The Privacy Paradox: A Facebook Case Study by 2014 TPRC Conference Paper. (Arlington, VA)

Conference Paper · September 2014

CITATIONS
0

READS
59

3 authors, including:

Kevin Benton
Indiana University Bloomington
11 PUBLICATIONS **152** CITATIONS
SEE PROFILE

L. Jean Camp
Indiana University Bloomington
230 PUBLICATIONS **1,810** CITATIONS
SEE PROFILE

The Privacy Paradox: A Facebook Case Study

Vaibhav Garg[a], Kevin Benton[b], L. Jean Camp[b]

[a]*Drexel University*
[b]*Indiana University*

Abstract

The utility of social networks is contingent on information sharing, which constrains privacy. Engaging in online social networks is seen to indicate that the participants either do not care about privacy, do not understand the risks of information sharing, or find privacy controls to be unusable. Given the contextual nature of privacy all three models may exist in the population and in fact in a single person. We introduce the three distinct academic threads leading to each model, i.e. rational economics, risk behavior, and human computer interaction. Further, we conduct a survey based study to elicit the relative strengths of these explanations for information sharing on Facebook (n=384). Our findings indicate that while all three explanations are relevant, their relative strengths are different. The perceived risk of sharing information is the most important determinant of privacy behaviors; to a lesser extent usability of privacy controls is important. Finally, privacy preferences is the least important factor; thus, the explanation that people don't care is weakest explanation of the privacy paradox (on Facebook).

Keywords: Privacy, Usability, Economics, Risk Perception, Facebook, OSNs

1. Introduction

Why does the same individual who expresses concern about privacy, behaves in a manner that systematically exposes their information (Awad & Krishnan, 2006)? The semantics of the underlying behavior illuminates three distinct constructs. Indeed, all three explanations may apply to the same person in different contexts. First, it is possible that people, in fact, **do not care** about privacy (Posner, 1981); people understand that privacy is a good thing, like freedom and happiness and this leads to a Wilder effect in polling (Steven E. Finkel et al., 1991). Second, people may care

about privacy; however, they **do not know** how their actions impinge privacy (Boyd & Hargittai, 2010). The third and final argument is that people care about privacy and know about the implications of information sharing; however, privacy controls are not usable! (Iachello & Hong, 2007; Lipford et al., 2008). Thus, privacy preferences are costly to implement.

The solution to the privacy paradox depends upon the research thread that one follows to find the answer. For a classic economist, privacy is a lack of information (Posner, 1981). Given that market efficiency is contingent on more information, individuals are rationally unconcerned; the value from information sharing outweighs the costs of privacy loss. Thus, the solution is to ensure that the full value of the information being transacted is realized by the individual who shares it. From a behavioral perspective, the problem is perceived risk vs. perceived benefit of information sharing (Garg & Camp, 2013). Risk perceptions of privacy risks can then be informed by appropriate risk communication (Huang et al., 2011). A final explanation is that current privacy enhancing technologies (PETs) are not adequately usable, i.e. PETs either cannot implement user privacy preferences in practice, or require too much expertise to be widely adopted. The solution then is to design PETs that are usable and align with user's needs. For example, Egelman et al. (2011) demonstrate that merely informing users of risk is not adequate, instead they should be provided with risk mitigating options.

Is it that people don't care? Or people don't know? Is it a question of usability? Or is it a combination of all three? Individuals may not care given the perceived benefits of information sharing, may underestimate their risk due to limited understanding of potential harm, and may simultaneously find PETs to be unusable. In this study we examine all three explanations and their relative merits by conducting a survey based study which collects data on Facebook users' self reported behaviors and attitudes. In section 2 we detail the literature on the three distinct explanations of the privacy paradox and discuss the role of demographics in privacy behaviors. In each process, we develop a set of hypotheses for expected information sharing behaviors on Facebook based on prior literature. Note that these three explanations are unlikely to be exhaustive. However, they are the most frequently examined in academic literature. Section 3 discusses the survey methodology. In the process we outline the challenges of conducting survey-based research on Mechanical Turk, as well as its advantages. In section 4 we present the results. Section 5 discusses the implications of our findings. Finally, section 6 concludes.

2. Background & Related Work

Individuals simultaneously express privacy concerns, while demonstrating information sharing on Online Social Networks; this is known as the privacy paradox (Barnes, 2006). As noted before, there are three classic explanations for this paradox, namely 1) people don't care, 2) people don't know, and 3) usability. These can be translated into empirically observable constructs as 1) amount of information shared, 2) perceived risk of information sharing, and 3) frequency of use of privacy controls respectively. The key underlying determinants of these can be inferred as 1) individual privacy preferences, 2) characteristics of privacy risk, and 2) usability of privacy controls respectively; these are detailed in this section.

In addition privacy behaviors are also impinged by demographic factors, as both the benefits and risks of information sharing are differently available to distinct populations (Reynolds et al., 2011); accessible risk information leverages the availability heuristic to impinge perceived risk (Fischhoff et al., 1993). Boyd & Hargittai (2010) note that the use of Facebook privacy controls is in fact on the rise and correlates strongly with the skill of the individuals (often determined by their education, income, and age).

$H_{0_{01}}$: There is no correlation between individual sharing behaviors and perceived benefit.

$H_{0_{02}}$: There is no correlation between individual perceptions of risk and perceived benefit.

$H_{0_{03}}$: There is no correlation between frequency of use of privacy controls and perceived benefit.

Women are more risk averse than men (Garg & Nilizadeh, 2013), both offline and online, and will thus seek to share less information (Hoy & Milne, 2010). Since applications such as Girls Around Me, specifically target women (Bilton, 2012); unsurprisingly, women have stronger beliefs about privacy on Facebook compared to male counterparts (Hoy & Milne, 2010). Despite higher privacy concerns, Reynolds et al. (2011) note that women have more open privacy settings than men.

$H_{0_{04}}$: There is no correlation between individual sharing behaviors and gender.

$H_{0_{05}}$: There is no correlation between individual perceptions of risk and gender.

$H_{0_{06}}$: There is no correlation between frequency of use of privacy controls and gender.

Christofides et al. (2012) find that older adults tend to share less infor-

mation than younger cohorts; thus age should correlate with information sharing behaviors. Boyd (2009) argues that teenagers accrue a higher level of social capital from social networking websites and would therefore have different perceptions of privacy compared to older cohorts, while Hoofnagle et al. (2010) posits that older adults' perceptions of privacy risk may be similar to those of young adults. However, Reynolds et al. (2011) observe that elders change their privacy settings more often than younger cohorts (though older adults found the controls less usable).

$H_{0_{07}}$: **There is no correlation between individual sharing behaviors and age.**

$H_{0_{08}}$: **There is no correlation between individual perceptions of risk and age.**

$H_{0_{09}}$: **There is no correlation between frequency of use of privacy controls and age.**

Individuals with higher incomes are more concerned about privacy and thus should share less information (Acquisti & Grossklags, 2005).

$H_{0_{10}}$: **There is no correlation between individual sharing behaviors and income.**

$H_{0_{11}}$: **There is no correlation between individual perceptions of risk and income.**

$H_{0_{12}}$: **There is no correlation between frequency of use of privacy controls and income.**

Individuals with higher levels of education tend to be more risk averse and thus should share less information (Sheehan, 2002).

$H_{0_{13}}$: **There is no correlation between individual sharing behaviors and education.**

$H_{0_{14}}$: **There is no correlation between individual perceptions of risk and education.**

$H_{0_{15}}$: **There is no correlation between frequency of use of privacy controls and education.**

Below we discuss the literature pertaining to the three paradigms of paradox: 1) people don't care, 2) people don't know, and 3) usability. These can be loosely mapped to the three dimensional conceptualization of PETs, i..e privacy as confidentiality, control, and counter-surveillance (Gurses & Berendt, 2010). Privacy as confidentiality assumes that if people care about privacy they should simply refrain from sharing information; thus, information sharing argues that people don't care. Counter-surveillance concerns itself with the problem of information asymmetries and lack of transparency

pertaining information flows; undesirable information disclosure then is a result of poor risk communication. Finally, privacy as control acknowledges the need to share information but only in a manner that allows an individual control over it's visibility and target audience; privacy violations then indicate lack of usability of PETs. These three conceptualizations of privacy being considered are by no means exhaustive (Garg et al., 2013). For example, we do not consider the notion of privacy as contextual integrity (Nissenbaum, 2009). However, we believe that these conceptualizations provide non-trivial explanations of the privacy paradox and are of significant interest to privacy researchers, as demonstrated by the extent of privacy literature corresponding to each research thread (outlined below).

2.1. People Don't Care: Privacy Loss or Enhancing Market Efficiency?

Posner (1977, 1981) has been most articulate in examining privacy as a transaction cost. His argument is grounded in the notion of privacy as confidentiality, i.e. privacy is the right to conceal information. Privacy then leads to information scarcity or information asymmetry, which under classical economic theory reduces market efficiency; alternatively, more information encourages competition. For example, by introducing simple price comparison of term life insurance, prices dropped up to 15% (Brown & Goolsbee, 2002). Thus, by providing more information the insurance market became more competitive, thereby improving economic outcomes for producers and consumers (Varian, 1992).

Similarly, perfect information allows for economically efficient price discrimination (Odlyzko, 2004), which refers to selling a single good at appropriate prices to different consumers based on their willingness to pay. Price discrimination can increase social welfare (Varian, 1985); consumers who pay more indirectly subsidize production for those that pay less, presuming economies of scale. This allows the consumer who would pay less to participate. These rational economics arguments imply that people do not (and should not) care about privacy. People understand that caring about privacy is socially validated, so there is a Wilder effect in polling, i.e. when surveyed individuals communicate a value that they consider to be socially acceptable (Steven E. Finkel et al., 1991). Thus, only individuals who have stronger privacy preferences should share less and vice versa.

$H_{0_{16}}$: There is no correlation between individual sharing behaviors and individuals privacy preferences.

Privacy as confidentiality, however, is a narrow conceptualization of the term (Solove, 2007). Even from a rational economics perspective informa-

tion sharing is not economically efficient if the value of the transaction is not equitably distributed amongst participating stakeholders, in proportion of each stakeholders' cost (Posner, 1981). There is academic evidence that the individual valuation of privacy does differ. For example, Huberman et al. (2005) illustrated that the price an individual demands to reveal personally identifiable information is a function of deviance from the norm. This is much more the case when deviance took a socially less desirable direction, i.e. heavier rather than thinner, older rather than younger. Such social responses to deviance have also been well-documented in the physical realm (Wolfgang & Wolfgang, 1971). Thus, individuals who have stronger privacy preferences should perceive the risk of information sharing to be higher.

$H_{0_{17}}$: There is no correlation between individual perceptions of risk and individuals privacy preferences.

It has been argued that a self regulated consumer privacy regime will emerge among self optimizing actors (Böhme & Koble, 2007). Providing privacy controls would allow stakeholders to identify the individuals who do care about privacy and therefore target them accordingly. It has been noted that in the physical and virtual markets for products providing unobservability do sell (e.g. curtains),"when privacy is offered in a clear and comprehensible manner, it sells" (Shostack & Sylverson, 2004). Thus, individuals who care about privacy should use privacy controls more frequently.

$H_{0_{18}}$: There is no correlation between frequency of use of privacy controls and individuals privacy preferences.

Unfortunately, there are economic and empirical arguments that the privacy market is not working; and it fails to function because of well-documented market flaws (Anderson & Moore, 2006). These arguments tend to address transparency and reliability of information about privacy itself; for example, information asymmetry. Thus, an alternative economics argument for the privacy paradox is that the privacy market does not have adequate signals. (In economics, signals are difficult to falsify but easy to evaluate data that differentiates types when there are superficially similar parties who are quite different.) For example, third party signals like TrustE Seal have been found to be positively correlated with adware, spyware and exploitive privacy policies (Edelman, 2009). Even more technologically secure signals have been found to be unreliable. In a study of HTTPS, 77.4% of users login credentials could be read due to merchant misconfiguration. Only one in seven websites correctly implement their certificates (Freudiger, 2011).

Similarly, why privacy policies are not worth reading, can be argued in formal mathematical terms (McDonald & Cranor, 2008). A model of the market with fluctuating numbers of reliable privacy-respecting merchants will not necessarily reach an equilibrium where it is efficient for consumers to read privacy policies. As the cost of investigating the privacy policy changes, and the reliability of what is read varies, there is no stable self-reinforcing equilibrium under which consumers should read privacy policies. That is to say, even if high quality privacy providers could communicate clearly about their policies and practices, then this alone will not solve the problem in a dynamic system. This model argues that direct incentives are required to protect privacy. The market by itself will not reach a equilibrium where privacy policies are readable, read, and reliable as long as there are firms that can prevaricate about privacy (Vila et al., 2003). Empirical comparison of social networks notes that privacy policies did not produce competitive success (Bonneau & Preibusch, 2009). In fact, there was a measurable decline that could be inversely correlated with claims of strong privacy protections. Thus, the next section discusses privacy paradox as a manifestation of information asymmetries or poor risk communication.

2.2. People Don't Know: Perceived Risk of Information Sharing

A strictly (classical) rational economics approach to privacy, that assumes information sharing as a transaction, argues that individual decision to share information demonstrates that the individual does not care about privacy. However, individuals are boundedly rational and may not have accurate information regarding the risk, more so privacy risks (Acquisti & Grossklags, 2005). Furthermore, a disconnect between expressed attitudes and observed behaviors is not unique to privacy preferences (online) but is also evident in other risk domains (offline) (Sherman, 1980). Elicitation of risk preferences for research purposes is typically disconnected from the context. The lack of in-situ elicitation means that the benefits of risk engendering activity, such as information sharing on social networks, is not often perceived salient (Keller et al., 2006). The distance from the event means that people would be more optimistic about their predicted behaviors (Liberman et al., 2007); it is always easier to quit smoking in a month than in an hour. This boundedly rational conceptualization of privacy decisions is then determined by the perceived risk of an activity, which itself depends on the risk information available to the individual (Huang et al., 2011). Thus, a second explanation of the privacy paradox is that of inadequate risk communication, i.e. privacy is valued but **people are unaware**

that they are at risk for loss of privacy when sharing information on social networks.

Previous studies in risk perception online are often limited to the context of e-commerce. For example, Tan (1999) found that consumers found online purchases to be more risky than in-store purchases. Jarvenpaa et al. (2000) addressed the relationship between perceived trust and perceived risk in online shopping. They found that the more consumers trusted an online retailer the less risky they felt it was. Perception of trust was found to be positively correlated with the store's perceived size and its perceived reputation. Bhatnagar et al. (2000) also considered the perceptions of risk in online shopping. They define risk in this domain as having two dimensions: product risk and financial risk. Product risk deals with the product itself; for example, whether the product will work on delivery. Financial risk deals with the monetary risk; for example, risk associated with providing credit card information online. Forsythe & Shi (2003) extended this framework to include psychological risk and time/convenience loss. Perceived risk can have a negative effect on online shopping behaviors (Drennan et al., 2006).

Park & Jun (2003) looked at the cultural differences in risk perception for Koreans and Americans. They found that risk perceptions of online shopping were higher amongst Koreans than Americans. However, the shopping behaviors were similar. Thus, Koreans were seen to be more risk taking online. Sjoberg & Fromm (2001) conducted a survey based study of Swedish population. They found that risk of information technology were usually considered pertinent to other people. Other risk studies have considered a general notion of computing (Turner et al., 2001; Salisbury et al., 2001; Suh & Han, 2003; Miyazaki & Fernandez, 2001). While they examine specific instances these do not identify the underlying components of perceived risk online. Stewart (2004) acknowledges the difficulty of identifying the underlying determinants of risk perception especially when affect heuristic plays a part.

Risk perceptions are influenced by a diversity of factors, e.g. medium of risk communication (Garg et al., 2012a), availability heuristic (Keller et al., 2006), affect heuristic (Stewart, 2004) etc. The seminal focus of risk perception research has been the characteristics of the risk (Starr, 1969; Fischhoff et al., 1978; Slovic, 1987). Specifically, Fischhoff et al. (1978) examined nine characteristics of risk for risks offline, namely 1) voluntariness, 2) immediacy, 3) knowledge to experts, 4) knowledge to exposed, 5) control, 6) newness, 7) common-dread, 8) chronic-catastrophic, and 9) severity. The

risk characteristics offline typically demonstrate two underlying factors, i.e. dread and familiarity (Slovic, 1987). Dread risk refers to activities that are uncontrollable, rare, catastrophic, and have severe consequences; familiarity refers to new risks whose consequences are not immediacy.

Voluntary risks often appear to be less scary than those that are involuntary. For example, individuals often express concerns about personal information being involuntarily collected by the government, i.e. big brother, but are simultaneously willing to provide the same information voluntarily on Facebook. In a lab-based study, Preibusch et al. (2012) noted that when individuals had the choice in providing information, i.e. when disclosure was optional rather than mandatory, participants provided more information.

$H_{0_{19}}$**: There is no correlation between individual sharing behaviors and the perceived voluntariness of the activity.**

$H_{0_{20}}$**: There is no correlation between individual perceptions of risk and the perceived voluntariness of the activity.**

$H_{0_{21}}$**: There is no correlation between frequency of use of privacy controls and the perceived voluntariness of the activity.**

The immediacy of the consequences could impinge the perceived risk of an activity. Offline smoking risks are often ignored since the consequences do not manifest till later in life. Online, while the benefit of sharing information is often immediate (Acquisti, 2004), e.g. social gratification as friends like a post, the risks are often delayed (such Facebook Fired), or even invisible (denial of employment opportunities). Wang et al. (2011) note that often the consequences of sharing information are felt after the individual presses share and not before.

$H_{0_{22}}$**: There is no correlation between individual sharing behaviors and the perceived immediacy of the consequences.**

$H_{0_{23}}$**: There is no correlation between individual perceptions of risk and the perceived immediacy of the consequences.**

$H_{0_{24}}$**: There is no correlation between frequency of use of privacy controls and the perceived immediacy of consequences.**

The knowledge to the exposed can both increase or decrease the perceived risk of an activity. Caine et al. (2011) note that providing better risk communication allows individuals to share information in a manner that is more aligned with their privacy preferences. Simultaneously, more knowledge can also increase risk taking as individuals may feel that they are now more able to manage the consequences of sharing.

$H_{0_{25}}$: There is no correlation between individual sharing behaviors and the perceived knowledge to the exposed.
$H_{0_{26}}$: There is no correlation between individual perceptions of risk and the perceived knowledge to the exposed.
$H_{0_{27}}$: There is no correlation between frequency of use of privacy controls and the perceived knowledge to the exposed.

The perceived knowledge to experts (or the effectiveness of expert systems) can also inform how risky information sharing is perceived. Due to inaccurate or incomplete understanding of information sharing, individuals may imagine privacy controls to be more enabling than they are. Offline, increased efficiency of expert systems has been correlated with individual risk compensation in a diversity of domains from automobile safety (Adams, 1999) to HIV prevention (Cassell et al., 2006).

$H_{0_{28}}$: There is no correlation between individual sharing behaviors and the perceived knowledge of experts.
$H_{0_{29}}$: There is no correlation between individual perceptions of risk and the perceived knowledge of experts.
$H_{0_{30}}$: There is no correlation between frequency of use of privacy controls and the perceived knowledge of experts.

When individuals perceive higher control on the consequences of an activity the perceived risk of the activity is reduced. The canonical example is air travel vs. driving. While the former is statistically less likely to result in fatalities, the latter is perceived less risky as individuals feel more in control. Online, Brandimarte et al. (2013) noted that individuals who perceive higher control over the information shared tend to share more.

$H_{0_{31}}$: There is no correlation between individual sharing behaviors and the perceived control over consequences.
$H_{0_{32}}$: There is no correlation between individual perceptions of risk and the perceived control over consequences.
$H_{0_{33}}$: There is no correlation between frequency of use of privacy controls and the perceived control over consequences.

The newness of a risk can both alleviate or aggravate perceived risk. Offline information sharing is old and and thus the consequences better understood than online. For example, information shared online can be aggregated across different databases and thus lead to privacy violations that were not originally known or accepted by the individual (Malin & Sweeney, 2001). This problem is exacerbated by the bounded rationality of humans, who are better at estimating averages rather than aggregates

(Tversky & Kahneman, 1974).
$H_{0_{34}}$: There is no correlation between individual sharing behaviors and the perceived newness of the risk.
$H_{0_{35}}$: There is no correlation between individual perceptions of risk and the perceived newness of the risk.
$H_{0_{36}}$: There is no correlation between frequency of use of privacy controls and the perceived newness of the risk.

Offline common risks are accepted, while rare risks are dreaded. There is an evolutionary incentive to accept common risks. If individuals dreaded the risk of crossing a road for every incidence of the activity, it would lead to a functional paralysis. Simultaneously, the consequences of rare risks are difficult to compute as (experiential) data is sparse even if available. Thus, it is reasonable to dread risks that are not commonly encountered as they are difficult to strategically mitigate (post hoc). Most information sharing platforms online provide no or limited feedback on privacy exposure; it is almost impossible for an individual to know whether the information shared is being accessed, by whom, or with what frequency (Patil & Kapadia, 2012).
$H_{0_{37}}$: There is no correlation between individual sharing behaviors and the perceived rarity of the information shared.
$H_{0_{38}}$: There is no correlation between individual perceptions of risk and the perceived rarity of the information shared.
$H_{0_{39}}$: There is no correlation between frequency of use of privacy controls and the perceived rarity of the information shared.

The impact of the risk is also judged by the number of individuals impinged in a single incidence of the risk manifesting. For example, fatalities in automobile accidents may be underestimated since it impacts a few individuals in a single incidence; airplane fatalities, though statistically less likely, appear more scary as more people can die in a single incidence. Information sharing on Facebook can violate the privacy of the individual as well as that of their friends; for example, through photo tagging.
$H_{0_{40}}$: There is no correlation between individual sharing behaviors and the catastrophic nature of its impact.
$H_{0_{41}}$: There is no correlation between individual perceptions of risk and the catastrophic nature of its impact.
$H_{0_{42}}$: There is no correlation between frequency of use of privacy controls and the catastrophic nature of its impact.

Finally, the severity of the consequences also informs the perceived risk of sharing. For example, acknowledging affinity for a television show may

merely lead to teasing in the peer (friend) group. Alternatively, the television show may be seen to be promoting values that are not seen to reflect of the local community. Then the consequences of public disclosure may be more severe, e.g. social discrimination. Severity of consequences manifests as the most important characteristic of risk offline (Fischhoff et al., 1978) as well as online (despite the lack of physical harm) (Garg & Camp, 2012).
$H_{0_{43}}$: There is no correlation between individual sharing behaviors and perceived severity of consequences.
$H_{0_{44}}$: There is no correlation between individual perceptions of risk and perceived severity of consequences.
$H_{0_{45}}$: There is no correlation between frequency of use of privacy controls and perceived severity of consequences.

To the extent that risk perceptions determine individual privacy behaviors, the solution is education and effective risk communication. Unfortunately, both education and risk communication have limitations. Visual indicators of risk such as pop-up warnings, have been inadequate at changing behaviors. For example, Riegelsberger et al. (2003) found that individuals responded more strongly to photos than more relevant trust cues. Effective risk communication designs, while grounding themselves in perceived risk must make risk more accessible by using appropriate mental models (Camp, 2009) and nudge the participant into risk mitigation (Acquisti, 2009). Simultaneously, education based efforts are expensive, require long term investment, must be adapted and revised given a constantly evolving threat landscape, may have limited impact for demographics with low cognitive plasticity (Garg et al., 2012b). Debatin et al. (2009) note that knowledge about privacy risks had limited impact on behaviors; only users who experienced privacy violations took steps to prevent future incidents.

2.3. Usability: Information Sharing as Interaction Failure

Lack of usability can significantly impinge real world systems (Inglesant & Sasse, 2010; Whitten & Tygar, 1999). Usability limitations of Facebook privacy controls are well documented (Iachello & Hong, 2007; Lipford et al., 2008). Researchers have suggested alternate solutions, e.g. the use of *social circles* rather than friends lists (Adu-Oppong et al., 2008), combining usability with risk communication (Ackerman & Cranor, 1999) etc. A universal design can be tricky as context matters, e.g. visualization can both improve usability (DiGioia & Dourish, 2005; Rode et al., 2006) and increase risk (Conti et al., 2005). Privacy decisions are not taken in isolation and tend to be a part of a complex system (Dourish & Anderson, 2006).

One approach is to automate privacy decisions, which while desirable is not very pragmatic (Edwards et al., 2008), e.g. due to lack of universal privacy preferences. Thus, non-experts would be perpetual part of the decision loop (Cranor, 2008). Hence, the design of controls must take usability into account (Sasse et al., 2001; Whitten & Tygar, 1999). Simultaneously, to be successful these controls should be meaningful, useful, and not just usable (Smetters & Grinter, 2002).

Facebook has been criticized both for the design of privacy controls and user awareness on the implications of information sharing (Grimmelmann, 2009). The former argument addresses Facebook's privacy controls, which have been considered both ineffective and unusable. The latter argument focuses on the non-expert's naivety regarding the visibility of their information. Non-experts may not even be aware either of privacy policies or privacy enabling controls.

$H_{0_{46}}$**: There is no correlation between individual sharing behaviors and usability of privacy controls.**

$H_{0_{47}}$**: There is no correlation between individual perceptions of risk and usability of privacy controls.**

$H_{0_{48}}$**: There is no correlation between frequency of use of privacy controls and usability of privacy controls.**

3. Methodology

In this paper we evaluate the relative merits of three dominant explanations of the privacy paradox (for Facebook), i.e. people don't care, people don't know, and that privacy controls are not usable; the three corresponding dependent variables are: 1) information shared, 2) perceived risk of sharing information, and 3) frequency of use of privacy controls. Our evaluation is grounded in the psychometric paradigm of expressed preferences; thus, we conducted a survey-based study, the details of which are outlined in this section. Our methodology was approved by the host Institutional Review Board to ensure that the human subjects involved were not exposed to harm and ethical requirements met.

3.1. Survey Design

The survey had two components: 1) demographic information and 2) privacy questions. Demographic questions were the same across all surveys. We collected responses on standard variables such as age, gender, income, and education. Additionally, we were interested in Facebook behaviors.

Thus we also collected information on the frequency of Facebook access, frequency of customizing privacy settings, location sharing, and status message update on Facebook. We were also interested in the participants' privacy risk preferences. These were operationalized using the Internet Users' Information Privacy Concerns (IUIPC) scale (Malhotra et al., 2004). IUIPC measures a diversity of privacy preferences, we used the subset of the scale which evaluates global privacy preferences (rather than specific preferences, e.g. related to consumer behaviors online).

We used the System Usability Scale to enumerate the usability of Facebook privacy controls. System Usability Scale (SUS) has the advantage of being used in several decades of usability evaluation (Brooke, 1996). Simultaneously, recent studies note the relevance and utility of this scale for current systems (Bangor et al., 2008). SUS also provides an absolute enumeration of usability. Thus, as Facebook controls and associated usability change over time, it is possible to do comparative analysis.

The privacy questions in the survey were concerned with information shared on Facebook. We considered 22 information items that can be shared on Facebook, namely: real name, date of birth (without year), date of birth (with year), address, telephone, email, website, music, movies, books, favorite television shows, interests, photographs, political affiliation, religion, sexual orientation, interested in, friends list, education, work experience, current work, and hometown. To account for primacy or recency effects, these information items were always presented in a random order to the participant. All participants had to indicate whether they shared any of these information items as well as if the information item was shared just with friends, friends of friends, or everyone.

Half the participants were asked to rate the risk of sharing individual information items, while the other half was asked to rate the benefit. The lowest rating that could be assigned was 10. An item marked 20 was twice as risky (or beneficial) as the least risky (or beneficial) item. This strategy was employed in the original survey by Fischhoff et al. (1978), and also in any follow up studies that used the nine dimensional model to evaluate perceived risk. Participants were randomly assigned to the risk or benefit category. Participants were asked to consider all risks and benefits. Risks were elaborated as financial risk (e.g. identity theft), psychological risks (e.g. discrimination in peer group), and physical risks (e.g. stalking). Similarly, benefits were explained as financial (e.g. cheaper deals through behavioral advertising), psychological (e.g. peer recognition of achievements),

and physical (e.g. friends coming around to help with a move).

Finally, all participants were asked to rate each information item on the nine dimensions of perceived risk. For example, the participants were given an information item (such as real name) and then asked if they shared the information voluntarily? The items were rates on a 7 dimensional Likert-like scale; e.g. 1=voluntary, 7=involuntary. The nine dimensions were defined as follows:
i) Voluntariness: Do you share this information voluntarily? Or this information demanded by external entities such as Facebook or friends etc.? (1=Voluntary; 7=Involuntary)
ii) Immediacy: Is the impact of sharing this information immediate or does it happen at a later point in time? (1=immediate; 7=delayed)
iii) Knowledge to exposed: To what extent are you aware of the consequences of sharing this information? (1=known precisely; 7=unknown)
iv) Knowledge to experts: To what extent do you think experts are aware of the consequences of sharing the information? (1=known precisely; 7=unknown)
v) Control: Do you think you have control on the consequences of sharing the information? (1=uncontrollable; 7=controllable)
vi) Newness: Do you think the implications generated from sharing this information are new? (1=new; 7=old)
vii) Chronic-catastrophic: Does sharing this information affect only you (chronic) or several people (catastrophic)? (1=chronic; 7=catastrophic)
viii) Common-Dread: Is sharing this information so common that you dont think about it? Or is it so unique that it fills you with dread? (1=common; 7=dread)
ix) 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. Mechanical Turk

We used Amazon's Mechanical Turk (AMT) service to recruit participants for the study. Typical academic surveys are conducted with college students. Thus, it is difficult to generalize from the results. AMT allows researchers to gather participants from a more diverse sample. A second advantage of AMT is that participants are typically paid lower compensation than on a college campus. Thus, researchers can gather more responses, which allows them to statistically identify correlations even when the effect

size is relatively small. A key difference between AMT and traditional studies is that participants are not being observed by the researchers (or their associates). This is both an advantage and a limitation. Since participants are not being observed, researchers are less likely to unwittingly prime the participants or contaminate the results. However, the participants, being financially motivated, are also likely to provide arbitrary responses to the survey questions. Since there is no correct response in a survey like this, it is difficult to establish post hoc whether the responses provided are meaningful or just noise.

To negate undue noise from from (cheating) participants, several possible solutions have been suggested (Kittur et al., 2008; Kelley, 2010; Mason & Suri, 2010). In this study we use four measures: 1) language, 2) HIT approval rating, 3) completion times, 4) validation questions. Given the complex language of the survey, participants were required to be native english speakers and this was advertised cogently in the job solicitation. (For example, we used SUS to measure the usability of Facebook controls. However, SUS has been found to be unreliable with non-native English speakers (Finstad, 2006).) Participants were then asked to note their native tongue in the middle of survey; those who responded with a language other than English, e.g. Hindi, were disqualified.

HIT refers to Human Intelligence Task. HIT approval ratings refers to the number of times the individual had previously successfully completed tasks on AMT. We asked that only individuals with a HIT approval rating of more than 95% should participate. This was put in as an automatic filter on AMT. Thus, individuals with lower ratings simply could not participate.

Completion times refers to the time it takes for an individual to complete the survey. Given the length of the survey (and based on the time it took for participants to complete the survey in testing/pilot stage) we presumed that the minimum amount of time required to complete the survey was 3 minutes. Thus, individuals who took less than 3 minutes were automatically disqualified.

We also asked participants two validation questions interspersed with survey questions. Validation questions have normatively correct/expected answers as compared to the survey responses. The job solicitation informed the participants that compensation for the task was contingent on answering the validation question correctly. Thus, for participants who are interested in being reimbursed would have to pay attention to all questions (since the validation questions did not differentiate themselves from survey questions).

For example, participants were asked to identify which social network they currently use, with one of the options being Facebook. Since participants were required to current Facebook users, those that did not choose the option were automatically disqualified. Participants were also asked to identify (from a list) the items for whom they did not provide the risk of sharing. Two of these items were favorite poem and favorite animal. Participants that did not select both were not included in the analysis.

3.3. Procedure

The survey was implemented using HTML/JavaScript so it could be completed using a standard web browser. The participants were randomly assigned either the benefit survey or the risk survey when they first visited the survey to avoid any selection biases associated with running each type independently. As the participants progressed, the survey would highlight areas they forgot to fill out or incorrectly filled out to help eliminate excessive rejections. We conducted the survey using Amazon's Mechanical Turk service. Participants were required to have a task approval rate of 95% or higher to avoid scammers. Additionally, participants were required to be located in the United States; this was verified by the mailing address associated with the participant's billing information. We received 400 responses in total, which was reduced to 376 after eliminating responses from participants that did not submit complete responses or did not follow the directions correctly.

3.4. Data Analysis

The data analysis was conducted in R. We examined the distribution of the various variables using Shapiro test. If the variables were not normally distributed we employed non-parametric tests; for example, we report the Spearman's ρ rather than Pearson's correlation coefficient. We used R's default packages to compute correlations. We also computed the validity of the three privacy paradox models based on their ability to explain the variance in: 1) information shared, 2) perceived risk, and 3) frequency of use of privacy controls. We calculated the linear regression given by 1, where IB refers to the distinct constructs of information sharing behaviors that correspond to the three explanations of the privacy paradox. The model is examined for both multicollinearity and heteroskedasticity. If the variance inflation factor is greater than 5 we assume multicollinearity; we examined heteroskedasticity using the Breuch Pagan test. In the presence of multicollinearity we leave the redundant independent variables out of

the regression models; in the presence of heteroskedasticity we compute the model estimates and standard errors using White-Huber corrected covariance matrices (Arellano, 1987). Finally, we examined whether the model can be reduced to a simpler underlying factors space; we use R's 'psych' to conduct factor analysis (assuming a varimax rotation as it provides the most orthogonal components).

$$\begin{aligned} IB = \beta_0 + \beta_1 * Gender + \beta_2 * Age + \beta_3 * Income + \beta_4 * Education \\ + \beta_5 * PrivacyPreferences + \beta_6 * Voluntariness + \beta_7 * Immediacy \\ + \beta_8 * Experts + \beta_9 * Exposed + \beta_{10} * Control + \beta_{11} * Newness \\ + \beta_{12} * Common - dread + \beta_{13} * Chronic - catastrophic + \\ \beta_{14} * Severity + \beta_{15} * Usability \end{aligned} \tag{1}$$

4. Results

This study investigates the privacy paradox and the three canonical explanations, i.e. people don't care, people don't know, and usability. It is outside the scope of this paper to provide an explicit normative definition of privacy. Gurses & Berendt (2010) provide a three dimensional categorization of privacy, which we adapt and adopt so as to make clear which aspects of privacy are being evaluated in this study. First, we consider privacy as confidentiality, i.e. in order to be private individuals must limit sharing. This is enumerated by the outcome variable, which measures whether the individual information items are shared or not and with whom. Second, privacy as control is examined by looking at privacy controls and the respective frequency of use. Finally, privacy as risk communication (or counter-surveillance) examines individual awareness of consequences and thus can be loosely mapped to perceptions of privacy risk. The three distinct explanations are examined using a survey-based study with 376 participants; description statistics regarding the participant sample and their responses have been included in the Appendix Appendix A.

We begin by presenting an empirical evaluation of the various hypotheses posited in section 2. We computed the correlation as Spearman's ρ; the results are given in table 1. Note that when both variables are present in both the benefit and risk group, e.g. age and information shared, we present the correlation of both groups together. We also compared the relationship between perceived risk and perceived benefit of sharing information; figure 1

examines the tradeoff for information sharing with friends, friends of friends, and everyone. (A straight forward correlation, and thus rejection of $H_{0_{01}}$, $H_{0_{02}}$, and $H_{0_{03}}$ is not possible since, the risk and benefit answers are given by different groups and thus are not paired.)

We also examined the validity of the three explanations of privacy paradox, along with the demographic variables, towards explaining privacy behaviors. So we conducted linear regression analysis based on Ordinary Least Squares, to the examine whether the variance is statistically significant or not. Since many of the independent variables were highly correlated we examined the regression model for multicollinearity. We assumed that a variance inflation factors of greater than 5 indicates the presence of multicollinearity. However, VIF values were less than 5 for the model. In addition we also examined the individual models for heteroskedasticity using Breuch Pagan test; if the residuals for the model were not normally distributed we calculated the model estimates using the White Huber covariance matrices that correct for heteroskedasticity (Arellano, 1987). The results have been presented in table 2.

Table 1: Hypothesis Testing: Correlation Analyses

ρ	Info. Shared	Perceived Risk			Controls
		f	fof	all	
Gender	-0.074***	-0.073***	-0.016	-0.031	0.018
Age	-0.079***	0.008	0.006	0.032*	-0.084***
Income	-0.082***	-0.006	-0.017	-0.015	-0.017
Education	-0.050***	0.081***	0.089***	0.099***	0.073***
Privacy Pref.	-0.059***	0.018	0.082***	0.046**	0.162***
Voluntary	-0.079***	0.155***	0.180***	0.182***	-0.001
Immediacy	-0.068***	0.052**	0.054***	0.062 ***	-0.22
Exposed	-0.053**	-0.003	-0.056***	-0.023	-0.037***
Experts	0.007	-0.032 *	-0.080***	-0.066***	0.051***
Control	0.012	-0.075***	-0.041*	-0.064***	-0.032**
Newness	-0.032**	0.042**	0.086***	0.093***	-0.018
Common-Dread	-0.191***	0.25***	0.395***	0.369***	0.063***
Chronic-Cat.	-0.027*	0.1456***	0.238***	0.248***	0.029**
Severity	-0.138***	0.268***	0.464***	0.453***	0.048***
Usability	0.057***	-0.044**	-0.087***	-0.075***	0.077***
p-value: *** $<$ 0.001 $<$ ** $<$ 0.01 $<$ * $<$ 0.05					

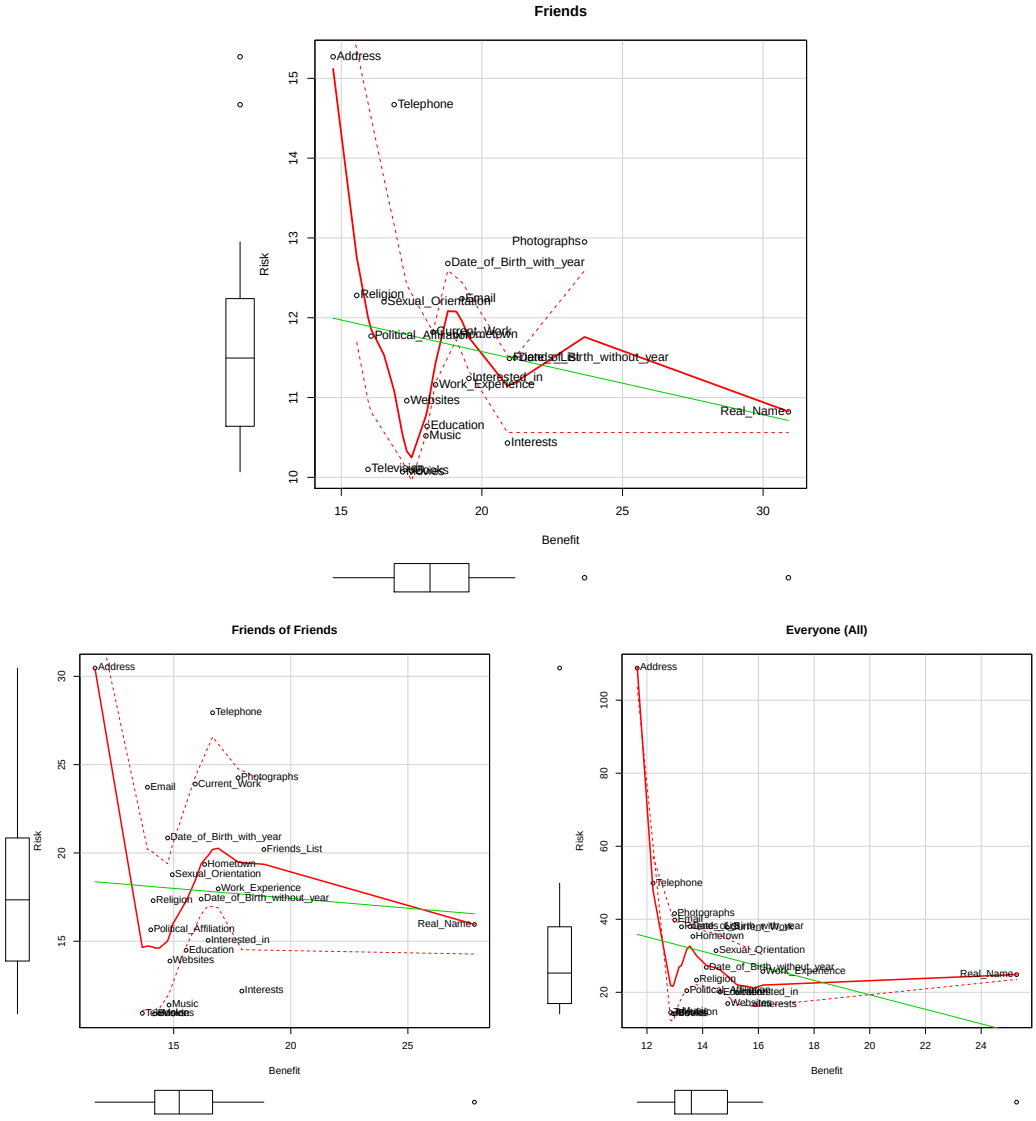

Figure 1: Risk vs. Benefit of Information Sharing

Table 2: Model Testing: Regression Analyses

Info. Behavior	Info. Shared		Perceived Risk						Privacy Controls	
	(*100)		f (*100)		fof (*10)		all		(*100)	
	E	SE	E	SE	E	SE	E	SE	E	SE
(Intercept)	164.66	7.686***	938.50	55.283***	84.61	21.751***	66.53	23.216**	104.99	8.474***
Gender	-8.13	1.997***	-56.95	24.279*	-26.97	11.612*	-17.76	6.005**	-1.50	2.171
Age	-2.92	0.549***	-3.35	6.141	-6.98	2.007***	0.72	1.704	-6.76	0.622***
Income	-2.63	0.508***	1.38	6.674	12.18	3.229***	-0.46	1.722	-2.63	0.604***
Education	-1.62	1.192	23.10	10.004*	18.80	3.459***	-1.42	3.724	15.38	1.286***
Privacy Preferences	-0.45	0.167**	6.67	2.044**	3.71	1.036***	0.29	0.470	2.53	0.172***
Voluntary	-1.82	0.466***	47.01	9.575***	17.52	4.518***	1.92	1.434	-1.18	0.523*
Immediacy	-1.39	0.437**	0.73	4.740	-0.65	2.074	0.85	1.388	-0.61	0.488
Exposed	-1.29	0.438**	16.18	6.024**	10.58	3.248**	3.71	1.341**	-1.27	0.491**
Experts	0.38	0.507	-16.83	5.036***	-10.30	2.603***	0.42	1.559	3.38	0.579***
Control	0.21	0.414	-17.81	6.059**	-11.05	2.574***	-4.16	1.245***	0.44	0.472
Newness	-0.48	0.437	18.01	3.046***	5.98	1.310***	0.29	1.323	-0.64	0.475
Common-Dread	-6.79	0.546***	-0.82	8.311	1.29	3.625	1.64	1.791	2.66	0.649***
Chronic-Catastrophic	1.55	0.464***	38.03	11.818**	22.45	6.015***	3.68	1.614*	-1.21	0.578*
Severity	-1.36	0.568*	15.05	8.860	0.26	3.462	2.17	1.800	-0.02	0.650
Usability	0.06	0.045	-4.17	0.915***	-2.62	0.496***	-0.94	0.136***	0.37	0.052***
p-value: *** $<$ 0.001 $<$ ** $<$ 0.01 $<$ * $<$ 0.05										
Residual Err./df	83.56/7231		744.2/3702		355.7/3671		180.2/3711		91.42/7231	
Missing Observations	1025		528		559		519		1025	
Multiple R-squared	0.0590		0.0709		0.0816		0.02845		0.0814	
Adjusted R-squared	0.571		0.0671		0.07785		0.02453		0.07949	
F-Statistic	$30_{15,7231}$ * **		$18.84_{15,3702}$ * **		$21.74_{15,3671}$ * **		$7.24_{15,3711}$ * **		$42.71_{15,7231}$ * * * *	

Table 3: Model Components: Factor Analyses

	F1	F2	F3	F4	F5	F6	F7	U
Gender					0.693		0.112	0.498
Age					0.206		-0.128	0.931
Income		0.109				0.269		0.903
Education				-0.109		0.504	-0.126	0.705
Privacy Preferences	0.117			-0.216				0.928
Voluntariness	0.236	0.235						0.868
Immediacy		0.869				0.101		0.227
Exposed		0.345	0.365	-0.183			-0.211	0.669
Experts			0.822					0.312
Control				0.631				0.598
Newness			-0.150	0.256				0.894
Common-Dread	0.752						-0.101	0.422
Catastrophic-Catastrophic	0.482							0.758
Severity	0.810							0.334
Usability							0.423	0.813
SS loadings	1.540	0.957	0.863	0.577	0.547	0.354	0.301	
Proportion Var	0.103	0.064	0.058	0.038	0.036	0.024	0.020	
Cumulative Var	0.103	0.166	0.224	0.262	0.299	0.323	0.343	

We also conducted factor analysis, since many of the independent variables were intercorrelated, on the model to understand the underlying components. We used R's psych package and use a varimax rotation, as it gives the most orthogonal components. We conducted a Scree test to identify the number of components; considering components with eigenvalues greater than 1 resulted in 7 distinct factors. The results of the factor analysis are given in table 3. The degrees of freedom for the model is 21 and the fit was 0.0142.

5. Discussion

Individuals who share information simultaneously express a concern regarding privacy. There are distinct explanations for this paradox in the privacy literature, we focus on three: 1) people don't care, 2) people don't know, and 3) usability. In this paper we examine the relative importance of each explanation for information sharing behaviors on Facebook. We operationalize the three corresponding information behaviors as: 1) information shared, 2) perceived risk, and 3) frequency of use of Facebook privacy controls. From table 2, it is evident that all three information sharing behaviors can be explained by the distinct conceptualizations of the privacy paradox, albeit to varying degrees (as suggested by the different adjusted R-square values for each model). Simultaneously, the different variables that correspond to the distinct conceptualizations of the privacy paradox can be reduced to an underlying factor space, table 3.

The most significant of these factors constitutes common-dread, chronic-catastrophic, and severity; this factor is similar to *dread*, as defined by Fischhoff et al. (1978). Of these severity the maximum amount of variance in the model that combines the three explanations of the privacy paradox. $H_{0_{43}}$, $H_{0_{44}}$, and $H_{0_{45}}$ can all be rejected. Individuals who considered consequences of sharing to be more severe shared less, perceived the risk of sharing to be higher, were concerned about limiting the audience, and used privacy controls more frequently. Thus, when the consequences are more severe individual behaviors are more aligned with their privacy expectations.

The same is true for common-dread and chronic-catastrophic. $H_{0_{37}}$, $H_{0_{38}}$, $H_{0_{39}}$, $H_{0_{40}}$, $H_{0_{41}}$,and $H_{0_{42}}$ can all be rejected. When the information shared was rare and the implication catastrophic individuals shared less, perceived a higher risk of sharing, were inclined towards limiting the audience, and used privacy controls to implement their expectations. Thus,

dread risk is the most significant determinant of privacy behaviors on Facebook, as it is offline (Fischhoff et al., 1978), despite the lack of physical harm.

The second and third factors constitute immediacy and knowledge, to the exposed and experts; thus, the second and third factor together are similar to *familiarity*, as as defined by Fischhoff et al. (1978). Immediacy explained more variance than knowledge to exposed/experts. $H_{0_{22}}$ and $H_{0_{23}}$ can be rejected, while $H_{0_{24}}$ can not. When the consequences of sharing were immediate individuals shared less, perceived higher risk of sharing, wanted to limit the audience of the posts, but did not use privacy controls more often. Thus, when the consequences were immediate the expression of privacy was primarily as confidentiality.

The association between knowledge and information behaviors in more complex. $H_{0_{25}}$ and $H_{0_{27}}$ can be rejected, while $H_{0_{26}}$ can be rejected partially. When individuals perceived more knowledge about the risk they shared less information and used privacy controls less; the relationship between knowledge to exposed and perceived risk is difficult to establish. $H_{0_{29}}$ and $H_{0_{30}}$ can be rejected, while $H_{0_{28}}$ can not. Thus, when experts are perceived to have more knowledge the perceived risk of information sharing is lower, individuals are less concerned about limiting the audience of their posts, and privacy controls are used more frequently. It is likely then that if experts are seen to know more about privacy risks individuals demonstrate risk compensation, i.e. the increased use of controls alleviates the perception of risk. Thus, here the expression of privacy is as control.

Voluntariness correlated with both the first and the second factor. It is also a significant component of the regression model, though its significance diminishes when as the audience of the posts increases. When information sharing appears voluntary people share more; simultaneously, the perceived risk of sharing is lower and so is the concern about sharing information with a larger audience. It is then not surprising that individuals do not use privacy controls; $H_{0_{19}}$ and $H_{0_{20}}$ can be rejected and $H_{0_{21}}$ can not.

The two remaining variables that correspond to the paradigm of people don't know, under bounded rationality, are control and newness. Together they constitute factor four, where control explains more variance in the model compared to newness. $H_{0_{32}}$ and $H_{0_{33}}$ can be rejected, while $H_{0_{31}}$ can not be. Thus, when the control appears greater the perceived risk of sharing is lower; simultaneously, controls are used less frequently. Individuals continue to share the same amount of information. This indicates that more

trust in controllability can both reduce the adoption of privacy controls while alleviating the perception of risk. From a policy perspective, Facebook may invest in creating more awareness of their controls as it reduces adoption and thus leads to increased audience for the posts.

Of all the dimensions of risk perception, newness had the least impact on information behaviors. $H_{0_{34}}$ and $H_{0_{35}} can be rejected, while H_{0_{36}}$ can not. Thus, when the information shared appears new individuals share more, the perceived risk of sharing is lower, while there is no impact on the frequency of use of privacy controls. Since the information shared is new, individuals may not fully understand the repercussions of sharing. Alternatively, sharing new information may lead to more social capital.

The nine determinants of perceived risk all constitute the first four factors of the model that describe the underlying components of the three explanations of the privacy paradox, for Facebook. Thus, we argue that the foremost explanation of the privacy paradox is that *people don't know*; thus, the solution is risk communication. The first two correspond to *dread and familiarity*, as as defined by Fischhoff et al. (1978) for offline risks, despite the lack of physical harm on Facebook. Thus, privacy decisions can be modeled as generic risk decisions under bounded rationality. Privacy risk communication on Facebook can draw from prior literature on offline risks. For example, risk information can be used more accessible by using appropriate mental models Garg et al. (2012a). Intuitively, the content of risk communication should focus on the factor space identified here and present the consequences of risk to be severe, catastrophic, and rare to encourage risk averse behaviors.

Gender differences represent factor 5 in the factor space that underlies the three explanations of privacy paradox examined in this paper. $H_{0_{04}}$ can be rejected; $H_{0_{05}}$ can be partially rejected; and $H_{0_{06}}$ can not be rejected. Women share less information compared to men; simultaneously, men perceive the risk of information sharing to be higher. Thus, men demonstrate risk taking behaviors, while women are risk averse on Facebook. Gender does not, however, correlate with the adoption of privacy controls. Gender differences also account for a significant amount of variance in all dependent variables, except adoption of privacy controls. We therefore argue that gender has a significant impact on information behaviors.

$H_{0_{07}}$ and $H_{0_{09}}$ can be rejected; $H_{0_{08}}$ can be partially rejected. Older adults share less information than younger cohorts. Age, however, correlates with the adoptions of privacy controls; younger adults are more engaged in

actively protecting their privacy than the elders. The perceived risk of information did not differ significantly based on age. However, older adults wanted to limit the size of their audience. Age was a minor component of factor 5 in the factor space. Overall, age differences are less significant than gender differences and primarily indicate lower participation on Facebook.

$H_{0_{10}}$ can be rejected; there was no evidence to reject $H_{0_{11}}$ and $H_{0_{12}}$. Individuals with higher income shared less information. However, the perceived risk of information sharing or adoption of privacy controls did not differ based on incomes. This indicates that higher incomes are more risk averse compared to lower income participants. The difference in income explains significant amount of variance in information shared, adoption of privacy controls, and perceived risk of sharing with friends of friends. Overall, income as a minor component of factor 6, explains a small but significant variance in the three underlying models of the privacy paradox and the information behaviors they correspond to.

Factor 6 is, however, primarily determined by education. More educated individuals shared less, perceived higher risk of sharing, were more inclined to limit the audience, and more frequently used privacy control to implement their inclination. Thus, $H_{0_{13}}$, $H_{0_{12}}$, and $H_{0_{13}}$ can all be rejected. Education's strong influence on information behaviors, table 2 and its significant contribution in explaining the variance in the underlying model, table 3, implies that more educated individuals implement better privacy decisions or decisions more aligned with their attitudes. This furthers our contention that the privacy paradox manifests because *people don't know.*

A second and weaker explanation is usability. It constitutes as factor 7, which explains the least amount of variance in the model that can be considered significant. $H_{0_{46}}$, $H_{0_{47}}$, and $H_{0_{48}}$ can all be rejected. When Facebook controls were considered usable individuals shared more, the perceived risk of sharing was lower as well as that of a bigger audience, and the frequency of use of privacy controls was higher. From a policy perspective perspective, Facebook should be invested in providing more usable controls, as usability is a significant indicator of Facebook use and results in more information sharing in a less restrictive manner that still aligns with user preferences. Overall, we argue that when people know the risk of information, the limited usability of privacy controls is a secondary deterrent to implementing privacy expectations for Facebook users.

The third explanation that people don't care, or privacy preferences, does not constitute a significant component of either of the factors; its high

uniqueness indicates that it has the highest amount of variance not explained in the model. $H_{0_{16}}$ and $H_{0_{18}}$ can be rejected, while $H_{0_{17}}$ can be partially rejected. Individuals who cared about privacy shared less, perceived a higher risk of sharing beyond the immediate friend circle, and used privacy controls more frequently. This indicates that individuals who cared more about privacy demonstrated information sharing behaviors aligned with their attitudes, with little evidence for paradox. Thus, we infer that privacy preferences is the least important factor underlying the privacy paradox.

Finally, it is interesting to examine the relationship twixt perceived risk and perceived benefit. The two obvious outliers are address and real name. Sharing the address is consistently perceived to be high risk and low benefit; simultaneously, sharing the real is seen as high benefit and low risk. Sharing the date of birth is always more benefit and less risk without the year than with it. There is no clear correlation between risk and benefit; though most information is considered to have either some risk and no benefit or some benefit and no risk. For privacy behaviors, it seems that individuals compartmentalize information into two distinct categories, one that is risky and the other that is beneficial; thus, individuals may not consider a tradeoff.

6. Conclusion & Future Work

There are three classic explanations of the privacy paradox: 1) people don't care, 2) people don't know, and 3) usability. In this paper we examined the relative strengths of the three as well as their ability to explain the amount of the information shared, the perceived risk of information sharing, and frequency of use of privacy controls; these correspond to three conceptualizations of privacy, or information behaviors, as confidentiality, control, and counter-surveillance. We find that variance in information behaviors is foremost explained by variables that correspond to people don't know. A second factor is demographic, specifically gender differences and education. The third significant factor was usability. When these factors are accounted for, people don't care has negligible impact on the model that underlies the three paradigms of the privacy paradox.

We argue that Facebook should invest in both more usable privacy controls and awareness of those controls. In general better controls and more information increased information sharing and lowered the perceptions of risk, thereby aligning expressed attitudes with observed behaviors and addressing the paradox. We note that privacy risks behaviors are determined

by *dread risk and familiarity* on Facebook, as for risks offline. Thus, Facebook privacy efforts should leverage prior research in risk communication offline. Specifically, risk averse behaviors can be encouraged if risk communication focuses on severe, catastrophic, and rare consequences of information sharing.

There are several limitations to this research. Risk behaviors are often continent on culture (Wildavsky & Dake, 1990), which is not examined here. Privacy behaviors also depend on context (Nissenbaum, 2009). The findings are not generalizable to other platforms and are specific to Facebook. Even within Facebook the participant pool is not a representative sample. Future research should address the limitations of this research, as well examine the three constructs through qualitative methods to extract a deeper understanding. Finally, future work should compare risk across domains, e.g. information sharing on Facebook vs. Twitter.

Acknowledgements

Withheld for review.

Appendix A. Descriptive Statistics

There were a total of 376 participants, of which 200 self identified as female, 176 as male, and 0 as other. 193 participants were assigned to the risk survey; 101 females and 92 males. 183 were assigned to the benefit survey; 99 females and 84 males. The distribution of participants by age, income, and education is given by tables A.4, A.5, and A.6 respectively. The distribution of participants by Facebook use, i.e. frequency of access, location sharing, status message update, and privacy settings customization is given by tables A.7, A.8, A.9, and A.10 respectively. Tables A.11 and A.12 note the mean risk and benefit of sharing individual information items on Facebook (with friends, friends of friends, and everyone); standard deviation of the respective means are parenthetically enclosed. Table A.13 presents the average amount of information shared by risk and benefit groups. (Not sharing an information item, e.g. real name, is coded as 0; sharing with friends, friends of friends, and everyone is coded as 1, 2, and 3 respectively.)

References

Ackerman, M., & Cranor, L. (1999). Privacy critics: Ui components to safeguard users' privacy. In *CHI'99 extended abstracts on Human factors in computing systems* (pp. 258–259). ACM.

Table A.4: Age

Age	Risk	Benefit
18-25	61	66
26-30	53	45
31-35	31	28
36-40	15	9
41-45	12	18
46-50	10	5
51-55	8	5
56-60	3	2
61-66	0	5

Table A.5: Income

Income	Risk	Benefit
<$ 10,000	9	16
$10,000-20,000	17	20
$20,000-30,000	26	23
$30,000-50,000	40	43
$50,000-75,000	50	35
$75,000-100,000	20	20
$100,000>	20	16
Don't Know	11	10

Table A.6: Education

Education	Risk	Benefit
Less than high school	2	1
High School	9	9
Some College	82	98
College graduate	70	47
Post-graduate training	30	28

Table A.7: Facebook Access

Frequency	Risk	Benefit
Less than once a month	4	5
Once a month	5	3
Once a week	26	17
Once a day	48	41
Several times a day	95	97
It's always on	15	20

Table A.8: Location Sharing

Frequency	Risk	Benefit
Less than once a month	150	134
Once a month	28	22
Once a week	12	16
Once a day	2	9
Several times a day	1	2

Table A.9: Status Message Update

Frequency	Risk	Benefit
Less than once a month	47	53
Once a month	33	29
Once a week	82	60
Once a day	23	25
Several times a day	8	16

Table A.10: Privacy Settings Customization

Frequency	Risk	Benefit
I have never changed my privacy settings	15	16
Less than once a year	31	25
Once a year	66	71
Once a month	81	67
Once a week	0	3
Once a day	0	1
Several times a day	0	0

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce* (pp. 21–29). ACM.

Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. *Security & Privacy, IEEE*, *7*, 82–85.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *Security & Privacy, IEEE*, *3*, 26–33.

Adams, J. (1999). Cars, cholera, and cows. *Policy Analysis*, (pp. 1–49).

Adu-Oppong, F., Gardiner, C., Kapadia, A., & Tsang, P. (2008). Social circles: Tackling privacy in social networks. In *Symposium on Usable Privacy and Security (SOUPS)*.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*, 610–613.

Arellano, M. (1987). Computing robust standard errors for within-groups estimators. *Oxford bulletin of Economics and Statistics*, *49*, 431–434.

Awad, N., & Krishnan, M. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS quarterly*, *30*, 13–28.

Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An empirical evaluation of the system usability scale. *Intl. Journal of Human–Computer Interaction*, *24*, 574–594.

Barnes, S. B. (2006). A privacy paradox: Social networking in the united states. *First Monday*, *11*.

Bhatnagar, A., Misra, S., & Rao, H. (2000). On risk, convenience, and Internet shopping behavior. *Communications of the ACM*, *43*, 105.

Bilton, N. (2012). *Girls Around Me: An App Takes Creepy to a New Level*. Technical Report New York Times. URL: `http://bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new-level/`.

Böhme, R., & Koble, S. (2007). On the viability of privacy-enhancing technologies in a self-regulated business-to-consumer market: Will privacy remain a luxury good? In *Workshop on Economics of Information Security. Available at (http://weis2007. econinfosec. org/papers/30. pdf)*. Citeseer.

Bonneau, J., & Preibusch, S. (2009). The privacy jungle: On the market for data

Table A.11: Risk Ratings: Mean (Standard Deviation)

Information	Friends	FoF	Everyone
Address	15.27 (13.21)	30.47 (48.42)	108.8 (736.97)
Books	10.08 (0.56)	10.89 (6.81)	14.1 (36.49)
Current Work	11.82 (7.81)	23.9 (53.06)	37.76 (97.61)
Date of Birth with year	12.68 (10.38)	20.85 (40.03)	38.01(106.42)
Date Birth without year	11.50 (8.00)	17.39 (38.63)	26.83 (78.51)
Education	10.64 (3.52)	14.49 (19.95)	20.06 (39.81)
Email	12.24 (8.78)	23.72 (57.65)	39.81 (106.61)
Friends List	11.49 (6.24)	20.2(59.38)	37.94 (138.27)
Hometown	11.78 (9.19)	19.35 (39.11)	35.3 (105.07)
Interested In	11.24 (4.75)	15.05 (20.46)	19.91 (39.37)
Interests	10.43 (1.91)	12.18 (8.40)	16.68 (36.91)
Movies	10.07 (0.49)	10.92 (6.84)	14.13 (36.40)
Music	10.52 (5.23)	11.39 (8.57)	14.61 (36.71)
Photographs	12.95 (8.94)	24.26 (41.10)	41.57 (87.78)
Political Affiliation	11.77 (4.93)	15.65 (19.66)	20.45 (38.99)
Real Name	10.82 (6.73)	15.95 (37.04)	24.84 (74.83)
Religion	12.28 (8.29)	17.3 (8.37)	23.25 (74.63)
Sexual Orientation	12.2 (10.10)	18.77 (40.83)	31.41 (106.81)
Telephone	14.67 (13.64)	27.94 (46.88)	49.89 (112.07)
Television	10.1 (0.63)	10.92 (6.84)	14.46 (36.77)
Websites	10.96 (6.07)	13.88 (20.09)	16.92 (37.75)
Work Experience	11.16 (7.14)	17.97 (38.88)	25.69 (75.62)

Table A.12: Benefit Ratings: Mean (Standard Deviation)

Information	Friends	FoF	Everyone
Address	14.71 (10.87)	11.64 (5.52)	11.65 (8.76)
Books	17.5 (15.42)	14.19 (10.37)	13.01 (11.07)
Current Work	18.26 (16.04)	15.92 (13.59)	14.89 (13.77)
Date of Birth with year	18.79 (19.35)	14.74 (12.88)	13.54 (14.62)
Date Birth without year	21.18 (20.93)	16.17 (16.02)	14.13 (15.84)
Education	18.05 (16.36)	15.53 (12.69)	14.63 (13.88)
Email	19.29 (17.63)	13.88 (9.83)	13 (11.97)
Friends List	20.98 (20.38)	18.85 (18.49)	13.24 (11.59)
Hometown	19.09 (18.39)	16.32 (14.46)	13.65 (13.21)
Interested In	19.54 (18.35)	16.47 (15.46)	15.23 (16.72)
Interests	20.91 (20.74)	17.91 (18.71)	15.88 (17.68)
Movies	17.18 (15.52)	14.39 (11.31)	12.94 (11.02)
Music	18.01 (17.26)	14.8 (13.07)	13.15 (11.11)
Photographs	23.65 (21.77)	17.75 (17.58)	12.99 (11.31)
Political Affiliation	16.06 (17.03)	14.02 (12.37)	13.43 (13.59)
Real Name	30.9 (78.66)	27.84 (82.36)	25.27 (80.76)
Religion	15.55 (15.31)	14.12 (15.31)	13.78 (15.06)
Sexual Orientation	16.52 (16.02)	14.94 (14.82)	14.48 (15.52)
Telephone	16.88 (14.84)	16.66 (50.79)	12.22 (11.04)
Television	15.95 (12.83)	13.66 (10.12)	12.85 (11.15)
Websites	17.33 (16.06)	14.84 (14.1)	14.9 (16.11)
Work Experience	18.35 (16.65)	16.9 (16.27)	16.16 (16.73)

Table A.13: Information Sharing Behaviors

Information	Benefit	Risk
Address	0.32 (0.51)	0.29 (0.48)
Books	0.99 (0.94)	0.98 (0.77)
Current Work	0.96 (0.90)	0.82 (0.70)
Date of Birth with year	0.85 (0.85)	0.88 (0.83)
Date Birth without year	1.10 (0.91)	1.15 (0.85)
Education	1.14 (0.92)	1.08 (0.77)
Email	0.85 (0.71)	0.83 (0.64)
Friends List	1.20 (0.81)	1.14 (0.70)
Hometown	1.21 (0.92)	1.18 (0.80)
Interested In	0.86 (0.89)	0.87 (0.84)
Interests	1.16 (0.84)	1.15 (0.72)
Movies	0.97 (0.93)	1.03 (0.80)
Music	1.00 (0.88)	1.06 (0.79)
Photographs	1.13 (0.65)	1.61 (0.58)
Political Affiliation	0.80 (0.96)	0.65 (0.69)
Real Name	1.65 (0.93)	1.60 (0.88)
Religion	.80 (0.92)	0.69 (0.76)
Sexual Orientation	0.86 (0.90)	0.84 (0.86)
Telephone	0.44 (0.59)	0.46 (0.55)
Television	0.93 (0.92)	0.96 (0.78)
Websites	0.91 (0.89)	0.80 (0.82)
Work Experience	0.95 (0.89)	0.84 (0.73)

protection in social networks. *The Eighth Workshop on the Economics of Information Security*, .

Boyd, D. (2009). Why youth (heart) social network sites: The role of networked publics in teenage social life. In *MacArthur Foundation Series on Digital Learning Youth, Identity, and Digital Media Volume*. Cambridge, MA: MIT Press.

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, *15*.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science*, *4*, 340–347.

Brooke, J. (1996). Sus-a quick and dirty usability scale. *Usability evaluation in industry*, *189*, 194.

Brown, J., & Goolsbee, A. (2002). Does the Internet make markets more competitive? Evidence from the life insurance industry. *Journal of political economy*, *110*, 481–507.

Caine, K., Kisselburgh, L. G., & Lareau, L. (2011). Audience visualization influences disclosures in online social networks. In *CHI'11 Extended Abstracts on Human Factors in Computing Systems* (pp. 1663–1668). ACM.

Camp, L. (2009). Mental models of privacy and security. *IEEE Technology and Society*, *28*, 37–46.

Cassell, M., Halperin, D., Shelton, J., & Stanton, D. (2006). Risk compensation: The achilles' heel of innovations in HIV prevention? *British Medical Journal*, *332*, 605–607.

Christofides, E., Muise, A., & Desmarais, S. (2012). Hey mom, whats on your facebook? comparing facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science*, *3*, 48–54.

Conti, G., Ahamad, M., & Stasko, J. (2005). Attacking information visualization system usability overloading and deceiving the human. In *Proceedings of the 2005 symposium on Usable privacy and security* (pp. 89–100). ACM.

Cranor, L. (2008). A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security* (pp. 1–15). USENIX Association.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*, 83–108.

DiGioia, P., & Dourish, P. (2005). Social navigation as a model for usable security. In *Proceedings of the 2005 symposium on Usable privacy and security* (pp. 101–108). ACM.

Dourish, P., & Anderson, K. (2006). Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-computer interaction*, *21*, 319–342.

Drennan, J., Mort, G., & Previte, J. (2006). Privacy, risk perception, and expert online behavior: an exploratory study of household end users. *Journal of Organizational and End User Computing*, *18*, 1–22.

Edelman, B. (2009). Adverse selection in online trust certifications. In *Proceedings of the 11th International Conference on Electronic Commerce* (pp. 205–212). ACM.

Edwards, W., Poole, E., & Stoll, J. (2008). Security automation considered harmful? In *Proceedings of the 2007 Workshop on New Security Paradigms* (pp. 33–42). ACM.

Egelman, S., Oates, A., & Krishnamurthi, S. (2011). Oops, i did it again: Mitigating repeated access control errors on facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2295–2304). ACM.

Finstad, K. (2006). The system usability scale and non-native english speakers. *Journal of usability studies*, *1*, 185–188.

Fischhoff, B., Bostrom, A., & Quadrel, M. J. (1993). Risk perception and communication. *Annual review of public health*, *14*, 183–203.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How safe is safe enough? a psychometric study of attitudes towards technological risks and benefits. *Policy sciences*, *9*, 127–152.

Forsythe, S., & Shi, B. (2003). Consumer patronage and risk perceptions in Internet shopping. *Journal of Business Research*, *56*, 867–875.

Freudiger, N. V. J. (2011). The inconvenient truth about web certificates. In *Workshop on the Economics of Information Security*.

Garg, V., & Camp, J. (2012). End user perception of online risk under uncertainty. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 3278–3287). IEEE.

Garg, V., & Camp, J. (2013). Cars, condoms, and facebook. In *Information Security Conference*.

Garg, V., Camp, L. J., Connelly, K., & Lorenzen-Huber, L. (2012a). Risk communication design: video vs. text. In *Privacy Enhancing Technologies* (pp. 279–298). Springer.

Garg, V., Camp, L. J., Lorenzen-Huber, L., & Connelly, K. (2012b). Risk communication design for older adults. *Gerontechnology*, (pp. 166–173).

Garg, V., & Nilizadeh, S. (2013). Craigslist scams and community composition: Investigating online fraud victimization. In *International Workshop on Cyber Crime*. IEEE.

Garg, V., Patil, S., Kapadia, A., & Camp, L. J. (2013). Peer-produced privacy protection. In *Symposium on Technology and Society*. ACM.

Grimmelmann, J. (2009). Saving Facebook. *Iowa L. Rev.*, *94*, 1137–1206.

Gurses, S., & Berendt, B. (2010). PETs in the Surveillance Society: A Critical Review of the Potentials and Limitations of the Privacy as Confidentiality Paradigm. *Data Protection in a Profiled World*, (pp. 301–321).

Hoofnagle, C., King, J., Li, S., & Turow, J. (2010). *How different are young adults from older adults when it comes to information privacy attitudes and policies?*. Technical Report Social Science Research Network. URL: `http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864`.

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult facebook users. *Journal of Interactive Advertising*, *10*, 28–45.

Huang, D.-L., Patrick Rau, P.-L., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on it adoption and security practices. *International Journal of Human-Computer Studies*, *69*, 870–883.

Huberman, B. A., Adar, E., & Fine, L. R. (2005). Valuating privacy. In *Workshop on the Economics of Information Security*. Cambridge, MA, USA. URL: `http://infosecon.net/workshop/pdf/7.pdf`.

Iachello, G., & Hong, J. (2007). End-user privacy in human-computer interaction. *Foundations and Trends in Human-Computer Interaction*, *1*, 1–137.

Inglesant, P., & Sasse, M. (2010). The true cost of unusable password policies: password use in the wild. In *Proceedings of the 28th international conference on Human factors in computing systems* (pp. 383–392). ACM.

Jarvenpaa, S., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information technology and management*, *1*, 45–71.

Keller, C., Siegrist, M., & Gutscher, H. (2006). The role of the affect and availability heuristics in risk communication. *Risk Analysis*, *26*, 631–639.

Kelley, P. (2010). Conducting usable privacy & security studies with amazons mechanical turk. In *Symposium on Usable Privacy and Security (SOUPS)(Redmond, WA*.

Kittur, A., Chi, E. H., & Suh, B. (2008). Crowdsourcing user studies with mechanical turk. In *Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems* CHI '08 (pp. 453–456). New York, NY, USA: ACM. URL: `http://doi.acm.org/10.1145/1357054.1357127`. doi:`10.1145/1357054.1357127`.

Liberman, N., Trope, Y., & Wakslak, C. (2007). Construal level theory and consumer behavior. *Journal of Consumer Psychology*, *17*, 113.

Lipford, H., Besmer, A., & Watson, J. (2008). Understanding privacy settings in Facebook with an audience view. In *Proceedings of the 1st Conference on Usability, Psychology, and Security* (pp. 1–8). USENIX Association.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Info. Sys. Research*, *15*, 336–355.

Malin, B., & Sweeney, L. (2001). Re-identification of dna through an automated linkage process. In *Proceedings of the AMIA Symposium* (p. 423). American Medical Informatics Association.

Mason, W., & Suri, S. (2010). Conducting behavioral research on amazons mechanical turk. *Behavior Research Methods*, (pp. 1–23).

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies,. *ISJLP*, *4*, 543.

Miyazaki, A., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs*, *35*, 27–44.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books.

Odlyzko, A. (2004). Privacy, economics and price discrimination on the internet. In L. J. Camp, & S. Lewis (Eds.), *Economics of Information Security* (pp. 187–212). New York, NY: Springer volume 12 of *Advances in Information Security*.

Park, C., & Jun, J. (2003). A cross-cultural comparison of Internet buying behavior: Effects of Internet usage, perceived risks, and innovativeness. *International Marketing Review*, *20*, 534–553.

Patil, S., & Kapadia, A. (2012). Are you exposed?: Conveying information exposure. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work Companion* (pp. 191–194). ACM.

Posner, R. (1977). Right of privacy, the. *Georgia Law Review*, *12*, 393–422.

Posner, R. (1981). The economics of privacy. *The American economic review*, *71*, 405–409.

Preibusch, S., Krol, K., & Beresford, A. R. (2012). The privacy economics of voluntary over-disclosure in web forms. In *Workshop in the Economics of Information Security*.

Reynolds, B., Venkatanathan, J., Gonçalves, J., & Kostakos, V. (2011). Sharing ephemeral information in online social networks: privacy perceptions and behaviours. In *Human-Computer Interaction–INTERACT 2011* (pp. 204–215). Springer.

Riegelsberger, J., Sasse, M. A., & McCarthy, J. D. (2003). Shiny happy people building trust?: photos on e-commerce websites and consumer trust. In *CHI '03: Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 121–128). New York, NY: ACM.

Rode, J., Johansson, C., DiGioia, P., Nies, K., Nguyen, D., Ren, J., Dourish, P., & Redmiles, D. (2006). Seeing further: extending visualization as a basis for usable security. In *Proceedings of the second symposium on Usable privacy and security* (pp. 145–155). ACM.

Salisbury, W., Pearson, R., Pearson, A., & Miller, D. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems*, *101*, 165–177.

Sasse, M., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link': a human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*, 122–131.

Sheehan, K. B. (2002). Toward a typology of internet users and online privacy concerns. *The Information Society*, *18*, 21–32.

Sherman, S. (1980). On the self-erasing nature of errors of prediction. *Journal of Personality and Social Psychology*, *39*, 211.

Shostack, A., & Sylverson, P. (2004). What price privacy? In L. J. Camp, & S. Lewis (Eds.), *Economics of Information Security* (pp. 129–142). New York, NY: Springer volume 12 of *Advances in Information Security*.

Sjoberg, L., & Fromm, J. (2001). Information technology risks as seen by the public. *Risk Analysis*, *21*, 427–442.

Slovic, P. (1987). Perception of risk. *Science (New York, NY)*, *236*, 280.

Smetters, D., & Grinter, R. (2002). Moving from the design of usable security technologies to the design of useful secure applications. In *Proceedings of the 2002 workshop on New security paradigms* (pp. 82–89). ACM.

Solove, D. J. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745.

Starr, C. (1969). Social benefit versus technological risk. *Science*, *165*, 1232–1238.

Steven E. Finkel, S. E., Guterbock, T. M., & Borg, M. J. (1991). Race-of-interviewer effects in a preelection poll virginia 1989. *Public Opinion Quarterly*, *55*, 313–330.

Stewart, A. (2004). On risk: perception and direction. *Computers & Security*, *23*, 362–370.

Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce*, *7*, 135–161.

Tan, S. (1999). Strategies for reducing consumers' risk aversion in Internet shopping. *Journal of Consumer Marketing*, *16*, 163–180.

Turner, C., Zavod, M., & Yurcik, W. (2001). Factors that affect the perception of security and privacy of e-commerce web sites. In *Fourth International Conference on Electronic Commerce Research, Dallas TX* (pp. 628–636). Citeseer.

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and

biases. *science*, *185*, 1124.

Varian, H. (1985). Price discrimination and social welfare. *The American Economic Review*, *75*, 870–875.

Varian, H. (1992). *Microeconomic analysis* volume 506. Norton New York.

Vila, T., Greenstadt, R., & Molnar, D. (2003). Why we can't be bothered to read privacy policies models of privacy economics as a lemons market. In *Proceedings of the 5th international conference on Electronic commerce* (pp. 403–407). ACM.

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011). I regretted the minute i pressed share: A qualitative study of regrets on facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (p. 10). ACM.

Whitten, A., & Tygar, J. (1999). Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *Proceedings of the 8th USENIX Security Symposium*. volume 99.

Wildavsky, A., & Dake, K. (1990). Theories of risk perception: Who fears what and why? *Daedalus*, *119*, 41–60.

Wolfgang, A., & Wolfgang, J. (1971). Exploration of attitudes via physical interpersonal distance toward the obese, drug users, homosexuals, police and other marginal figures. *Journal of Clinical Psychology*, *27*, 510–512.