequences, they would feel more comfortable with engaging in a risky activity. Experimental validation for this intuition is available online for information sharing behaviors. Brandimarte et al. note that individuals who felt more in control, shared more information [**?**].

H_{0_5} : There is no correlation between the perceived risk of sharing an information item and perceived control over consequences.

The newness of a risk impinges the individual ability for objective evaluation. New risks would be poorly understood and thus likely to be exaggerated or underestimated. For example, offline information sharing is likely one to one.

Online, information shared on different platforms, at various times, with distinct entities can be aggregated and thus the potential for privacy violations is exponentially higher. Such privacy risks are neither tractable for the end-users, as humans are better at averages than aggregation [**?**], nor accepted by them [**?**].

H_{0_6} : There is no correlation between the perceived risk of sharing an information item and its perceived newness.

Perceptions of risks that are commonly encountered are typically lower than those rarely encountered. The evolutionary rationale for such perceptions is intuitive. If individuals constantly worried about the risk of crossing the street if would lead to a functional paralysis. Simultaneously, the data on rare risks would be sparse; thus, it would be difficult to ex-ante approximate a strategy for risk mitigation. Information sharing is a risk that is commonly encountered and is commonly beneficial as it increases market efficiency; however the data on privacy risks is difficult to obtain. Even when information is shared willingly, it is difficult (in fact impossible) for an individual to identify how often the information was accessed, by whom, and for how long [**?**].

H_{0_7} : There is no correlation between the perceived risk of sharing an information item and its perceived rarity.

Catastrophic risks, where many people are impacted in a single incidence of an event, may appear more scary than those in which only an individual is impacted. For example, terrorist attacks often impact multiple individuals and thus can be overestimated. Food poisoning appears to impinge solitary individuals and thus appears relatively benign. However, in most countries more individuals die of food poisoning than of terrorist attacks.

H_{0_8} : There is no correlation between the perceived risk of sharing an information item and catastrophic nature of its impact.

The perceived severity of the consequences of information sharing also impinges the perceived privacy risk. For example, acknowledging affinity for an unconventional book may simply lead to teasing the peer group; however, sharing sexual orientation can lead to social discrimination, denial of employment, and even physical violence for traditionally vulnerable communities.

H_{0_9} : There is no correlation between the perceived risk of sharing an information item and perceived severity of impact.

While perceptions of risks are driven by the characteristics of the risk, individual demographic considerations are equally important. It has been argued that individuals should not care about privacy as information sharing increases market efficiency [**?**]. Then only those who have something to hide should care about privacy. Alternatively, conceptualizing privacy as a property right, individuals who can not procure the full value of information shared should be concerned about privacy [**?**]. It has been noted that as individual characteristics differed from the norm, individuals cared about privacy more [**?**]. Thus, individuals with less stringent privacy preferences should have have lower perceived risk of sharing information on Facebook.

$H_{0_{10}}$: There is no correlation between perceived risk of sharing and individual privacy preferences.

Factors such as income, age, and gender are equally relevant. Individuals with lower incomes are less concerned about privacy [**?**]. Older adults may share less information than younger cohorts [**?**]. Women are more risk averse than men both online and offline [**?**] and thus should share less information [**?**].

$H_{0_{11}}$: There is no correlation between perceived risk of sharing and income.

$H_{0_{12}}$: There is no correlation between perceived risk of sharing and age.

$H_{0_{13}}$: There is no correlation between perceived risk of sharing and gender.

Finally, the perceived risk of an activity is also influenced by its perceived benefit. Previous research indicates that for most activities there exists a negative correlation between the respective perceived risk and perceived benefit [**?**]. Thus, activities that are considered to be less risky are seen as more beneficial and vice versa. The canonical counterexample in an American context is nuclear energy, which is seen as both higher beneficial and highly risky.

$H_{0_{14}}$: There is no correlation between perceived risk of sharing an information item and the corresponding perceived benefit.

3 Methodology

In this research we are concerned with the underlying determinants of perceived risk, as well as the relationship between perceived risk and perceived benefit, as they pertain to sharing information on Facebook. To the extent that information sharing on Facebook is a risk, we posit that perceived risk would be informed by nine characteristics of risk [**?**]: 1) voluntariness, 2) immediacy, 3) knowledge to the exposed, 4) knowledge to experts, 5) control, 6) newness, 7) common-dread, 8) chronic-catastrophic, and 9) severity.

There are two methodologies to evaluate perceived risk: 1) revealed preferences [**?**] and 2) expressed preferences [**?**]. A revealed preferences approach is based on the assumption that over a period of time, through trial and error, society has reached an optimal level of risk. Thus, perceived risk can be evaluated by examining past data based of risk behaviors. This approach is, however, difficult to apply to privacy risks. First, databases of past behaviors are rarely available. Second, privacy risks are constantly evolving; even on Facebook the constant evolution of the privacy controls and default settings changes the risk to which individuals are exposed. Finally, revealed preferences only declare previously acceptable risk but not what is desirable in the future [**?**].

The alternative methodology is the psychometric paradigm of expressed preferences, which survey individuals to elicit perceived risk. Previous research has identified, acknowledged, and addressed the limitations of this methodology [**?**]. However, given that privacy decisions are situated in the context of praxis [**?**], a survey based is additionally limited as it may not illuminate deeper specific factors that can be discovered from an in-situ study. To reduce the impact of divergent contexts, we focus our study on information sharing on Facebook and target a relatively self similar demographic in terms of age, education etc. by selectively recruiting participants from an undergraduate computer science class.

3.1 Survey Design

We use the psychometric paradigm of expressed preferences to survey individuals regarding the perceptions of information sharing on Facebook. The design of the survey was kept similar to the original instrument used by Fischhoff et al. for consistency. All participants began by providing relevant demographic information: 1) gender, 2) age, and 3) household income. Furthermore, participants provided Facebook specific demographic information: 1) frequency of Facebook accesses, 2) frequency of status message updates on Facebook, and 3) frequency of location sharing on Facebook. Finally, individual privacy preferences of the participants were enumerated by using a subset of the Internet Users' Information Privacy Concerns (IUIPC) scale [**?**]. The subset measures global privacy concerns rather than concerns about specific contexts such as consumer privacy.

A typical Facebook profile consists of twenty-two information items: real name, DoB (without year) or DoB (with year), current address, telephone, email id, personal website, music, movies, books, television, personal interests, photographs, political affiliation, religious affiliation, sexual orientation, friends list, education, work experience, current employment, and hometown. All participants were asked to identify which of these information items they shared on Facebook and with whom, i.e. friends, friends of friends, or everyone. (No sharing was coded as 0, sharing with friends, friends of friends, and everyone was coded as 1, 2, and 3 respectively.)

Participants then rated the risk (or benefit) of sharing individual information item on Facebook. Participants were not given a definition of what is implied by risk (or benefit). (As in the original study by Fischhoff et al. participants did not rate both risk and benefit. If the same participant imagines both the risks and benefits of sharing an information item, then it is possible that one would impact the other. That is a participant who imagines the risk of sharing their birthday, may have a harder time imagining the corresponding benefits.) Participants rated the least risk (or beneficial) item '10'. Thus, if sharing your DoB with the year gave you the least risk (or benefit), then that would be rated '10'. Each subsequent item was to be evaluated in comparison with this item. Thus, an item that was rated '20' would be twice as risky (or beneficial) as the least risky (or beneficial) item.

All participants rated the risk of each of the 22 information items on the nine dimensions of perceived risk [**?**]. The nine dimensions were defined as:

1. Voluntariness: Do you share this information voluntarily? Or is this information demanded by external entities such as Facebook, friends, etc.? (1=Voluntary; 7=Involuntary)
2. Immediacy: Is the impact of sharing this information immediate or does it happen at a later point in time? (1=immediate; 7=delayed)
3. Knowledge to exposed: To what extent are you aware of the consequences of sharing this information? (1=known precisely; 7=unknown)
4. Knowledge to experts: To what extent do you think experts are aware of the consequences of sharing the information? (1=known precisely; 7=unknown)

5. Control: Do you think you have control of the consequences of sharing the information? (1=uncontrollable; 7=controllable)
6. Newness: Do you think the implications generated from sharing this information are new? (1=new; 7=old)
7. Chronic-catastrophic: Does sharing this information affect only you (chronic) or several people (catastrophic)? (1=chronic; 7=catastrophic)
8. Common-Dread: Is sharing this information so common that you don't think about it? Or is it so unique that it fills you with dread? (1=common; 7=dread)
9. Severity: How severe do you think are the consequences of sharing this information? (1=certain to not have adverse consequences; 7=certain to have adverse consequences)

3.2 Procedure

The study was conducted using paper surveys. The order of presentation of the 22 information items was static and consistent across all survey instruments. Participants were recruited from a convenience sample of college undergraduates. Students were allowed a two-course-credit bonus to incentivize participation, contingent on their having used Facebook. The course credits were restricted to two as requested by the course instructors so that survey participation would be proportional to alternative opportunities for extra credit. The alternative was to opt out and write a short essay (≈500 words) instead. Each essay would have qualified for two credits and the topic of the essay was privacy or Facebook. The survey was deployed amongst two sections of the class. Both sections had access to both forms of the survey. Participants blindly selected from two stacks of the survey instruments. There were approximately 200 potential participants and approximately 100 students in each section. To ensure minimal harm to participants, appropriate precautions were taken and the study was approved by the Institutional Review Board (IRB) at the researchers' home institution.

4 Results

Of the 200 students who took the survey, 74 were returned. Thus, the response rate was approximately 37%. One of the surveys was discarded as it was completely empty. Two survey instruments were discarded as participants did not follow the instructions. Specifically, participants were asked to rate the nine dimensions on a scale of 1 through 7. However, one of the participants provided ratings higher than 7. Participants were also asked to give the item with the lowest perceived risk a rating of 10. A second participant provided risk ratings less than 10. Thus, there were 71 correctly completed survey instruments returned.

40 participants completed the perceived benefit survey. Of these, 30 were men and 10 were women. 38 participants were between the ages of 18-25 while 2 participants were between the ages 26-30.

Table 1. Distribution of Participants by Household Income

Income	Benefit	Risk
Less than $10,000	4	6
$10,000 to less than $20,000	0	2
$20,000 to less than $30,000	1	1
$30,000 to less than $50,000	4	2
$50,000 to less than $75,000	3	1
$75,000 to less than $100,000	4	2
$100,000 or more	12	6
Don't know	12	10

31 participants completed the perceived risk survey. Of these, 24 were men and 7 were women. 30 participants were ages 18-25, and 1 participant was 26-30.

We acknowledge that this is a convenience sample. Participants consisted of individuals in an undergraduate computer science class. Therefore, they are likely to be more informed. Table 1 provides a distribution of participants by household income. Distribution of participants by frequency of status message update, current location update, and Facebook access respectively is given by Table 2. The average privacy rating for participants completing the benefit survey was 26.81579, while that for risk was 26.03571. A one-sided T-test did not indicate a statistically significant difference with p-value=0.7935. Table 3 notes the number of participants who report sharing specific risk items as well as with whom those items are being shared, i.e. friends, friends of friends, or everyone.

Table 4 provides the median and the mean values for the perceived benefit and perceived risk of sharing each of the 22 information items. The correlation for the mean values of perceived benefit and perceived risk was not statistically significant with a p-value= 0.6321. The correlation for the median values was similarly not significant statistically with a p-value=0.9367.

Participants were also asked to rate the 22 risk items on Fischhoff's nine dimensions. The mean ratings are given in Table 7.

We computed the (Spearman) correlation between the nine dimensions of perceived risk as shown in Table 5. We also constructed an Ordinary Least Squared (OLS) linear regression model with perceived risk as the dependent variable and Fischhoff's nine dimensions as independent variables; Table 6. To alleviate the impact of outliers we took a log base 10 transform of the perceived risk as the dependent variable.

5 Discussion

In this paper, we examine the perceived benefit of information sharing on Facebook, compared to the perceived risk. There are several limitations to our study. First, we had a relatively small sample size of n=71. Second, the study was conducted with college undergraduates and the findings may not generalize to a larger population. Third, most participants in the study were frequent Facebook users (Table 2), and thus the findings may not apply to those who indicate moderate use. Third, our sample was gender skewed; the majority of participants

Table 2. Number of Participants: Frequency of Status Message, Current Location Update, & Facebook Access

	Status Message		Current Location		Facebook Access	
Frequency	Benefit	Risk	Benefit	Risk	Benefit	Risk
Less than once a month	14	10	31	28	2	1
Once a month	5	6	5	1	1	0
Once a week	19	12	4	1	3	5
Once a day	2	2	0	0	8	8
Several times a day	0	0	0	0	23	12
It is always on	—	—	—	—	3	4

were male. Our findings thus may not generalize to a more gender-balanced population. Since the order of presentation of items was static in this survey, the findings may be affected further by primacy or recency effects. The potential for this is non-negligible as correlation of this order with perceived risk is statistically significant (Table 5). This, however, only limits us in not allowing for the comparison of relative sensitivity of different information items. Our analysis of the relative importance of Fischhoff's nine dimensions and the framework itself would still be valid[1]. Finally, the impact of our findings is constrained by the limitations of survey-based methodology. For example, participants may simply lie or to a lesser degree demonstrate Wilder effects. Despite these limitations this study allows us to test a set of falsifiable hypotheses. These hypotheses should subsequently be tested with a larger sample and a more diverse population.

Table 5 indicates that hypotheses $H_{0_1}, H_{0_3}, H_{0_5}, H_{0_7}, H_{0_8}$, and H_{0_9} can be rejected; however, there is limited evidence to reject to H_{0_2}, H_{0_4}, and H_{0_6}. Thus, perceptions of privacy risks are lower when information sharing appears voluntary, individuals know more about the risk, the consequences of sharing appear controllable, the information is commonly shared, information sharing impacts only individuals, and the severity of consequences appears low.

The rejection of H_{0_1} and H_{0_5} indicates a counterintuitive insight for the providers of Online Social Networks, specifically Facebook. If individuals perceived higher control on consequences of sharing and sharing appears voluntary individuals share more. Thus, if OSN providers want to encourage individuals to share information, they should provide better PETs and empower their users. In this our research reifies previous results [**?**,**?**]. Simultaneously, we note that merely providing technical controls may not be adequate as lowered perceptions of risk could lead to compensation through increased information sharing.

The rejection of H_{0_3} is also counterintuitive. We agree that there is need to educate end-users about the consequences of sharing information. However, our results suggest that education is not a panacea as more informed individuals may feel a false sense of safety as awareness lowers perceptions of risk. Simultaneously,

[1] We computed a separate OLS regression model with information order as one of the dependent variable. However, the order in which information was presented was not statistically significant.

it is in the interest of OSN providers to invest in such educational campaigns as it lowers the inhibitions of their users. The impact of such educational input is made salient by Table 6, as knowledge to the exposed is a statistically significant determinant of perceived risk.

Intuitively, information that is commonly shared is perceived to be less risky. However, often commonly shared attributes such as real name can lead to privacy violations. For example, using real name on OSNs can make it easier for an adversary to search and locate an individual's profile. (Note that while individuals do not consider Real Name to be a commonly shared attributed (mean=3.0; Table 7); it is a required information item on Facebook.) Items marked as commonly shared by the participants, such as sexual orientation or political affiliation, can clearly have a real life impact. (In fact many of the participants report sharing such sensitive information online. For example, 54 participants report sharing their sexual orientation on Facebook; Table 3.)

Table 3. Information Sharing Practices: Perceived Benefit & Perceived Risk

	Benefit			Risk		
Information Item	Friends	FoF*	Everyone	Friends	FoF*	Everyone
Real Name	4	6	30	7	1	22
DoB (without year)	10	8	19	13	6	8
DoB (with year)	11	7	11	16	3	6
Address	14	1	1	5	1	1
Telephone	20	3	1	8	1	1
Email	24	5	5	16	4	5
Website	14	5	3	4	1	4
Music	18	8	6	15	4	4
Movies	17	8	5	14	4	5
Books	16	8	5	12	4	5
Television	17	8	6	13	4	5
Interests	19	6	9	14	5	4
Photographs	29	7	2	19	8	0
Political Affiliation	18	2	2	10	2	1
Religion Affiliation	20	3	2	13	3	3
Sexual Orientation	18	7	6	14	3	6
Interested in	20	5	9	17	5	4
Friends List	20	7	7	16	7	4
Education	15	5	13	15	5	9
Work Experience	15	4	9	14	4	5
Current Employment	13	4	10	13	5	3
Hometown	21	5	14	15	3	8

*Friends of friends

Information that impacts fewer individuals is perceived to be less risky. This is not problematic when individuals correctly assess whether the information is catastrophic in nature or not. However, from Table 7 we note often this assessment may be incorrect; for example, individuals consider that Friends List is not

a catastrophic risk. Arguably, sharing the friends list would not only impinge the individual sharing but also all their friends.

Sharing information when the severity of consequences is lower is also perceived to be less risky. Offline severity is the most important determinant of perceived risk [**?**]. There is evidence that severity is very important even for perceptions of privacy risks. Severity is significantly correlated with perceived risk (Table 5) and also statistically significant in the regression model (Table 6).

The nine-dimensional framework provided a statistically significant explanation (p-value<<0.001) of the (13.17%) variance in perceived risk of information sharing on Facebook (Table 6). Perceptions of privacy risks on Facebook may then be similar to those offline and may be addressed by translating offline strategies online. For example, public awareness campaigns have successfully addressed drunken driving [**?**]. Our results indicate that it is in the interest of OSN providers to facilitate similar campaigns online and simultaneously provide (subsidized/usable) technical solutions for privacy. Investment in such awareness may be additionally justified by the costs of self-regulated behavior under a perceived panopticon that may hamper information sharing [**?**].

Table 4. Perceived Benefit Vs. Perceived Risk

	Benefit		Risk	
Information Item	Median	Mean	Median	Mean
Real Name	12	20.47	10	18.95
DoB (without year)	12	14.88	10	15.43
DoB (with year)	12	15.12	12	17.55
Address	10	11.24	15	22.09
Telephone	11	14.29	15	26.09
Email	11	13.29	14	24.87
Website	10	15.35	10	12.05
Music	10	12.76	10	11.19
Movies	10	13.24	10	10.81
Books	10	10.82	10	11.23
Television	10	14.82	10	11.00
Interests	11	16.35	10	11.50
Photographs	12	19.53	12	19.26
Political Affiliation	10	10.24	10	12.90
Religion Affiliation	10	10.41	12	13.67
Sexual Orientation	10	10.53	10	14.29
Interested in	11	11.00	10	12.29
Friends List	12	17.53	10	11.90
Education	12	17.12	10	13.00
Work Experience	11	16.65	11	13.57
Current Employment	11	17.12	10	13.50
Hometown	12	14.65	10.50	17.45

Individual privacy preferences were strongly and positively correlated with the perceived risk of information sharing, rejecting $H_{0_{10}}$. Thus, while privacy decisions are often contextual, general risk attitudes towards information sharing

significantly impinge on an individual's decision to divulge information on social networking sites as well. Given that contextual user education about information sharing may be expensive and less tractable, general awareness about privacy, if leveraged, would still improve outcomes.

Table 5. Correlation

Dimension	Correlation
Voluntariness	0.194***
Immediacy	-0.085
Knowledge to Exposed	-0.197***
Knowledge to Expert	-0.086
Control	-0.106*
Newness	-0.070
Common-Dread	0.114*
Chronic-Catastrophic	0.163***
Severity	0.167***
Demographic Factor	**Correlation**
Gender	0.031
Income	0.034
Facebook Access	-0.007
Status Update	-0.049
Location Update	-0.0180
Privacy	0.150**
Info Order	-0.122**
Info Shared	0.073
p-value: $0 <$ *** $< 0.001 <$ ** $< 0.01 <$*< 0.05	

$H_{0_{11}}, H_{0_{12,and}H_{0_{13}}}$ could not be rejected. $H_{0_{11}}$ was difficult to test. About one-third of the sample, i.e. 22 participants did not report their household income, while another third, i.e. 24 participants, had a income higher than $75,000. $H_{0_{12}}$ could not be tested as most participants were of the same age. $H_{0_{13}}$ similarly could not be tested appropriately as the sample was heavily gender skewed with more than three-fourths of the participants being male.

Finally, $H_{0_{14}}$ could not be rejected. In similar offline studies, perceived risk has been negatively correlated with perceived benefit for most activities, e.g. smoking. The lack of correlation suggests that certain information items are not perceived as beneficial, but are shared due to the design of the website, the need to fill in blanks, etc. [**?**].

6 Conclusion and Future Work

Condoms alone do not limit the spread of Sexually Transmitted Diseases (STDs) as individuals compensate by have mulpitle partners or more risky sexual encounters [**?**]. The effective strategy has been addressing behaviors, for example in Uganda, rather than a singular reliance on technology. Similarly, it is imperative to address non-expert behaviors and lower the individual risk budget for security and privacy risks online. We must begin by identifying the pertinent

Table 6. Linear Regression Model

Dimension	Estimate	Std. Error
(Intercept)	1.080	0.0342***
Voluntariness	0.008	0.0042
Immediacy	-0.006	0.0039
Knowledge to Exposed	-0.015	0.0038***
Knowledge to Expert	0.003	0.0052
Control	0.006	0.0040
Newness	-0.007	0.0037
Common-Dread	0.005	0.0034
Chronic-Catastrophic	0.004	0.0051
Severity	0.016	0.0047***
p-value: 0 < *** < 0.001 < ** < 0.01 <*< 0.05		
Multiple R-squared: 0.1498, Adjusted R-squared: 0.1317		
F-statistic: 8.282 on 9 and 423 DF, p-value: 2.174e-11		

information, for the specific user, in the relevant context. The first step then is to investigate the determinants of risk perceptions online.

In this paper we use the psychometric paradigm of expressed preferences to survey individuals regarding the perceived risk of sharing information on Facebook. Our analysis is grounded in a classic nine dimensional model that has informed decades of research in risk and decision making offline [**?**]. The results starkly resemble previous research on offline risks, despite the lack of physical harm online. This has the promise of translating existing literature in risk communication and public policy for security and privacy risks online. Arguably, previous successful offline solutions would not always be appropriate online. However, by grounding our efforts to reduce online harm in the extant rich body of academic and practitioner initiatives to manage risk offline, allows us to avoid making the same mistakes and reinventing the wheel.

We translated the nine dimensional model for privacy risks on Facebook. We validated results from previous studies that observed non-expert privacy behaviors; thus we used an expressed preferences methodology to validate prior results based in revealed preferences. Specifically we note systems that allow voluntary disclosure and greater control may encourage more information sharing. Simultaneously, more informed users have lower perceptions of risk and thus may share more. Thus, there is a perverse incentive for OSN providers, like Facebook, to empower their users to protect privacy. Educated users may demonstrate behaviors that reduce harm for a single incidence of information disclosure. However, as perceived risk of information sharing decreases they may share information more frequently. Thus, the overall privacy risk remains the constant, i.e. the risk thermostat is not impinged as individuals compensate [**?**].

Finally, while the acceptability of privacy risks manifests contextually, our results indicate that baseline privacy preferences may significantly inform individual perceptions. Thus, risk communication through generalized privacy campaigns is needed and can be potentially effective. Risk communication designers

should focus on the relevant determinants of perceived risk on Facebook, i.e. severity and knowledge to the exposed.

Table 7. Mean Ratings on Fischhoff's Nine Dimensional Scale

Information Item	Voluntary	Immediacy	Exposed	Expert	Control	Newness	Common	Chronic	Severity
Real Name	3.207	2.071	2.964	1.536	3.50	5.607	3.0	1.607	4.00
DoB (without year)	2.821	2.37	3.111	1.926	4.111	5.148	2.519	2.037	3.296
DoB (with year)	3.071	2.643	3.143	1.393	3.857	4.929	2.964	2.679	4.679
Address	4.259	3.667	3.111	1.741	4.185	4.889	4.333	4.63	6.074
Telephone	3.889	3.222	3	1.593	4.37	4.741	3.963	4.259	5.741
Email	4.207	3.036	2.964	1.607	4.214	4.393	2.893	2.821	4.679
Website	2.857	3.593	3.778	2.037	4.778	4.037	2.704	2.593	3.407
Music	1.379	3.214	3.964	2.786	5.286	4.571	2.321	1.607	2.00
Movies	1.321	3.074	3.889	2.704	5.148	4.556	2.481	1.481	1.926
Books	1.321	3.148	3.889	2.815	5.222	4.556	2.519	1.333	1.926
Television	1.241	3.071	3.714	2.75	5.25	4.50	2.429	1.5	2.143
Interests	1.5000	3.148	3.704	2.667	5.037	4.259	2.444	1.333	2.148
Photographs	2.897	3.393	3.357	1.75	4.143	4.214	4.607	3.5	4.929
Political Affiliation	2.333	3.654	4.296	2.333	5.074	3.963	2.556	2.407	3.00
Religion Affiliation	1.929	3.444	4.185	2.296	5.111	3.889	2.963	2.481	3.0
Sexual Orientation	2.111	3.5	4.077	1.962	5.231	4.192	2.923	2.192	2.885
Interested in	1.379	3.25	3.75	2	5.143	4.036	2.643	2.143	2.714
Friends List	2.966	3.25	3.429	2.464	4.571	3.821	5.5	2.75	3.357
Education	1.857	3.111	3.704	1.815	4.889	4.481	3.852	1.741	2.963
Work Experience	2.148	3.5	3.308	1.769	4.615	4.654	3.538	1.885	3.538
Current Employment	2.37	3.615	3.50	1.769	4.846	4.846	4.423	2.923	4.192
Hometown	2.964	3.593	3.963	1.778	4.778	4.148	4.593	3.037	4.148

Future work should address the limitations of this study, i.e. a larger more diverse pool of participants should be approached to participate as survey respondents. Since privacy risks are context driven, participants can be asked to express preferences by responding to specific scenarios. Finally, conceptions of privacy may differ across cultures and thus follow up studies should also examine perceived risk for a culturally different population.