E-waste Information Security Protection Motivation: The Role of Optimism Bias

<table>
<thead>
<tr>
<th>Journal:</th>
<th><em>Information Technology &amp; People</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>Manuscript ID</td>
<td>ITP-09-2019-0458.R2</td>
</tr>
<tr>
<td>Manuscript Type:</td>
<td>Article</td>
</tr>
<tr>
<td>Keywords:</td>
<td>Security &lt; Theoretical concept, Cognitive theories &lt; Theory, End users &lt; People, Electronic mediated environment &lt; Study setting, Information management &lt; IT/IS management &lt; Practice, Empirical study &lt; Methodology, Hypothesis testing &lt; Methodology, Survey &lt; Methodology, Structural equation modeling &lt; Quantitative method &lt; Method</td>
</tr>
</tbody>
</table>
E-waste Information Security Protection Motivation: 

The Role of Optimism Bias

Abstract

Purpose - Electronic waste (e-waste) such as discarded computers and smartphones may contain large amounts of confidential data. Improper handling of remaining information in e-waste can, therefore, drive information security risk. This risk, however, is not always properly assessed and managed. We take the Protection Motivation Theory (PMT) lens of analysis to understand intentions to protect one’s discarded electronic assets.

Design/methodology/approach - By applying structural equation modeling, we empirically tested the proposed model with survey data from 348 e-waste handling users.

Findings – Results highlight that (1) protection intention is influenced by the perceived threat of discarding untreated e-waste (a threat appraisal) and self-efficacy to treat the discarded e-waste (a coping appraisal), and (2) optimism bias plays a dual-role in a direct and moderating way to reduce the perceived threat of untreated e-waste and its effect on protection intentions.

Originality/value - Results support our assertions and portray a unique theoretical account of the processes that underline people’s motivation to protect their data when discarding e-waste. As such, this study explains a relatively understudied information security risk behavior in the e-waste context, points to the role of optimism bias in such decisions and highlights potential interventions that can help to alleviate this information security risk behavior.

Keywords: information security; protection motivation theory; optimism bias; e-waste information security; threat; coping.

Paper type Research Paper
Introduction

E-waste refers to electronic equipment and its parts that have been treated by their owners as waste, without any intention of reusing it (UNU-IAS, 2014). While some e-waste (e.g., computer screens, calculators) may not include confidential data, others are discarded products that have permanent information storage capacity (e.g., a tablet, game console, computers, smartphone, disks, digital cameras), and as such often include confidential data. The possibility that such information is retrieved and exploited by unauthorized third parties presents privacy and information security risks for users. As such, discarding e-waste is not only an environmental matter (Gaidajis et al., 2010) but also a critical information security issue. The risk potential of e-waste has been growing. According to a report from the World Economic Forum, e-waste is now the fastest-growing waste stream in the world, generating 48.5 million tons of waste in 2018 (WEF, 2019). Many such devices include private data traces. Therefore, managing e-waste data before discarding is an important responsibility of device owners that can have major implications for their privacy and data security.

While it can also be important for organizations, we focus here, as a first step, on individual users and their motivation to protect confidential information on personal devices when they discard them.

The information security research has primarily highlighted malicious external attackers (e.g. Mukhopadhyay et al., 2019) and organization insiders’ violation behaviors (e.g. D’Arcy and Lowry, 2019). Less is known about information security risks in e-waste. Nevertheless, unsecure disposal of e-waste, as well as its contained data, is a common risk omission behavior. A survey revealed that 75 percent of businesses do not delete data or use an insecure way to erase confidential data, leaving organizations highly susceptible to data breaches (KrollOntrack, 2010). An Australian institution randomly purchased 52 recycled computers from the online marketplace eBay and discovered that 30 percent of their hard disks contained highly confidential information such as individual bank account credentials, client email address lists, and communication contents sourced from law firms, and medical facilities (NAID, 2014). It was also reported that many obsolete hard drives from unknown sources (individual and organizational) were sold on open-markets, and these drives contained massive amounts of private data including credit card numbers, account information, and records of online transactions (PBS, 2010). It was also reported that a discarded disk containing unencrypted and confidential documents belonging to a U.S. government contractor
was available for sale (Robert, 2009). Thus, dealing with e-waste properly is imperative for reducing privacy and information security threats for individuals and firms. Nevertheless, there is a notable lack of research focusing information security from an e-waste perspective (Alghazo et al., 2018).

Here, we rely on and extend the protection motivation theory (PMT) (Rogers, 1983) to explain the cognitive mechanisms that drive people to protect their information assets when discarding e-waste. PMT has been commonly used to predict people’s behavioral intentions to engage in information security protective actions (Boss et al., 2015; Johnston et al., 2015; Menard et al., 2017). One key contribution of this work is by extending such findings to the unique context of e-waste. PMT suggests that people’s motivation to protect themselves from risks stems from evaluating threats (threat appraisal) and their perceived ability to cope with the threat (coping appraisal). We focus on such, albeit contextualized appraisals in our model, and suggest that protection intentions are driven by how threatening not dealing with e-waste data is perceived to be and how efficacious a person is in dealing with (wiping/securing) e-waste data.

Extending this traditional PMT view and relying on theories of biased decision making and risk assessments of information systems users (Bazerman and Moore, 2008; Farivar et al., 2017; Oechssler et al., 2009; Windmann and Kruger, 1998), we also suggest that the threat appraisal process is susceptible to cognitive biases, and specifically to optimism bias. Optimism bias reflects the tendency for people to believe that they are more likely to experience positive events and less likely to experience negative events when compared with similar others (Weinstrin, 1980). It, therefore, leads people to underestimate and improperly weigh risks; this bias can, therefore, alter their motivation to cope with risks. For example, executives often optimistically believe that their companies are less vulnerable than others and have better abilities and means to control threats to information security (Rhee et al., 2012). Thus, they feel less vulnerable to information security threats and have less control over the protection of IS assets (Rhee et al., 2005). We accordingly posit that people high in optimism bias will underestimate e-waste risks and marginalize such risks in the protection motivation development process. This extension of PMT is a second key contribution of this work.

As noted above, testing and validating this model makes several important contributions. First, it explains common, yet understudied, risky IS security behaviors, by applying an established
framework, namely PMT. Second, it introduces a new important bias to the arsenal of biases in decision making the IS literature has focused on (Jeyaraj et al., 2006; Kim and Kankanhalli, 2009; Lim et al., 2000; Minas et al., 2014; Steelman and Soror, 2017). This new bias can help explaining many other suboptimal IS use behaviors (e.g., avoiding updating anti-virus or anti-phishing software, and avoiding password changes). We suggest that this is one of many potentially important biases that can affect PMT processes (see discussion in the next section). Lastly, our study extends the PMT by introducing bounded rationality in the form of optimism bias into the model. Given that IS user decisions are not fully rational (Bulgurcu et al., 2010; Kim and Kankanhalli, 2009), setting bounded rationality around rational-based models is an important extension that makes such models more realistic. From a practical standpoint, our study illuminates a relatively under-explored but prevalent information security risk and points to possible interventions to cope and alleviate such risk.

The paper proceeds as follows. The next section discusses the theoretical background, then develops a research model with hypotheses. The following sections describe the research design and methodology. Finally, results are presented, and the theoretical and practical implications are discussed.

Research Background

Protection Motivation Theory

Protection Motivation Theory (PMT) provides a viable theoretical framework in predicting coping behavior when people perceive a threatening situation (Rogers, 1983). PMT suggests that people’s motivation to protect themselves is the result of a person’s appraisal of the threat and a coping appraisal. Threat appraisals assess the extent to which an individual believes the consequences caused by a threat are serious, and the probability that a threat will negatively affect the person. Coping appraisals explain how effective the response is to deal with threats, the ability required to respond to these threats, and the feasibility of implementing coping measures. If people believe a coping measure is effective and feasible, and they have the ability or confidence to execute it, they will be more likely than otherwise to execute the coping behavior. PMT has been widely used in the adoption of information security technologies to avoid harm from malware (Chenoweth et al., 2009; Lee et al., 2007; Lee and Larsen, 2009), predicting policy compliance (Ifinedo, 2012; Pahnila et al.,...
2007; Vance et al., 2012), improving online information security behaviors (Van Bavel et al., 2019) and suppressing omission behavior (Workman et al., 2008). We, postulate that it can also serve as a basis for explaining e-waste protection behaviors.

Risk Appraisal and Cognitive Bias

Many information security behavior studies assume that the decision to act or not to act to protect one’s security based on a proper weighing of risks and benefits of the target behavior (or its omission) and developing conscious intentions based on the assessed reward-risk balance (Bulgurcu et al., 2010; Cheng et al., 2013; Herath and Rao, 2009). PMT, for instance, assumes that people cognitively weigh the information they gather from various external sources and events for developing threat and coping appraisals, which are in turn used for developing coping decisions (Youn, 2009).

However, cognitive biases often alter people’s rationality under risk conditions (Kahneman and Tversky, 1979) and drive people to take unnecessary risks (Tsou et al., 2015). It is, therefore, reasonable to expect that biases that implicate risk assessments would change the boundary of rationality in PMT assessments. Specifically, cognitive biases are defined as “a pattern of deviation in judgment that occurs in particular situations, leading to perceptual distortion, inaccurate judgment, illogical interpretation, or what is broadly called irrationality” (Kahneman and Tversky, 1972). Such biases stem from the human tendency to prefer heuristics over actual information for mental conservation purposes, and/or from integrating less relevant information (e.g., negative emotions) that leaves strong “markers” in people’s brains, into current decisions (Kahneman and Egan, 2011). They may also stem from the distortion of knowledge, which includes the sense of erroneous belief (Rhee et al., 2005).

Cognitive biases are typically a barrier to effective information security management, since they may cause individuals to discount the negative outcomes and the uncertainty associated with their decisions, thereby leading to the underestimation of risks (Shaver and Scott, 1991; Simon et al., 1999). For example, people almost invariably tend to exaggerate their controllability when engaging in information security decisions and actions (Rhee et al., 2005), and in an organization context, executives had this very optimism bias regarding malware threats (Loch et al., 1992). We summarized in Table 1 key cognitive biases in information security behavior and included examples
that demonstrate how cognitive biases can lead to suboptimal responses to IS security threats. Here, we suggest that while many such biases can alter PMT processes, we have a theoretical reason to integrate optimism bias into the PMT framework. Hence, without discounting the potential of other biases to distort PMT processes, we focus, as a first step, on optimism bias as the focal bias in PMT processes. Consequently, we do not get into discussing which biases work and which are stronger; we just suggest that there is a theoretical reason to integrate optimism bias into PMT. This is only the first step in understanding how biases might influence PMT decisions.

Table 1. Key Biasing Factors relevant to Information Security Behavior

<table>
<thead>
<tr>
<th>Biases</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affect Bias</td>
<td>People tend to make judgments and decisions quickly based on their affective impressions.</td>
<td>Tsohou et al. (2015)</td>
</tr>
<tr>
<td>Anchoring</td>
<td>The human tendency to rely too heavily on the first piece of information offered (the &quot;anchor&quot;) when making decisions.</td>
<td>Camp (2009)</td>
</tr>
<tr>
<td>Confirmation Bias</td>
<td>People seek or interpret evidence in ways that are partial to existing beliefs, expectations, or a hypothesis in hand.</td>
<td>Tsohou et al. (2015)</td>
</tr>
<tr>
<td>Loss Aversion</td>
<td>The disutility of giving up an object is greater than the utility associated with acquiring it.</td>
<td>Tsohou et al. (2015)</td>
</tr>
<tr>
<td>Framing Effect</td>
<td>People react to a particular choice in different ways depending on how it is presented.</td>
<td>Harrington et al. (2006)</td>
</tr>
<tr>
<td>Pluralistic Ignorance</td>
<td>A majority of individuals in a group or society falsely assume that most of their peers behave or think differently from them when their attitudes and/or behaviors are similar in fact.</td>
<td>Lee et al. (2008)</td>
</tr>
<tr>
<td>Illusion of Control</td>
<td>The tendency to overestimate one’s degree of influence over other external events.</td>
<td>Wang et al. (2011)</td>
</tr>
<tr>
<td>Optimism Bias</td>
<td>People show a consistent tendency to believe that they are less at risk of experiencing a negative event themselves compared to others.</td>
<td>Rhee et al. (2005)</td>
</tr>
<tr>
<td>Status Quo Bias</td>
<td>People tend to favor the existing situation and will tend to avoid the effort involved in changing their choices.</td>
<td>Kajtazi et al. (2014)</td>
</tr>
<tr>
<td>(Sunk Cost)</td>
<td>People engage in risky behavior when they perceive increased safety in a particular area (i.e., a false sense of security).</td>
<td>Zhang et al. (2009)</td>
</tr>
<tr>
<td>Overconfidence</td>
<td>Individuals’ tendency to overrate self-perceived competence in comparison to their actual competence.</td>
<td>Wagner and Mesbah (2019)</td>
</tr>
</tbody>
</table>

Optimism Bias in E-waste Security Risk Appraisal
For a rational e-waste owner, an accurate appraisal of potential risks is an important precondition for correctly (i.e., based on reasonably accurate risks and gains) coping with information security risks. However, optimism bias (or unrealistic optimism) leads to a biased assessment of vulnerability to security-related risks (Tsouh et al., 2015). People with biased optimism often show a tendency to believe they are less likely than others to experience negative events (Rhee et al., 2005; Rhee et al., 2012). They may, therefore, be likely to believe that their own e-wastes may not be a target for private information hunters, or have a distorted belief that it is not a big deal even if their personal information falls into a wrong hand. As an example, it was reported that a young girl traded-in her damaged iPhone at a cellphone retailer in a shopping mall, and all of her private information was later retrieved by a stranger thousands of miles away (CBCNews, 2018). This girl never thought this could happen and did nothing to deal with the data before selling the used phone. This may be explained by optimism bias; it behooves IS researchers to examine how such bias can misinform people’s risk assessments in the context of e-waste handling. In general, biases can act to change people’s perceptions of a situation (typically to make it perceived as less risky than it actually is) and the way risks are weighed in risk-gain balance calculation (typically people under-weigh risks) (Kahneman and Tversky, 1979). Here, we account for both of these effects of optimism bias on protection motivation in the context of e-waste handling.

**Research Model and Hypothesis Development**

In this study, we focus on optimism bias based on the following reasons. First, PMT provides a framework to evaluate threats, countermeasures, and coping intentions (Boss et al., 2015). However, considering the existence of biases in human thinking, the appraisal processes of PMT will likely be affected by them (Floyd et al., 2000). To date, we still know little about how optimism bias, as one type of cognitive bias, affects the basic elements of PMT. Therefore, our study on optimism bias extends the basic PMT framework to account for biased risky behavior; by doing so, it can inform theory in the broader realm of risk behaviors as related to IT. Second, a pilot study (n=115 home e-waste discarders) revealed that optimism bias can be prevalent (see Appendix A) and it can serve as a basis for interventions that promote safer e-waste handling. As such, e-waste provides a good context for validating optimism bias effects. Because of the optimism bias, people may fail to assess the information security threats accurately and objectively and then develop inadequate
responses. Therefore, our study introduced optimism bias into the PMT to explore how optimism bias extends the PMT, and we believe the integration of irrational-based optimism bias into a rational-based core PMT model is a necessary extension to show how irrationality affects rational thinking processes. We note that other biases can achieve similar effects on shifting users away from the rational-optimal decision, but we focus on optimism bias as the first step in a program of research on the broader role of biases in shifting PMT processes.

We built a research model that captures risk protection behavior by integrating optimism bias and PMT constructs, as shown in Figure 1. According to PMT, threat and coping appraisals determine an individual’s motivation to cope with information security risks of e-waste. Considering that the full or core version of the PMT model should be chosen to use based on their research objectives, and researches should not always build off the full PMT nomology (Aurigemma et al., 2019), we only selected certain core concepts to explain the e-waste information security behaviors in this paper. Threat appraisal is captured with a perceived threat, and coping appraisal is represented by self-efficacy to cope with the threat. Extending this view, the model proposes that optimism bias impacts protection motivation in the context of e-waste by reducing the perceived threat and underweighing the assessed threats when developing intentions to cope with it.

![Research Model](image-url)

**Figure 1. Research Model**

Threat perceptions are based on the perceived vulnerability and perceived severity of the threat (Liang and Xue, 2009; Liang et al., 2019). The perceived threat, therefore, integrates both of these dimensions and measures how people assess the magnitude and likelihood of threats to their personal information. Such threat appraisals inform the development protection motivation in the
context of IS (Putri and Hovav, 2014; Siponen et al., 2014; Srisawang et al., 2015; Workman et al., 2008). This happens because coping with threats requires effort and resources, and without seeing the need to allocate such resources, people are reluctant to mobilize efforts for the coping task. Applied to our context, when e-waste owners believe that their discarded e-waste is a vulnerable target for information security threats that may potentially result in serious damages, they will be more motivated than otherwise to take action to protect information on their discarded e-waste. Thus, it is proposed that

**H1. Perceived threat increases intentions to protect information on one’s e-waste.**

The coping appraisal can include three components: response efficacy, self-efficacy, and response cost. Nevertheless, response costs do not consistently motivate coping (Crossler et al., 2014; Ifinedo, 2012; Menard et al., 2017). Similarly, response efficacy does not significantly influence threat-response behaviors (Boss et al., 2015) and information security policy compliance (Siponen et al., 2014). Accordingly, Warkentin et al. (2016) suggested that people will consider the threat (risk perceptions) as well as their ability (self-efficacy) to perform the information security actions, but will not consider the effectiveness of the actions. We follow this approach here and focus on self-efficacy to perform the e-waste information protection action.

Self-efficacy refers to the belief that people have the ability to perform a recommended measure (Crossler et al., 2014). Having the knowledge/information and confidence to be able to take protection measures is important to cope with potential risks (Arachchilage and Love, 2014). For example, knowledge increases personal abilities to deal with mobile loss and theft risks (Tu et al., 2015). Since e-waste handling is typically the responsibility of the owner, self-efficacy is important for e-waste owners to cope with information security risks. People with a high level of self-efficacy may have a stronger form of self-conviction about their ability to mobilize the needed resources to successfully execute a task (Rhee et al., 2009). Indeed, users are more motivated to perform IT information security behaviors, such as using anti-virus and anti-spyware software, as their levels of task self-efficacy increase (Liang and Xue, 2010; Workman et al., 2008; Grimes and Marquardson, 2019). This happens because of self-efficacy influences the amount of effort, self-regulation, and the initiation and persistence of coping efforts in the face of obstacles (Bandura, ...
1986). It is, therefore, reasonable to expect that the ability of e-waste owners to select and apply an
effective solution to cope with potential information leakage risks will motivate their intention to
cope with such risks. Hence:

**H2. Self-efficacy increases intentions to protect information on one’s e-waste.**

Optimism bias in our context captures an underestimation of the likelihood of experiencing
information security risks when disposing of e-waste. We accordingly capture this concept as the
gap between a person’s subjective risk perception and actual or objective knowledge of the threat.
People typically believe that negative events are unlikely to happen to them, and consequently,
misjudge risk (Cho et al., 2010; Dinev et al., 2015; Rhee et al., 2005). For example, employees
often underestimate the probability of information security breaches (Herath and Rao, 2009), which
can lead to insecure computing behaviors (Rhee et al., 2005) or imprecise IT risk assessments
(Warkentin et al., 2013). Hence, people with high optimism bias are not effective at making accurate
risk predictions. Such overly optimistic beliefs can drive e-waste owners to relax their vigilance
regarding objective threats and under-estimate the level of risk they are facing.

**H3. Optimism bias reduces the perceived threat.**

Another way that cognitive biases influence decisions is through reduction of the weight given to
risks in the mental risk-gain that underlies behavior (Kahneman and Tversky, 1979). That is the
same level of risk as judged by two people may create different action potentials for them, depending
on how much weight these risks are given in the process of developing intentions (Farivar et al.,
2017). Optimism bias is one factor that changes (reduces) the weight people attribute to risks. For
example, Nandedkar and Midha (2012) found that people with high optimism bias have a favorable
attitude towards music piracy because they perceive the risks of piracy (e.g., financial, social,
performance, and prosecution risks) to be lower. Zhang et al. (2018) also suggested that people with
high optimism bias may believe they have greater control over the outcome, therefore, they perceive
low privacy risks. Applied here we postulate that e-waste owners high in optimism bias may under-
weigh information risks; even if the risk is judged to be high, it will not influence coping intentions
as the risk will only marginally be integrated into one’s mental calculus. Accordingly, we
hypothesize:
**H4.** Optimism bias negatively moderates (weakens) the relationship between perceived threat and intention to protect information on one’s e-waste.

**Research Methodology**

**Measurement Development**

Items to capture perceived threat were adapted from Tu et al. (2015) and Woon et al. (2005). The scale taps into risk vulnerability and severity perceptions in the context of e-waste. The self-efficacy scale was adapted from Tu et al. (2014) and Ng et al. (2009) and extended based on the research context of e-waste handling. Coping intention items were developed to capture owners’ motivation to undertake protection measures, including the use of data cleaning software, data cleaning services, and finding reasonably safe disposal channels to handle the discarded devices to avoid information leakage from e-waste. Intention scales were adapted from Tu et al. (2015) and extended with context-specific items.

Cognitive bias is a pattern of deviation in judgment that occurs in particular situations, leading to perceptual distortion, inaccurate judgment, illogical interpretation, or irrationality. Such biases stem from the human tendency to prefer heuristics over actual information for mental conservation purposes, and/or from integrating less relevant information. Since no predefined scales were found for the optimism bias construct in our e-waste context, new multiple-item scales were constructed following common scale development guidelines. As pointed by Rhee et al. (2012) (P225), “The optimistic bias was estimated by using comparative likelihood. The likelihood can be measured either directly or indirectly. Direct comparison involves an individual’s single estimate of his own likelihood of experiencing an event relative to a target’s likelihood of the same event. Indirect comparison involves two estimates. One is an individual’s likelihood and the other is a target’s likelihood of an event occurring in the future. The discrepancy between two likelihood estimates is treated as a bias estimate.” Based on their definition, we used direct comparison method to measure optimism bias in our paper. We first developed a set of items based on the construct definition, relevant studies that focused on it (Campbell et al., 2007; Rhee et al., 2005; Rhee et al., 2012), and knowledge regarding e-waste information security practices. Our measurement questions emphasize the perceived risk differences between the subject and public knowledge. For example, in the OB1 scale “no one would be interested in the information stored in a discarded smartphone of ordinary
people like me”, the participant is asked to compare their own (like me) risk perceptions with the other people’s (not like me by default) risks perceptions on information security. Although we did not use indirect comparison method with two-step comparison, our optimistic bias is still a comparative likelihood estimation. Next, we discussed these items with a panel of 10 people experienced with e-waste. The modified and selected items were then presented to 24 respondents who had experience with e-waste disposal. They affirmed the content validity of the scale and its reliability ($\alpha =0.797$). All constructs were measured reflectively with multiple items on a five-point Likert scale.

**Pilot Test**

Given the context-adapted, new, and translated measures, we pilot-tested the survey with 115 participants who had experience in the disposal of IT devices. All scales were valid and reliable; all items loaded on their receptive constructs, all loadings exceed 0.7, and cross-loadings were below 0.4. Appendix B provides details about the items, and Appendix C provides the reliability and validity results of the pilot study.

**Main Study**

To get data from a wide range of participants, we commissioned a professional and well-known online survey firm WJX (Wen Juan Xing (Survey Star), www.wjx.cn) in China. WJX, like her Western counterparts such as Amazon mTurk, provides online survey services and recruits respondents from the public. It has been shown that data coming from such online survey firms are reliable and can serve well the needs of IS research projects in top journals (Lowry et al., 2014; D’Arcy and Lowry, 2019; Hua et al., 2018; Yazdanmehr and Wang, 2016).

The responses from the pilot test showed that people had discarded a greater number of smartphones than other electronic devices such as laptops, tablets, and desktop PCs. Thus, the survey used for the main study focused on participants who had experience or planned to deal with discarded smartphones. Participation in the survey was voluntary and anonymous, but a bonus incentive was provided for participants who filled out the survey completely, and was not throughout by quality checks (attention questions), which were embedded in the survey.

The survey was distributed randomly. WJX uses several sample identifying technologies, such
as IP verification and unique PC detection (the same IP and PC can only be used to complete the survey once), and minimum time-spend check (automatically removes responses that completed in an unreasonable time) to ensure that each survey respondent is unique, real and fully engaged. Besides, we also set three attention questions to ensure engagement. Responding incorrectly would remove the participant before survey completion.

To ensure data quality, the responses were further scrutinized. We received 398 responses; of these, 30 were deleted because they were incomplete. We next examined outliers with the z-score method (Tabachnick and Fidell, 2007), because even a few outliers can distort the results (Cousineau and Chartier, 2010). We identified and removed 20 outliers. The removal followed guidelines by Hair et al. (2014). The retained sample included 348 usable responses.

Table 2 presents the demographic characteristics of respondents. Most of them were at the bachelor and junior college education level, and their ages were mostly in the range of 20-40 years. Nearly 43% of them were knowledge workers and 50% had manual labor jobs.

### Table 2. Demographic Characteristics of the Sample (N=348)

<table>
<thead>
<tr>
<th>Category</th>
<th>Number</th>
<th>%</th>
<th>Category</th>
<th>Number</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sex</td>
<td></td>
<td></td>
<td>Monthly Income</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>164</td>
<td>47.1</td>
<td>Less than 1,000</td>
<td>27</td>
<td>7.8</td>
</tr>
<tr>
<td>Female</td>
<td>184</td>
<td>52.9</td>
<td>1,000-3,000</td>
<td>55</td>
<td>15.8</td>
</tr>
<tr>
<td>Edu</td>
<td></td>
<td></td>
<td>(RMB)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High school &amp; below</td>
<td>32</td>
<td>9.2</td>
<td>3,001-6,000</td>
<td>164</td>
<td>47.1</td>
</tr>
<tr>
<td>Bachelor &amp; Junior college</td>
<td>236</td>
<td>67.8</td>
<td>6,001-10,000</td>
<td>83</td>
<td>23.9</td>
</tr>
<tr>
<td>Master &amp; Doctor</td>
<td>80</td>
<td>23.0</td>
<td>More than 10,000</td>
<td>19</td>
<td>5.5</td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td></td>
<td>Work types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20 and younger</td>
<td>7</td>
<td>2.0</td>
<td>knowledge workers</td>
<td>148</td>
<td>42.5</td>
</tr>
<tr>
<td>21-30</td>
<td>170</td>
<td>48.9</td>
<td>Physical workers</td>
<td>173</td>
<td>49.7</td>
</tr>
<tr>
<td>31-40</td>
<td>117</td>
<td>33.6</td>
<td>Others</td>
<td>27</td>
<td>7.8</td>
</tr>
<tr>
<td>41-50</td>
<td>32</td>
<td>9.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>51 and older</td>
<td>22</td>
<td>6.3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Data Analysis and Results

After data collection, we followed standard data validation procedures to check the data quality and accuracy. We first examined data quality vis-a-vis skewness, kurtosis, and variance inflation factor (VIF). Skewness scores were between −2 and +2, which demonstrate that data did not significantly deviate from the normal distribution (Meyers et al., 2006). VIF values ranged from 1.015 to 1.207. All were below 3.3 (Diamantopoulos and Siguaw, 2006), indicating that multicollinearity was not an issue in these data. Next, correlations, reliability, and validity indices
were generated. As shown in Table 3, the scales were reasonably valid and reliable with Cronbach’s $\alpha$ coefficients and composite reliability scores (CR) exceeding 0.7 and average variance extracted (AVE) values over 0.5.

### Table 3. Reliability, Validity, and Correlations

<table>
<thead>
<tr>
<th></th>
<th>Mean</th>
<th>Std Dev</th>
<th>Cronbach’s $\alpha$</th>
<th>AVE</th>
<th>CR</th>
<th>SE</th>
<th>OB</th>
<th>PT</th>
<th>INT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-efficacy</td>
<td>3.117</td>
<td>0.892</td>
<td>0.840</td>
<td>0.573</td>
<td>0.843</td>
<td>0.757</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optimism Bias</td>
<td>2.422</td>
<td>1.041</td>
<td>0.837</td>
<td>0.563</td>
<td>0.837</td>
<td>0.750</td>
<td>0.750</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perceived Threat</td>
<td>3.957</td>
<td>0.618</td>
<td>0.842</td>
<td>0.575</td>
<td>0.843</td>
<td>-0.096</td>
<td>-0.494</td>
<td>0.758</td>
<td></td>
</tr>
<tr>
<td>Intention</td>
<td>3.893</td>
<td>0.653</td>
<td>0.845</td>
<td>0.579</td>
<td>0.846</td>
<td>0.073</td>
<td>-0.299</td>
<td>0.619</td>
<td>0.761</td>
</tr>
</tbody>
</table>

*Note. Boldface items are the square root of the average variance extracted (AVE).*

Next, we examined common methods bias (CMB) risk using the common latent factor method as per Podsakoff *et al.* (2012). A common latent factor that captures the communal variance of all model indicators was added to the confirmatory factor analysis (CFA) model, which included all of the model’s factors. The CFA model was then estimated in AMOS 24 with and without this common latent factor and the differences in loadings were found to be negligible (average = 0.007) and below the 0.2 cutoffs. Thus, it was concluded that bias as a result of CMB is unlikely to be pertinent in these data.

Consequently, the two-step approach for estimating the model (Anderson and Gerbing, 1988) was followed. First, a CFA model was estimated. Acceptable levels of goodness-of-fit were observed: $\chi^2 (98) =176.80$, $\chi^2/df = 1.804$; RMSEA = 0.048, with 95 percent confidence interval of (0.037~0.059); SRMR=0.043; CFI = 0.967; TLI =0.960; GFI=0.941; AGFI=0.918. Thus, we estimated the structural model. We did it hierarchically: first, we estimated to direct effects model, and then we added the moderation effect.

The main effects model exhibited good fit: $\chi^2 (122) =207.65$, $\chi^2/df = 1.702$; RMSEA = 0.045, with 95 percent confidence interval of (0.034~0.055); SRMR=0.041; CFI = 0.964; TLI =0.955; GFI=0.938; AGFI=0.913. The results are given in Figure 2; they lend support to H1~H3. The $R^2$ for perceived threat was 0.250, and that for intention was 0.417. Control variables explained 1.6% of variation of behavior intention. There was no sex-based difference in protection intention, but age reduced such intentions ($\beta = -0.127$, $p < 0.01$).
We next added the moderator (a multiplicative term was created by cross-multiplying the items of the perceived threat with optimism bias and standardized the items) in order to test H4. The model presented good fit: $\chi^2 (137) = 220.09$, $\chi^2/df = 1.606$; RMSEA = 0.042, with 95 percent confidence interval of (0.031–0.052); SRMR=0.041; CFI = 0.966; TLI =0.957; GFI=0.938; AGFI=0.914. The results support H4; they showed negative moderation of optimism bias ($\beta = -0.099$, $p < 0.05$). They are depicted in Figure 3.

To shed further light on the moderation effect, we plotted the main effect associations at different levels of the moderator. As Figure 4 shows, the regression lines between perceived threat and intentions become steeper as optimism bias decreases. At high levels of optimism bias (+3 SD from the mean), the effect of perceived threat on protection motivation becomes non-significant.
Figure 4. Simple Slopes for the Moderating Effect of Optimism bias

Note: ***p<0.001, **p<0.01, *p<0.05; n.s. represents non-significant

Discussion

This study sought to examine the drivers of intentions to take action to protect one’s information on discarded e-waste and to extend the PMT to account for the possibly biasing effect of optimism bias. Consistent with PMT and with many studies (Crossler et al., 2014; Hanus and Wu, 2016; Malimage and Warkentin, 2011) that employed it for explaining IS security protection motivations, our findings indicated that perceived threat and self-efficacy drive people’s protection intention in the context of e-waste. These results indicated that e-waste owners simultaneously appraise the vulnerability and severity of the e-waste information privacy threats, as well as their abilities to cope with the potential harms; and that they rationally use such judgments for developing intentions to act to prevent unauthorized information retrieval from their discarded e-waste. This is consistent with studies such as Tu et al. (2015), which indicated that perceived threat and self-efficacy are critical factors that motivate coping with IT-related threats.

Extending this basic PMT view, we showed that optimism bias negatively influenced threat perceptions related to unauthorized information retrieval from the discarded e-waste. Optimism bias also negatively moderated the relationship between perceived threat and protection intention. E-waste owners high in optimism bias did not properly weigh unauthorized information retrieval from
the discarded e-waste risks in their mental calculus leading to protection decisions. Prior studies highlighted the role of threat appraisal under the PMT framework in predicting the protection motivation of individuals (Menard et al., 2014; Srisawang et al., 2015). Nevertheless, little consideration was given to the boundary conditions of such effects and the circumstances that weaken or strengthen this association. Our study adds such an explanation; it unravels one mechanism (optimism bias) that attenuates the weighing of perceived threat in PMT processes. It, therefore, extends the PMT by pointing to one critical mechanism that governs the “threat→motivation” link and points to boundary conditions for this link. Specifically, it shows that threat appraisal does not motivate coping behaviors when people are high in optimism bias.

Overall, the findings indicate that (1) PMT represents a rational process of how e-waste owners identify and handle the threats of discarding e-waste, and (2) optimism bias is an irrational inhibitor that interrupts the process by modifying the weighing of threat perceptions; it does so through a direct suppressive effect on threat appraisal and a moderation effects on the path between threat appraisal and protection intentions. This can explain why some e-waste owners are fewer cautious with regards to discarding their e-waste.

**Theoretical Contributions**

Our study makes several important theoretical contributions. First, it explains a common, yet overlooked IS security risk behavior, namely e-waste handling, by applying and extending the established framework of PMT. The e-waste information security context is different from contexts emphasized in prior IS research (Crossler et al., 2014; Hanus and Wu, 2016; Malimage and Warkentin, 2011), such as device loss and theft risk (Tu et al., 2015). This unexplored risk is relatively prevalent and severe. It may lead to private information leakage and potential threats to property, personal, and even national security. It is therefore important to study this risk; this study makes first strides toward this end. While we identify several key predictors of intentions to cope with this risk, these are just preliminary findings. In detail, based on PMT, this study confirmed its viability in e-waste information security; e-waste owners’ threat perceptions and coping self-efficacy motivated their willingness to engage in protection actions. This context serves as a fertile ground for further explorations of factors and theories that can explain intentions to cope with e-waste risks.
Second, our study extended the PMT by highlighting a new important bias, namely optimism bias, as a key boundary condition and modulator of risk considerations, at least in the e-waste context. The findings may go beyond the e-waste context and suggest that optimism bias is important to consider in other risky decision situations. They, therefore, add optimism bias to the arsenal of biases in decision making the IS literature has focused on (Jeyaraj et al., 2006; Kim and Kankanhalli, 2009; Lim et al., 2000; Minas et al., 2014; Steelman and Soror, 2017). Specifically, our results demonstrated that optimism bias plays a dual-role in IS risk assessments: first, it reduces risk perceptions; and second, it leads to under-weighing of the assessed threats when developing intentions to cope with them. Thus, people’s perceptions and behavioral intentions are weakened for individuals high in optimism bias. While we demonstrated such effects in the case of e-waste, these notions can likely be extended to other IS security contexts as already indicated by the fact that optimism bias can attenuate online piracy intentions (Nandedkar and Midha, 2012) and Facebook cyberbullying and scams (Kim and Hancock, 2015). Therefore, this study serves as one pillar on which future research on how optimism bias attenuates IS decision-makers’ rationale can build.

Lastly, our study extends the PMT by introducing bounded rationality in the form of optimism bias into the model. Prior studies suggested that people’s information security decisions are made based on rational reflection (Hu and Xu, 2018; Li et al., 2018; Liang and Xue, 2009). However, IS users are not fully rational (Bulgurcu et al., 2010; Kim and Kankanhalli, 2009), and their rational information security actions can be interrupted by various biases (Kajtazi et al., 2014; Rhee et al., 2012). Thus, our study extends prior studies by setting boundary conditions for the PMT effects; they are not as effective when one is high in optimism bias. This result calls for further research on when and why PMT considerations work, or do not work, in IS security settings.

**Practical Implications**

Our research findings point to several practical implications for individuals and organizations. First, our findings show that if the objective is to increase people’s protection motivation in the context of e-waste, then governments and organizations can do so by increasing perceived threats and self-efficacy. Perceived threats can be augmented via fear appeals in media and advertising channels (Johnston and Warkentin, 2010; Passyn and Sujan, 2006; Wall and Buche, 2017). Self-efficacy can
be augmented via providing online tutorials, training (Bandura, 1997; Gist and Mitchell, 1992) and/or making the task simple (Yi and Hwang, 2003), for instance, by providing simple tools (apps) that can wipe devices in one click. Second, our findings show that the success of such interventions can depend, in part, on a person’s optimism bias. Hence, organizations may try to at least measure such biases during recruitment and training events, and identify individuals who may be more (or less) at risk for under-weighing e-waste handling and possibly other IS security risks.

Lastly, the findings show that e-waste handling is not uniform and lacks common practices. Thus, companies need to develop effective data erasing functions and services, so people can wipe data easily and effectively before discarding storage devices. This need is augmented in the widening use of BYOD (Bring your own devices) (Tu and Yuan, 2015). As such, extending our findings to organizations, organizations should specify e-waste handling policies for discarding company or privately owned devices that have been used for business purposes.

Limitations and Future Research Directions

First, we focused on one context (e-waste), of one type of device (mobile) and a specific group of individuals (Chinese, in non-work settings). Generalizability should be extended by replicating our findings in different use contexts. Second, we measured protection motivation (intention) but not actual behavior. While many intentions translate into actual behaviors, some do not. Hence, future research can examine when and why some protection motivations do or do not translate into actual protection behaviors. Third, this study focused on one type of cognitive biases. There can be many other biases that set boundaries around rational PMT considerations, and we call for future research to examine them. This way, our study can pave the way for the examination of other biases in PMT decisions in the context of IT.

Conclusion

This study integrates optimism bias into the PMT framework to examine a common but understudied risky IS security behavior, namely discarding e-waste. Results indicated that perceived threat and self-efficacy drive intentions to protect information on e-waste. They also revealed a dual-effect of optimism bias: it reduces perceived threat and weakens the relationship between perceived threat and protection motivation. The results of this study should be of interest to e-waste owners
and information security professionals in companies struggling with e-waste disposal issues, and to information systems scholars interested in IS security behaviors and cognitive biases. We call for more research on these topics, and extending our view of the model of the decision-making process of how people deal with e-waste information security, as described in this paper.
Appendix A. An Investigation of E-waste Discarders’ Optimism Bias

The pilot study’s objective was to understand whether optimism bias exists among e-waste discarders (home users) when handling their devices. We recruited 115 participants who were current users with experience in the disposal of discarded IT devices. This was a separate sample from the one used in the main study. Findings revealed that people have discarded a greater number of smartphones than any other electronic devices such as laptops, tablets, and desktop PCs. We next investigated the data wiping actions the responses took: 14.8% did not take any action, and 85.2 reported they took data wiping actions before e-waste disposal, such as removing external storage and simple data cleanup such as deleting files, restoring factory settings, and using cleanup software. Out of the respondents who employed wiping methods, 46.9% showed, through their reported beliefs, optimism bias toward their wiping methods and believed their effectiveness. The other 53.1% were pessimistic or neutral. The results showed the existence of optimism bias among e-waste discarders. Please note that people do not directly identify optimism bias on their own behavior. Instead, when they report optimistic beliefs regarding the effectiveness of their wiping methods which in fact are not effective, we can judge that they have optimism bias. Please note that people do not directly identify optimism bias on their own behavior. Instead, when they report optimistic beliefs regarding the effectiveness of their wiping methods which in fact are not effective, we can judge that they have optimism bias.

Appendix B. Measurement Scales

Perceived Threat (PT) Adapted from (Tu et al., 2015; Woon et al., 2005)
PT1. There is a great possibility that my discarded smartphone would become a target of data-stealing
PT2. Information security in a discarded smartphone is a serious problem for me
PT3. Information stored in my discarded smartphone could be exposed and, thus, my privacy would be invaded
PT4. People who get my discarded smartphone may access and disclose my private information, which would be a serious problem for me

Self-efficacy (SE) Adapted from (Ng et al., 2009; Tu et al., 2014)
SE1. I have the capability to take measures to clean information from my discarded smartphone
SE2. I have the capability to erase information from my discarded smartphone to avoid it being accessed or stolen
SE3. I have the capability to use data wiping software and other methods to prevent others from getting my privacy information from my discarded smartphone
SE4. I have the capability to take information erasing measures to prevent data recovery to my private information through the discarded smartphone

Intention (INT) Adapted from (Tu et al., 2015)
INT1. I intend to take measures to erase information from my discarded smartphone
INT2. I am willing to take measures to clean all the information in my discarded smartphone
INT3. I will dispose of my waste smartphone properly to prevent information from being acquired by others*
INT4. I plan to use a safe and reliable channel to deal with my discarded smartphone to avoid the information being obtained by others*
Optimism Bias (OB) Self-developed

OB1. No one would be interested in the information stored in a discarded smartphone of ordinary people like me*
OB2. I would not be so unlucky to suffer the event that someone getting information from my discarded smartphone*
OB3. I believe people who get my discarded smartphone will never try to access or restore my information*
OB4. It is no big deal for me if someone to get information from my discarded smartphone*

Note: *self-developed items.

Appendix C. Pilot Test Results

<table>
<thead>
<tr>
<th></th>
<th>Mean</th>
<th>Std Dev</th>
<th>Cronbach’s α</th>
<th>AVE</th>
<th>CR</th>
<th>SE</th>
<th>OB</th>
<th>PT</th>
<th>INT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-efficacy (SE)</td>
<td>2.967</td>
<td>0.819</td>
<td>0.912</td>
<td>0.792</td>
<td>0.938</td>
<td>0.890</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optimism Bias (OB)</td>
<td>2.343</td>
<td>0.921</td>
<td>0.817</td>
<td>0.609</td>
<td>0.861</td>
<td>0.203</td>
<td>0.780</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perceived Threat (PT)</td>
<td>3.952</td>
<td>0.750</td>
<td>0.908</td>
<td>0.784</td>
<td>0.954</td>
<td>0.098</td>
<td>-0.155</td>
<td>0.885</td>
<td></td>
</tr>
<tr>
<td>Intention (INT)</td>
<td>3.762</td>
<td>0.780</td>
<td>0.936</td>
<td>0.839</td>
<td>0.935</td>
<td>0.375</td>
<td>0.108</td>
<td>0.596</td>
<td>0.916</td>
</tr>
</tbody>
</table>

Note. Boldface items are the square root of the average variance extracted (AVE).
References


Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap", *Journal of


Information Systems, Psychology, and Behavioral Economics: Thinking Outside the “Apco” Box", *Information

Farivar, S., Turel, O., and Yuan, Y. (2017), "A Trust-Risk Perspective on Social Commerce Use: An Examination


system design to increase security intentions", *Decision Support Systems*, Vol. 119, pp. 23-34.


equation modeling (PLS-SEM)*, Sage publications.


and Home Computer User Security Behavior Intentions", In *Proceedings of the 27th International Conference
on Information Systems*, Milwaukee, Wisconsin, USA.


Security Policy Non-Compliance Behavior", In *Proceedings of the 51st Hawaii International Conference on
System Sciences* Hawaii, USA, pp. 3688-3697.

Hua, J., Chen, Y., and Luo, X. (2018), "Are we ready for cyberterrorist attacks?—Examining the role of individual

Ifinedo, P. (2012), "Understanding Information Systems Security Policy Compliance: An Integration of the Theory


Rogers, R. W. (1983), "Cognitive and Psychological Processes in Fear Appeals and Attitude Change: A Revised


Warkentin, M., Z. Xu, and L.A. Mutchler. (2013), "I’m safer than you: The role of optimism bias in personal IT risk


