JYU DISSERTATIONS 408

Hojat Mohammadnazar

Disentangling a Complicated Relationship

Information Technology and Consideration of Harm in Information Security

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY

JYU DISSERTATIONS 408

Hojat Mohammadnazar

Disentangling a Complicated Relationship

Information Technology and Consideration of Harm in Information Security

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella julkisesti tarkastettavaksi heinäkuun 3. päivänä 2021 kello 14.

Academic dissertation to be publicly discussed, by permission of the Faculty of Information Technology of the University of Jyväskylä, on July 3, 2021 at 14 o'clock.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2021

Editors
Marja-Leena Rantalainen
Faculty of Information Technology, University of Jyväskylä
Ville Korkiakangas
Open Science Centre, University of Jyväskylä

ISBN 978-951-39-8761-9 (PDF)
URN:ISBN:978-951-39-8761-9
ISSN 2489-9003

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-8761-9

ABSTRACT

Mohammadnazar, Hojat
Disentangling a complicated relationship: information technology and consideration of harm in information security
Jyväskylä: University of Jyväskylä, 2021, 108 p.
(JYU Dissertations
ISSN 2489-9003; 408)
ISBN 978-951-39-8761-9 (PDF)

Information Systems Security (ISS) risks have the capacity to harm others; thus, behaviors carrying such risks may raise moral concerns. Existing research shows that moral considerations of users could play an inhibitory role, discouraging users from engaging in activities that undermine ISS. However, information technology (IT) may create difficulties for users to understand and perceive the moral implications of their ISS decisions. If such difficulties distract or confuse users regarding the potential harm and ways to prevent such harm, moral considerations may not play the inhibitory role that previous ISS research has reported. Therefore, examining the role of IT characteristics in users' moral considerations is of necessity.

With this in mind, this dissertation aims to conceptualize and examine the potential means via which IT characteristics could introduce challenges to moral considerations of users. It will achieve this through a literature review and conceptualization of the role of IT characteristics in moral considerations of ISS, followed by an empirical study. The empirical examination concerns the process whereby individuals become aware of the potential harmful consequences of their actions for the welfare of others and realize that a decision-making situation is morally relevant. This process is called moral sensitivity and involves recognition of the parties involved, potential consequences for those involved and the possible courses of action in a given situation. By examining moral sensitivity, several IT characteristics are unearthed, perceptions of which could be linked with recognition of harm and users' emotional engagement in ISS decisions. In doing so, this dissertation contributes to the disentanglement of links between users' understanding of harm, their perceptions of IT characteristics, and their affective experiences in ISS decisions.

Keywords: information security, moral sensitivity, IT characteristics

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Mohammadnazar, Hojat
Monimutkaisen suhteen purkaminen: IT ja tietojärjestelmäturvallisuuden moraaliset näkökohdat
Jyväskylä: University of Jyväskylä, 2021, 108 p.
(JYU Dissertations
ISSN 2489-9003; 408)
ISBN 978-951-39-8761-9 (PDF)

Tietojärjestelmäturvallisuuteen liittyvät riskit voivat vahingoittaa muita; näin ollen tällaisia riskejä kantava käyttäytyminen voi herättää moraalisia huolenaiheita. Olemassa olevat tutkimukset osoittavat, että käyttäjien moraaliset näkökohdat voivat olla estävässä roolissa, mikä estää käyttäjiä osallistumasta tietojärjestelmäturvallisuutta heikentävään toimintaan. Tietotekniikka voi kuitenkin aiheuttaa käyttäjille vaikeuksia ymmärtää ja havaita tietojärjestelmäturvallisuuspäätöstensä moraalisia vaikutuksia. Jos tällaiset vaikeudet häiritsevät tai hämmentävät käyttäjiä mahdollisista haitoista ja tavoista estää tällainen vahinko, moraaliset näkökohdat eivät välttämättä ole siinä estävässä roolissa, jonka aiempi tietojärjestelmäturvallisuustutkimus on raportoinut. Siksi on välttämätöntä tarkastella IT-ominaisuuksien roolia käyttäjien moraalisissa näkökohdissa.

Tätä varten väitöskirjan tavoitteena on käsitteellistää ja tutkia mahdollisia tapoja, joilla IT-ominaisuudet saattavat tuoda haasteita käyttäjien moraalisille näkökohdille. Se saavuttaa tämän tekemällä kirjallisuuskatsauksen ja käsitteellistämällä IT-ominaisuuksien roolin tietojärjestelmäturvallisuuden moraalisissa näkökohdissa. Tätä seuraa empiirinen tutkimus. Empiirinen tarkastelu koskee prosessia, jossa yksilöt tiedostavat tekojensa mahdolliset haitalliset seuraukset muiden hyvinvoinnille ja ymmärtävät, että päätöksentekotilanne on moraalisesti merkityksellinen. Tätä prosessia kutsutaan moraaliseksi herkkyydeksi, ja siihen kuuluu asianosaisten tunnistaminen, mahdolliset seuraukset asianosaisille ja mahdolliset toimintatavat tilanteessa. Moraalista herkkyyttä tutkimalla kaivetaan esiin useita IT-ominaisuuksia, joiden käsitykset voivat liittyä haittojen tunnistamiseen ja käyttäjien emotionaaliseen sitoutumiseen tietojärjestelmäturvallisuuspäätöksiin. Näin tehdessään tämä väitöskirja edistää linkkien selvittämistä käyttäjien haittojen ymmärtämisen, heidän käsitystensä IT-ominaisuuksista ja heidän affektiivisten kokemustensa välillä tietojärjestelmäturvallisuuspäätöksissä.

Avainsanat: tietojärjestelmäturvallisuus, moraali, IT-ominaisuus

Author

Hojat Mohammadnazar
Faculty of Information Technology
University of Jyväskylä
Finland
Email: hmnazar@protonmail.com
ORCID: 0000-0002-2192-2210

Supervisors

Professor Mikko Siponen
Faculty of Information Technology
University of Jyväskylä
Finland

Dr. Liisa Myyry
Faculty of Educational Sciences
Centre for university teaching and learning
University of Helsinki
Finland

Reviewers

Professor John D'arcy
Department of Accounting & MIS
Lerner College of Business and Economics
University of Delaware
USA

Professor Karin Hedström
Center for Empirical Research on Information Systems
Örebro University
Sweden

Opponent

Professor Jongwoo (Jonathan) Kim
College of Management
University of Massachusetts Boston
USA

ACKNOWLEDGEMENTS

The present doctoral dissertation is the outcome of a process replete with many detours, ebbs and flows. Many a great mind has made the passage through this process possible to whom I am most grateful.

I wish to extend my gratitude to my advisors Prof. Mikko Siponen and Dr. Liisa Myyry. Mikko's expertise has been a constant source of inspiration in subjects ranging from moral philosophy, philosophy of science and information security management all of which may be spotted through-out the present dissertation. His no-nonsense way of work has instilled in me some of the most valued qualities for a researcher: critical thinking, clarity of thought and brevity of communication. Meanwhile, Liisa's vast knowledge of moral psychology has provided me with the privilege of insights that would otherwise have been outside my limited field of view. Additionally, I wish to thank Professor Tuure Tuunanen for his encouraging remarks during my doctoral education and for his course in information system theories that perhaps sowed the seedlings of a research career in my mind and triggered the whole process to begin with.

For reviewing my dissertation, I would like to thank Prof. John D'arcy and Prof. Karin Hedström. Their comments have not only been helpful for polishing the present document but also for future research endeavors. Furthermore, I wish to extend my appreciation to Prof. Kim for accepting to be my opponent.

I am grateful to my co-authors, Dr. Hadi Ghanbari, Dr. Wael Soliman and Dr. Mirja Pulkkinen for their commitment to collaboration, exchange of knowledge, and valuable brainstorming sessions. I am indebted to my voice actors Joh, Will, Heta and Imre for their remarkable work and for their availability at different stages for recording the scenarios. Special thanks to Will and Valtteri for their linguistic support and to Manja, Truth, and Fufan for their fellowship and comradery.

I wish to thank the nice people from the Extreme Executioners, the Sohwi's Drink-n-Nag vent-out group, and that cat I once saw having a stroll on a cold freezing night in Kuokkala. You people and cat (of course) have kept me sane, driven me nuts and provided much needed support. In this regard, special thanks goes to Iballa for the countless moments of joy, "interesting" cakes and "controversial" discussions.

Last but not least, my warmest appreciation to my family for their kindness, love and support.

Jyväskylä 12.06.2021
Hojat Mohammadnazar

FIGURE

FIGURE 1 Model of the role of IT in moral considerations in ISS 30
FIGURE 2 Density plot for moral sensitivity scores (all groups) 49
FIGURE 3 Density plot for no engagement group 50
FIGURE 4 Density plot for low engagement group 50
FIGURE 5 Density plot for high engagement group 50
FIGURE 6 Time analysis of low engagement group 63
FIGURE 7 Time analysis of high engagement group 64
FIGURE 8 Time analysis of IT characteristics in low engagement group 65
FIGURE 9 Time analysis of IT characteristics in high engagement group ... 65

TABLE

TABLE 1 Literature review search 17
TABLE 2 Moral consideration in ISS literature 18
TABLE 3 Summary of developed scenarios 37
TABLE 4 A scoring template example 41
TABLE 5 Scoring formulas 41
TABLE 6 Data collected per group of respondents per scenario 44
TABLE 7 Statistics for moral sensitivity scores 49
TABLE 8 Instances of expressions of IT characteristics 51
TABLE 9 Correlations for IT characteristics 56
TABLE 10 Correlations for affective responses 61

CONTENTS

ABSTRACT
TIIVISTELMÄ (ABSTRACT IN FINNISH)
ACKNOWLEDGEMENTS
FIGURES AND TABLES
CONTENTS

1 INTRODUCTION 11
1.1 Research objectives 13
1.2 Scope and structure 15

2 LITERATURE REVIEW 17
2.1 Moral considerations in ISS research 18
2.1.1 Components of moral behavior 20
2.1.2 Moral development 22
2.1.3 Moral obligation 23
2.1.4 Ethical orientations 23
2.1.5 Normative beliefs 24
2.1.6 Moral intensity 24
2.2 Literature review findings 25

3 CONCEPTUALIZING IT CHARACTERISTICS IN MORAL CONSIDERATIONS 29
3.1 Qualities of the IT artifact 30
3.2 Qualities of IT interaction 31
3.3 IT-induced experiences 33

4 EMPIRICAL STUDY OF MORAL SENSITIVITY 35
4.1 Method 36
4.1.1 Development of scenarios 37
4.1.2 Development of audio recordings 39
4.1.3 Development of the scoring system 39
4.1.4 Data collection 41
4.1.5 Analysis 44
4.2 Results 47
4.2.1 Moral sensitivity in ISS 48
4.2.2 Role of IT characteristics 51
4.2.3 Role of affect 57
4.2.4 Elapsed time 61

5 DISCUSSION 67
5.1 Research contributions 71
5.2 Practical contributions 73

5.3 Future research and limitations 74
5.3.1 Moral considerations and dual processing 74
5.3.2 IT characteristics and emotions 75
5.3.3 Frustration and experience of alienation 76
5.3.4 Desirable versus undesirable behavior 76

6 CONCLUSIONS 78

REFERENCES 79

APPENDICES 92
Appendix 1 Summary of reviewed studies and key findings 92
Appendix 2 Examples of expressions of IT characteristics 104
Appendix 3 Examples of expressions of affective responses 106

1 INTRODUCTION

Information Systems Security (ISS) refers to the protection of information assets in terms of confidentiality, integrity, and availability. ISS decisions may carry moral concerns (Siponen 2001). Imagine an online gaming company that produces services for children. In order to operate their services, this company collects names, genders, birthdays as well as parents names, and home addresses of its users, that is, children. An employee at this service company who has access to the aforementioned information does not follow secure authentication procedures and chooses a weak password for accessing the system. In the event of an ISS attack, this employee becomes a weak link in the secure system of the company and his weak password is cracked with relative ease, consequently granting an attacker access to the children's information. At this point, the attacker has this information: "This is Bobby, who is 8 years old, I know his parents and I know where he lives". The gravity of the consequences of such knowledge at the wrong hands requires little explanation. This scenario indicates how an employee's ISS decision, which may at first glance appear a personal decision, could have consequences for the welfare of others. The decision of the employee to violate the ISS procedures of their employer could inflict potentially irreversible harm on others.

Given the growing emergence of online services and smart devices such as toys and home appliances, moral decision-making in ISS has become crucial for the wellbeing of communities, and societies. Therefore, addressing these moral concerns —such as those in the afore-discussed example— is of necessity. In today's networked and highly connected environment, one's insecure actions could lead to harmful consequences for many. Consequences of insecure actions include harm to individual privacy and intellectual property, but can escalate to unimaginable highs. Consequently, users have a moral responsibility to maintain secure behavior. In a connected environment, securing information assets is a shared responsibility from which no one is spared (Cook 1986). In other words, the responsibility to secure information assets is not exclusive to the ISS experts but is shared by everyone (Ladd 1982).

Having recognized the moral concerns associated with ISS, prior research has examined moral considerations of users such as their beliefs, judgments, attitudes, and normative evaluations in ISS decisions (D'Arcy et al. 2009; Lankton et al. 2019; Li et al. 2014; Park et al. 2017; Vance et al. 2012; Xu and Hu 2018), and developed models of moral decision-making (Banerjee et al. 1998; Cronan et al. 2005; Leonard et al. 2004; Loch and Conger 1996). Findings of these studies suggest that when users view an ISS decision such as ISS policy violation (Hu et al. 2011; Vance and Siponen 2012; Xu and Hu 2018) or Information Technology (IT) misuse (D'Arcy et al. 2009; D'Arcy and Devaraj 2012; Lowry et al. 2014; Park et al. 2017) as morally questionable, they are more likely to avoid ISS misbehavior and follow recommended ISS procedures (Cram et al. 2019; Moody et al. 2018; Sommestad et al. 2014). However, moral concerns in ISS arise in the context of IT use. Prior research has often overlooked IT as a facilitator (Chatterjee et al. 2015), or instrument (Johnson 2009) that could challenge users' moral considerations, making it difficult for them to extend their sense of morality to ISS (Johnson 2009; Siponen and Vartiainen 2002).

IT, due to its characteristics, creates new possible ways to perform an action (Johnson 2009; Wall 2010) and in doing so it could change the way users interpret, and understand moral issues (Loch and Conger 1996). Imagine the distance created between the employee and the children in the afore-discussed example as a result of IT use. This distance is often minimal in real-world situations making it more straightforward to grasp the potential harmful consequences of one's decisions. In IT use context, however, the distance between the employee and the children may be considerable (Friedman 1997; Peslak 2008; Siponen and Vartiainen 2002). This IT characteristic, therefore, could make it difficult for the employee to perceive the extent to which they could inflict harm on the children, and to recognize the potential victims of their ISS decisions (Siponen and Vance 2010), leading to a lack of attention to the potential moral issues in secure authentication procedures. Although the potential impact of IT on moral considerations of users has long been acknowledged (Gattiker and Kelley 1999; Johnson 2009; Pemberton 1998), efforts to investigate IT characteristics in moral considerations of users have been rare and far between in ISS research (Chatterjee et al. 2015; Dorantes et al. 2006; Loch and Conger 1996).

The aim of this dissertation is to conceptualize and examine the potential means via which IT characteristics could introduce challenges to moral considerations of users. To do so, this dissertation conceptualizes and examines the potential impact of IT characteristics on moral considerations of users. Specifically, the dissertation focuses on moral sensitivity as a moral consideration whereby one realizes the moral relevance of a decision-making situation and the possibility that their actions could have harmful consequences for others (Rest 1986). In doing so, the dissertation examines the impact of perceptions of IT characteristics on users' understanding of the moral relevance of ISS decisions.

This dissertation contributes to our understanding of moral sensitivity as one of the processes that enable and drive users' moral decisions (Rest 1986) by outlining that such a process might be subject to dual processing using type1

processing which is characterized as quick, intuitive and autonomous and type2 processing which is reflective, slow and resource demanding (Evans and Stanovich 2013; Kahneman 2011). Such an understanding of the underlying processes of moral decision-making is crucial if we are to provide sensible solutions to address moral concerns in ISS (Gattiker and Kelley 1999; Thong and Yap 1998). Prior research has often assumed that users are morally sensitive in ISS decisions, however, this dissertation shows that if users make quick and instantaneous decisions, they might not be aware of the moral relevance of an ISS decision. If users are not morally sensitive, they may not engage their moral schemata to begin with (Rest 1986) and the inhibitory role of moral considerations in their ISS decisions may become irrelevant. Therefore, this dissertation contributes to the development of moral interventions (Banerjee et al. 1998; Cook 1986; Li et al. 2014; Loch and Conger 1996; Moores and Chang 2006; Siponen 2001; Stahl 2012; Vance et al. 2019) that enable users to understand the moral implications of ISS decisions and extend their sense of morality to ISS issues.

In examination of moral sensitivity, this dissertation uncovers the intertwined links between users' understanding of harm, their perceptions of IT characteristics and their affective experiences, showing that not only perceptions of IT characteristics may impact users' understanding of harm but that perceptions of psychological distance in IT interaction may impact their emotional engagement in ISS decisions. By outlining several IT characteristics relevant to moral considerations in ISS, this dissertation contributes to the uncovering of the role of the IT artifact in ISS research (Benbasat and Zmud 2003; Lowry et al. 2017; Orlikowski and Iacono 2001). IT artifact as a central feature of research on information systems has often been considered absent in ISS research (Lowry et al. 2017). By focusing on IT characteristics, this dissertation conceptualizes the potential role of IT artifact qualities and IT interaction qualities as well as IT-induced experiences such as anxiety in moral considerations of users in ISS decisions. In doing so, the dissertation contributes to paving the path for development of context-specific theory (Hong et al. 2014), specifically, theories of moral considerations in the ISS context.

1.1 Research objectives

Moral beliefs, judgments, obligations, and ideologies have been shown to have an inhibitory role, discouraging users from engaging in policy violation (Hu et al. 2011; Vance and Siponen 2012; Xu and Hu 2018) and IT misuse (Banerjee et al. 1998; D'Arcy et al. 2009; D'Arcy and Devaraj 2012; Lowry et al. 2014; Park et al. 2017). Furthermore, moral considerations have been shown to encourage policy compliance (D'Arcy and Lowry 2019; Li et al. 2014; Yazdanmehr and Wang 2016). However, moral decision-making presupposes the realization that one is facing a moral problem. Without such realization, one might not examine a situation in moral terms at all. In other words, in the absence of the realization that one is

facing a moral problem, moral beliefs, judgments, obligations, and ideologies may become irrelevant. This realization occurs in a process referred to as moral sensitivity (Rest 1986).

Moral sensitivity regards one's ability to perceive a situation as morally relevant (Rest 1986). It entails consideration of parties involved in a given situation, courses of action possible and the consequences of actions on the involved parties (Rest 1986). As such, moral sensitivity addresses one's understanding of harmful consequences for potential victims in a given situation and the means to avoid harm. Previous research has shown that moral sensitivity is context-specific (McNeel 1994). Furthermore, affective responses such as experience of emotions like empathy and guilt have been shown to be conducive to moral sensitivity (Decety et al. 2011, 2012; Morton et al. 2006).

IT, however, could challenge the realization that an ISS decision is morally relevant as it creates challenges for users to extend their sense of morality to such decisions (Siponen and Vartiainen 2002) and to identify potential victims (Siponen and Vance 2010). Therefore, IT could challenge the moral sensitivity process in an ISS decision-making situation by making it difficult for users to understand the harmful consequences of ISS decisions for potential victims. If users are not able to understand the harmful consequences of ISS violations, whether moral beliefs, judgments, obligations, and ideologies play an inhibitory role in their decision-making becomes irrelevant.

Given that lack of moral sensitivity in ISS decisions could raise questions regarding the inhibitory role of morality in such decisions, and bearing in mind its context-specificity, this dissertation examines the moral sensitivity process in ISS decision-making situations. Despite previous attempts to examine moral sensitivity in ISS decisions (Dorantes et al. 2006; Goles et al. 2006) a context-specific understanding of this process is lacking. In doing so, the role of IT characteristics is highlighted as IT could create difficulties for moral considerations of users. Furthermore, bearing in mind the difficulty of users to recognize potential victims in ISS decisions (Siponen and Vance 2010) —which may affect their emotional engagement in ISS decisions— and considering the conducive role of emotional engagement such as experience of feelings of empathy to moral sensitivity (Decety et al. 2011, 2012; Morton et al. 2006), this study examines experience of emotions in ISS decision-making situations in order to provide further insights on the inner mechanics of the moral sensitivity process in ISS.

Therefore, aligned with the aim of the dissertation, which is to conceptualize and examine the potential means via which IT characteristics could introduce challenges to moral considerations of users, the following research questions are examined with respect to moral sensitivity as a moral consideration:

1) How morally sensitive are users in ISS decision-making situations?
2) What is the role of IT characteristics in users' moral sensitivity and understanding of harm in ISS decision-making situations?
3) What is the role of emotions in users' moral sensitivity and understanding of harm in ISS decision-making situations?

4) How does the moral sensitivity process unfold in ISS decisions?

These questions will be addressed by conceptualizing the role of IT in moral considerations of ISS decisions, then conducting an empirical study on moral sensitivity in which respondents would listen to audio recordings of scenarios involving a morally relevant ISS dilemma and answer a few questions. Each scenario is developed based on the ISS policies of the two large Nordic universities where the study is conducted and the roles of the potential respondents in the research settings. During data collection no references to morality or ethics is made, nor are any questions regarding IT characteristics posed to the respondents. This approach could allow elicitation of respondents' personal interpretations of the ISS dilemma in the scenarios.

1.2 Scope and structure

The aim of this dissertation is to conceptualize and examine the role of IT characteristics in creating difficulties for users to apply their sense of morality to ISS decision-making situations. In order to do so, the dissertation focuses on moral sensitivity. Study of moral sensitivity in ISS decisions is appropriate as users may have difficulties in understanding the potential harm involved in ISS decisions which may lead them to simply bypass moral decision-making. Moral sensitivity logically as well as chronologically could precede moral judgment (Rest 1986), that is, the judgment made by a user that an action is right or wrong. Without moral sensitivity one may not make a moral judgment and may not engage in moral decision-making at all.

In examination of moral sensitivity, this dissertation focuses on users whose decisions could have harmful consequences for others such as the organization they are affiliated with, its staff members, and its clients. Such harmful consequences could involve exposure of intellectual property, information assets and violation of privacy. Intellectual property and privacy are topics with longstanding history and prominence in examination of ethics and morality (Culnan and Williams 2009; Hansen and Walden 2013; Higgins and Wilson 2006; Hinduja and Ingram 2008; Loch et al. 1998; Stahl 2004). However, in this dissertation, intellectual property and privacy are addressed insofar as they concern the consequences of a user's ISS decisions. In other words, the dissertation does not address the ethical considerations of an organization towards its clientele regarding privacy (Culnan and Williams 2009), nor does it address moral considerations of a consumer regarding intellectual property violations of consumer goods such as unauthorized downloading of software and digital material (Hansen and Walden 2013).

The remainder of this dissertation is structured as follows. Section 2 presents a systematic review of the literature on moral considerations in ISS research. In this section, moral considerations examined in the extant literature are presented, and common patterns among these studies are discussed. Section 3 builds on the results of the literature review to present a conceptualization of

the role of IT in moral considerations of users in ISS decisions. In this section, (1) Quality of IT artifact, (2) Quality of IT interaction, and (3) IT-induced experiences are discussed and their potential impact on moral considerations of users are outlined. Section 4 introduces the empirical study of moral sensitivity including methods, and findings. Next comes discussions (section 5) of findings regarding examination of moral sensitivity in ISS. Lastly, in section 6, concluding remarks are presented.

2 LITERATURE REVIEW

In this section, moral considerations examined in the extant ISS literature are presented, and common patterns in the research findings are discussed. Doing so lays the groundwork for conceptualization of the role of IT characteristics in moral considerations of ISS decisions and highlights the significance of examining moral sensitivity in such decisions. Following a structured literature review approach (Webster and Watson 2002), we started extraction of material using keyword searches in the Science Direct, and AIS Library databases in October 2019 after an initial search on ProQuest library. Table 1 indicates the keywords used and number of returned results. The keyword search was followed by a backward and later a forward search. Papers were included in the review set if they were complete empirical papers that examined a moral notion with respect to an ISS activity, and contained clear methodology. Studies on consumer ethics such as piracy were excluded when they did not focus on piracy as an ISS-related moral issue. Intervention studies that focused only on the effectiveness of an ISS solution were also excluded. However, studies on ethical/unethical IT use were included insofar as the scenarios examined represented IT misuse cases. After evaluating each study against our inclusion and exclusion criteria, 63 empirical studies were included in the review set. Summary of the literature review along with key findings is available in Appendix 1.

TABLE 1 Literature review search

Search string	**Database**	**Results**
("information security" OR cyber?security) AND (moral* OR ethic*)	Science Direct, AIS library	748, 936
(misuse or abuse) AND (moral* or ethic*)	Science Direct, AIS library	209, 116

2.1 Moral considerations in ISS research

Review of the literature led to the identification of several moral considerations. Moral considerations were coded and categorized according to definitions provided in each study as well as items used for their elicitation in questionnaires and interviews. Each moral consideration in prior research was examined and measured using several constructs (Table 2). While in some cases these constructs have slightly different questionnaire items, they often examined the same underlying moral consideration.

TABLE 2 Moral consideration in ISS literature

Moral considerations {Description}	**Constructs**	**Source**
Moral Sensitivity {Interpretation of a situation as morally relevant. (Rest 1986)}	Recognition of Ethical Problem	(Dorantes et al. 2006)
	Perceived ethical problem	(Goles et al. 2006)
	Moral recognition	(Scilhavy and King 2009)
Moral Judgment {Right/wrong judgment regarding an act.}	Moral beliefs	(D'Arcy and Devaraj 2012); (Vance and Siponen 2012); (Hovav et al. 2012); (Hu et al. 2011); (Bansal et al. 2016); (Vance et al. 2019); (Xu and Hu 2018); (D'Arcy and Lowry 2019)
	Moral judgment	(Peslak 2008); (Dorantes et al. 2006); (Harrington 1997); (Kuo et al. 2010); (Haines and Leonard 2007); (D'Arcy and Hovav 2009)
	Permissiveness	(Gattiker and Kelley 1999)
	Attitude	(Winter et al. 2004); (Cronan et al. 2005); (Leonard and Cronan 2005); (Leonard et al. 2004); (Leonard and Cronan 2001); (Banerjee et al. 1998); (Walstrom 2006); (Hsu and Kuo 2003); (Zhang et al. 2006); (Kowalski and Kowalski 1990); (Kowalski 1990)
	Ethical judgment	(McMahon and Cohen 2009); (Ellis and Griffith 2001); (Sacco and Zureik 1990); (Pierce and Henry 2000); (Harrington 1996); (Pierce and Henry 1999); (Harris et al. 2010)
	Moral commitment	(D'Arcy et al. 2009); (Son and Park 2016)
	Act evaluation	(Friedman 1997)
	Unethicalness	(Khazanchi 1995)
	Moral norms	(Merhi and Ahluwalia 2019)
	Abusiveness	(Ugrin and Michael Pearson 2013)

Moral considerations {Description}	**Constructs**	**Source**
	Personal norms/ethics	(Li et al. 2010); (Li et al. 2014)
Moral Intention {One's intention to perform a moral act.}	Moral intent	(Harrington 1997); (Dorantes et al. 2006); (Haines and Leonard 2007); (Harrington 1996)
	Ethical behavioral Intention	(Hsu and Kuo 2003)
	Intention and desire in ethical behavior	(Chu et al. 2015)
	Ethical/unethical behavioral intention	(Grace 2013); (Scilhavy and King 2009); (Peterson 2002); (Leonard et al. 2004); (Leonard and Cronan 2001); (Banerjee et al. 1998); (Hsu and Kuo 2003)
	Intention toward unethical IT use	(Chatterjee et al. 2015); (Chatterjee et al. 2011)
Moral Intensity {One's understanding of the importance of a moral situation or its characteristics that determine its moral imperative (Jones 1991)}	Moral intensity	(Dorantes et al. 2006); (Grace 2013); (Goles et al. 2006); (Vance et al. 2015); (Peslak 2008)
	Perceived importance (PIE)	(Haines and Leonard 2007); (Cronan et al. 2005); (Leonard et al. 2004); (Liao et al. 2009); (Zhang et al. 2006)
Moral Obligation {One's sense of obligation in a moral situation. (Schwartz 1977)}	Personal norms Moral obligations Personal ethics	(Yazdanmehr and Wang 2016); (Haines and Leonard 2007); (Leonard et al. 2004); (Banerjee et al. 1998); (Leonard and Cronan 2001); (Lee et al. 2007); (Yoon and Kim 2013); (Al-Omari et al. 2013); (Zhang et al. 2006)
Moral Development {One's preferene for different types of moral reasoning based on level/stage of moral development (Kohlberg et al. 1983). Moral reasoning may lead to a moral judgment.}	Moral development	(Leonard and Cronan 2005); (Leonard et al. 2004); (Banerjee et al. 1998); (Leonard and Cronan 2001). (Leonard et al. 2004); (Myyry et al. 2009)
Ethical orientations {The degree to which one's believes a desirable outcome can be achieved by doing the right thing as idealism and the degree to which one believes universal moral rules determine right or wrong as relativism.(Forsyth 1980)}	Relativism and Idealism	(Chatterjee et al. 2015); (Chatterjee et al. 2011); (Dorantes et al. 2006); (Ellis and Griffith 2001); (Scilhavy and King 2009); (Winter et al. 2004); (D'Arcy et al. 2014, 2018)

Moral considerations {Description}	Constructs	Source
Normative beliefs {Deontology as the degree to which an act is morally right/wrong due to its inherent features and Teleology as the degree to which as act is right/wrong due to its outcomes (Normative theories in philosophy)}	Deontology and Teleology	(Al-Omari et al. 2013); (Grace 2013); (Lowry et al. 2014)

2.1.1 Components of moral behavior

According to Rest (1986), moral behavior is a collection of four interrelated processes, rather than a unitary process. These four processes that are known as components of moral behavior are: 1) moral sensitivity, 2) moral judgment, 3) moral motivation, and 4) moral character (Rest 1986). Within the framework of this four-component model, moral sensitivity is a component in which one becomes aware of the moral relevance of a situation, moral judgment is a component in which a user makes a wrong/right judgment, moral motivation refers to prioritization of a moral course of action over other possible courses of action, and moral character is a matter having the strength, courage and skills to implement a moral course of action (Rest 1986). Failure in any of the aforementioned components could result in non-realization of a moral act (Rest 1986).

It should be noted that the four-component model applies to activities in which one could exercise volition. Furthermore, although the order of the components is logical rather than chronological, chronological order of the components might still be important (Rest 1994). For instance, moral sensitivity could both logically as well as chronologically precede moral judgment and is thus crucial for making a moral decision. While capturing the processes of moral behavior, the four-component model is not limited to a certain philosophical doctrine, such as teleology or deontology. Furthermore, the four-component model could accommodate different standpoints, such as the affective and cognitive understanding of moral behavior (Rest 1983). Typically only two of the components of the four-component model are studied at the same time, although in some studies three of them have been investigated (Hardy 2006; Morton et al. 2006). In ISS literature three components, namely, moral sensitivity, moral judgment, and moral motivation have received scholarly attention as users' moral considerations are concerned.

Moral sensitivity refers to one's awareness of moral situations and the effect of their actions on other people (Rest 1986). It involves perceiving a situation as morally relevant, identifying the parties involved, and envisioning the possible courses of action and the consequences of the actions for those involved (Rest 1986). Previous research shows that moral sensitivity is context-specific (McNeel

1994) and that it can be primed (Sparks 2015) and enhanced by education (Baab and Bebeau 1990; Clarkeburn 2002; Myyry and Helkama 2002). In ISS literature, moral sensitivity has been studied by examining users' moral recognition, that is, users' understanding that a given scenario has moral content. In this respect, perception of moral content was found to be related to moral judgments in IT misuse scenarios (Dorantes et al. 2006; Goles et al. 2006; Scilhavy and King 2009).

The moral judgement component of the four-component model refers to the process whereby an individual makes a right/wrong judgment on an issue. Moral judgment is the most widely studied component of Rest's model and many of the afore-discussed moral considerations in this section such as moral development, moral obligations, ethical orientations, and normative beliefs fall under this component insofar as they concern the *process* of making a right/wrong judgment. In addition to examination of the process of moral judgment, prior ISS research has examined the right/wrong judgment of users when they face ISS decisions in different capacities and using constructs such as attitude, moral beliefs, ethical judgment, permissiveness, and moral norms (Table 2). The results of these studies predominantly point to the role of moral judgments in discouraging ISS policy violations (Vance and Siponen 2012; Xu and Hu 2018) and IT misuse (Banerjee et al. 1998; D'Arcy and Devaraj 2012).

Moral motivation, as the third component in the model, refers to one's prioritization of a moral course of action over other possibilities. A user might decide to carry out or refrain from certain acts in order to pursue objectives that might not necessarily be in line with their moral judgment. In doing so, the user would prioritize the possible courses of action. Rest (1986) defined moral motivation as pertaining to an individual's value priorities and, more specifically, to the importance they give to moral values in contrast to other values. Identity (Hardy 2006) and moral emotions, such as empathy and guilt (Silfver-Kuhalampi 2009), have been identified as sources of moral motivation. In ISS research, moral motivation is often examined as moral intention (Harrington 1996, 1997) as the dependent variable in research models. Findings regarding moral intention suggests that moral considerations such as moral judgments, moral obligations and moral intensity exert an influence on moral intentions of users (Banerjee et al. 1998; Chatterjee et al. 2011; Dorantes et al. 2006; Haines and Leonard 2007; Scilhavy and King 2009). Other factors that could affect moral intention in the literature have been subjective norms (Chatterjee et al. 2011, 2015) and responsibility denial (Harrington 1996, 1997).

Moral character has not been under investigation in ISS research despite several studies examining personality characteristics and traits such as Machiavellianism (Scilhavy and King 2009; Winter et al. 2004). This is because moral character is related to implementation of a course of action. In ISS research, behavior or implementation of a course of action has rarely been studied and prior research often examines users' intention rather than implementation of an act (behavior) rather than the act itself.

2.1.2 Moral development

One's level of moral development indicates their capacity and preference to utilize different reasoning schemata when they make a moral judgment (Rest et al. 2000). Research on moral development levels pioneered by Piaget and Kohlberg focuses on cognition and provides a framework of the structure of moral thought based on which individual moral reasoning is assessed. According to the theory of cognitive moral development (Colby et al. 1983) moral development levels are pre-conventional, conventional, and post-conventional, each comprising two stages of development which an individual (typically a child) progresses through in a stage-by-stage manner as their moral reasoning develops. More recent interpretations of moral development emphasize that rather than a strong stage model, one's moral development indicates a preference for a particular type of reasoning (Rest et al. 2000).

According to the theory (Rest et al. 1969), the pre-conventional level of moral development reflects obedience and egoistic reasoning, that is, the basis of moral reasoning at this level is avoiding punishment (stage 1) or receiving something in exchange (stage 2). The next level is the conventional level where moral reasoning is on the basis of helping and pleasing others by following norms and shared values (stage 3) or by showing respect for an authority (stage 4). Lastly, in the post-conventional level, reasoning is based on consideration of the welfare of the majority (stage 5) or on principles of moral behavior (stage 6). Recent findings concerning moral development levels indicate a rather transformed stage model compared to the original formulation, at least among adults and adolescents (Rest et al. 2000; Thoma and Dong 2014). According to recent findings, stages 2 and 3 cluster together to represent a level of moral reasoning that reflects self-interest and self-preservation, while stage 4 reflects norm-preservation (Thoma and Dong 2014).

Several studies have examined moral development in ISS decisions. Findings of one such study contested the idea that principled reasoning is used for making moral judgments in the ISS context (Myyry et al. 2009). This study reported that, when facing an ISS issue with moral underpinnings, obedient reasoning (lower levels of moral development) better explains the intentions and actions of users than principled and ideological reasoning (higher level of moral development). However, there is evidence suggesting that the higher-level principled reasoning is used in ISS decision-making under certain circumstances. Specifically, higher levels of moral development seem to come into play when one tends to have an internal locus of control, work in a rule-oriented organizational climate (Banerjee et al. 1998), or exhibit low ego strength (Leonard and Cronan 2001). Another study has reported the impact of higher levels of moral development in situations where a scenario is perceived as ethically important (Leonard et al. 2004).

2.1.3 Moral obligation

Moral obligation corresponds to one's personal feelings and obligations to refrain from or engage in an activity (Beck and Ajzen 1991; Schwartz 1977). According to Schwartz (1977), one's experience of feelings of moral obligation manifests their self-expectations. One's self-expectations, fueled by the desire to keep self-integrity and to avoid self-concept distress, Schwartz (1977) argued, are what drive people to act altruistically. The feelings of moral obligation are experienced when one's internalized values and norms are activated and self-expectations are evaluated against these internalized norms and values (Schwartz 1977). Moral obligations are often referred to as personal norms or personal normative beliefs. Several studies have shown a link between experience of feelings of moral obligation and intention to comply with ISS policy (Al-Omari et al. 2013; Yazdanmehr and Wang 2016), and to use IT securely (Yoon and Kim 2013). Conversely, evidence suggests moral obligation could be linked negatively to intention to misuse IT (Banerjee et al. 1998; Leonard and Cronan 2001).

2.1.4 Ethical orientations

Idealism and relativism are ethical orientations that according to Forsyth (1980), form the basis of individuals' ethical ideologies for making moral judgments. Forsyth (1980) laid out four ethical ideologies according to one's degree of relativism and idealism. In this context, idealism is understood as the extent to which a desirable outcome can be achieved by doing the right thing (Forsyth 1980). Relativism, on the other hand, is the degree to which one believes universal moral rules rather than relative moral rules determine right or wrong (Forsyth 1980). Forsyth's taxonomy of ethical ideologies outlines (1) situationism, (2) absolutism, (3) subjectivism and (4) exceptionism as four ethical ideologies that differ in their extent of idealism and relativism. In this taxonomy, situationists and absolutists manifest high idealism. However, unlike absolutists who are low on relativism, situationists are high on relativism. Meanwhile, exceptionists and subjectivists exhibit low idealism. While exceptionists exhibit low relativism, however, subjectivists are high on relativism.

In ISS research, rather than the four ethical ideologies, scholars have often examined ethical orientations of idealism and relativism. The findings suggest that while the relativistic orientation seems to encourage users to morally disengage from compliance with ISS requirements, idealistic orientation seems to have no effect in discouraging disengagement (D'Arcy et al. 2014, 2018). Furthermore, depending on one's skill level in using computers, high idealism and low relativism have been shown to play different roles in judging the acceptability of an act of privacy violation (Winter et al. 2004). Others, however, have reported no evidence regarding the effect of relativism in ISS decisions (Ellis and Griffith 2001; Scilhavy and King 2009).

Similar to Forsyth (1980) who articulated relativism and idealism as two sets of beliefs involved in making moral judgments, Chatterjee et al. (2011, 2015) proffered technological relativism and technological idealism. In this context,

technological idealism is the extent to which one believes technology should not be used to harm anyone. Technological relativism, on the other hand, is the degree to which one believes using technology should conform to a set of rules and codes. The findings with regard to this formulation of relativism and idealism do not provide evidence of their role in users' ISS decisions. For instance, Chatterjee et al. (2011) could not find evidence of either technological idealism or technological relativism exerting an influence on attitude toward IT misuse either in their American nor Finnish sample. A subsequent study by Chatterjee et al. (2015) reported that only when one exhibits very high or very low degrees of technological idealism does it affect their attitude toward IT misuse.

2.1.5 Normative beliefs

Normative beliefs refer to a set of beliefs that result from evaluations based on normative theories in philosophy. Hunt and Vitell (1986) argued that moral judgement essentially boils down to a bipartite system of evaluation: deontological evaluation and teleological evaluation. Deontological evaluation refers to right/wrong judgments that are based on inherent features of an act regardless of its potential outcomes, while teleological evaluations refer to right/wrong judgments based on the potential outcomes of an act.

Studies that examined deontological and teleological evaluations in ISS suggest that such moral considerations are important in ISS decisions. Grace (2013) reported that both deontological and teleological evaluations were important in shaping IT misuse intentions. Meanwhile, Al-Omari et al. (2013) argued that different forms of teleological and deontological evaluation such as egoism and formalism, respectively, exert an influence on intention to comply with ISS policies. Furthermore, depending on one's collectivist or individualist culture, teleological and deontological evaluation could discourage engaging in IT misuse (Lowry et al. 2014).

2.1.6 Moral intensity

Moral intensity refers to one's understanding of the importance of a moral situation or characteristics that determine its moral imperative (Jones 1991). Jones (1991) proposed moral intensity as an aggregate measure comprising six components: magnitude of consequences, social consensus, probability of effect, temporal immediacy, proximity, and concentration of effect. Jones (1991) posited that moral intensity of a situation could act as a vivid and salient stimuli that draws attention to the moral issue in a given situation, thus, emotionally or cognitively engaging an individual in that situation. Furthermore, moral intensity could underscore one's moral responsibility, that is, it could remind an individual that they have a choice to make (Jones 1991). Therefore, Jones (1991) argued that when intensity of a situation is low, a decision maker is less likely to recognize the moral problem in a situation, more likely to use lower levels of moral reasoning and less likely to intend to act on a moral course of action.

ISS studies have shown evidence of the negative effect of moral intensity on intention to violate access policy (Vance et al. 2015) and intention to misuse IT in several scenarios (Dorantes et al. 2006; Goles et al. 2006). Additionally, moral intensity has been found to exert an influence on users' recognition of moral content in IT misuse scenarios (Dorantes et al. 2006; Goles et al. 2006). The moral intensity of a situation has also been shown to exert an influence on the moral judgment of users (Dorantes et al. 2006; Grace 2013). In this respect, different components of moral intensity have been found to affect moral judgments about different IT issues (Peslak 2008).

Moral intensity is conceptually related to the perceived importance of an ethical issue known as the PIE construct (Robin et al. 1996). The difference between the PIE construct and moral intensity, according to Robin (1996), is that the PIE takes perceptions of the moral agent into account given their organizational environment. PIE has been shown to be related to one's moral judgment (Cronan et al. 2005; Haines and Leonard 2007; Liao et al. 2009; Zhang et al. 2006) and intention to behave ethically (Leonard et al. 2004) in IT misuse scenarios.

2.2 Literature review findings

Review of the literature on moral considerations of users in ISS decisions revealed several underlying patterns. These patterns concern the role of morality in ISS research, the focus of prior research on moral judgment, attention to cognition, and examination of IT characteristics in moral considerations of users.

First, besides two studies that were conducted qualitatively (Chang 2011; Friedman 1997) and the study by Bauer and Bernroider (2017) that used a mixed method, research on users' moral considerations has been conducted predominantly using cross-sectional or factorial surveys. Overall, except Lee et al. (2007) and Son and Park (2016), majority of the studies in the literature demonstrated that users' moral considerations could discourage undesirable ISS behavior (e.g., ISP violations, IS misuse) (Banerjee et al. 1998; D'Arcy et al. 2009; D'Arcy and Devaraj 2012; Lowry et al. 2014; Park et al. 2017) and encourage desirable ISS behavior (e.g., ISP compliance) (D'Arcy and Lowry 2019; Li et al. 2014; Yazdanmehr and Wang 2016). Notably, studies that did not find evidence of the influence of moral considerations on users' decisions (intention or behavior) were examining personal web usage at work (Lee et al. 2007; Son and Park 2016). Findings regarding the significance of moral considerations confirmed those previously reported by Cram et al. (2019) and Sommestad et al. (2014).

Second, few studies examined the process of moral decision-making; rather moral considerations of users have often been given an inhibitory role in research models. To explain ISS decisions, most studies integrate moral constructs into theories such as the theory of planned behavior (Lee et al. 2007; Zhang et al. 2006), the theory of reasoned action (Leonard and Cronan 2001; Loch and Conger 1996), the rational choice theory (D'Arcy and Lowry 2019; Hu et al. 2011; Li et al. 2010),

and deterrence theory (D'Arcy et al. 2009; D'Arcy and Devaraj 2012). Our review showed that in ISS studies morality is often considered an internal control mechanism (Bauer and Bernroider 2017; Hovav et al. 2012; Kowalski 1990; Kowalski and Kowalski 1990; Sacco and Zureik 1990; Yoon and Kim 2013), that is, a mechanism that allows individuals to regulate their behavior. Some scholars see morality as an internal and informal self-sanctioning mechanism (D'Arcy et al. 2014; Hovav et al. 2012; Park et al. 2017; Xu and Hu 2018; Yazdanmehr and Wang 2016). Others have considered morality as a concern that is independent from cost-benefit evaluations including sanctions (Li et al. 2010), an internal force against which economic costs and benefits are assessed (Hu et al. 2011), a concern that produces self-approval, virtue, or pride (Lankton et al. 2019), a societal concern for governance in a decentralized and borderless environment (McMahon and Cohen 2009) and a mechanism that motivates rule-following (Ugrin and Michael Pearson 2013). Overall, the understanding of morality in ISS research underlines its inhibitory role in ISS decisions. Morality is known to have long-lasting effects on decision-making due to the inseparability of moral integrity, and self-identity (Hardy and Carlo 2005; Lapsley and Narvaez 2004). Therefore, examination of the underlying processes that drive moral decisions and how moral evaluation of rules, policies, norms and sanctions takes place seems an area of great interest to ISS research.

Third, our review of the literature indicated that much of the scholarly attention has been focused on users' moral judgment or moral obligations (See Table 2). Moral judgment and moral obligation are conceptually similar and overlap in that they inquire one's right/wrong judgment regarding a morally relevant act. However, moral obligations are considered the manifestation of one's self-expectations which elicit their experience of feelings of obligation (Schwartz 1977). Notably, examination of moral obligation in the literature often involves elicitation of moral judgments with questions such as "It would be morally wrong for me to [engage in ISS behavior]" in addition to elicitation of sense of obligation with questions such as "I feel morally obligated to [engage in an ISS behavior]" (see Al-Omari et al. 2013; Yoon and Kim 2013). This focus on moral judgment indicates extended research attention to moral judgment component of moral behavior in the four-component model (Rest 1986). Moral behavior, however, is not a unitary process limited to moral judgment but according to the four-component model (Rest 1986), it is a collection of four interrelated processes. Therefore, further attention to other processes of moral behavior such as moral sensitivity in ISS research seems necessary. In order to highlight why examination of other processes involved in moral behavior such as moral sensitivity might be of interest to ISS research, consider moral sensitivity. If users are not morally sensitive about an ISS decision such as password sharing, they may not engage in moral judgement to begin with. This in turn could mean that despite the inhibitory effect of moral judgment on users' intentions to avoid password sharing, users may fail to make a moral judgment in a password sharing situation.

Fourth, a closer look at Table 2 reveals that the studied considerations in prior ISS research often examine one's *reasoning* or beliefs, judgments and intentions that could be arrived at by *reasoning*. For instance moral development, ethical orientations, normative beliefs in Table 2 seem to elicit types of reasoning carried out by users when they face moral issues. Meanwhile recognition of moral issues, intentions to act, beliefs and judgments often instruct users to engage in reasoning with questions such as "Is [an ISS decision] morally relevant", or "Is it morally wrong to engage in [an ISS behavior]". This pattern suggests that with the exception of moral intensity and some instances of moral obligation where ones' *feelings* of moral obligation are elicited (Yazdanmehr and Wang 2016), examination of moral considerations in the extant literature involves conscious reasoning. In other words, the literature focuses primarily on cognition in moral considerations with little attention to affect. Studying affect, however, is of importance as recent findings in moral psychology have highlighted the role of affect in moral considerations of individuals (Blasi 1999; Haidt 2003; Tangney et al. 2007). Current debates suggest that experience of moral emotions such as prosocial moral feelings is a matter of integration of both cognition and affect (Moll and de Oliveira-Souza 2007) and emotions have emerged as another source of moral judgment (Greene et al. 2001, 2004; Hofmann and Baumert 2010). Furthermore, emotions such as empathy and guilt have been shown to be conducive to moral sensitivity (Decety et al. 2011, 2012; Morton et al. 2006). Given these, it is fitting that study of moral considerations in ISS highlight and examine affect as well as cognition. Of particular interest is the experience of moral emotions (Haidt 2003) such as guilt and empathy in morally relevant ISS situations.

Lastly, few studies in the review set have examined IT characteristics in their research models particularly with respect to moral considerations of users. Previous discussions regarding the role of IT in users' moral considerations suggest that IT could make it difficult for users to extend their sense of morality to IT use situations (Siponen and Vartiainen 2002). Therefore, users' perceptions of IT characteristics may exert an influence on the outcome of moral decision-making processes in situations involving IT. In this regard, morally relevant ISS decisions may not be an exception and users' ISS decisions may be subject to influence from their perceptions of IT characteristics. Nevertheless, IT characteristics were rarely investigated in the extant literature and the only such characteristics examined were non-traceability/anonymity (Chatterjee et al. 2011, 2015; Zhang et al. 2006), reproducibility, proximity to victim, and intangibility (Friedman 1997). Furthermore, a few studies in the extant literature examined experiences that might be induced by IT. Security-related stress (D'Arcy et al. 2014, 2018), moral stress (Pierce and Henry 2000), and deindividuation (Hsu and Kuo 2003; Loch and Conger 1996) are such experiences examined. Given the potential role of IT in creating difficulties for moral considerations of users (Chatterjee et al. 2015; Johnson 2009; Siponen and Vartiainen 2002), further attention to IT characteristics and user experiences that they might induce seems necessary.

Given these findings, it seems that even though implications of moral considerations in ISS decisions have long been the subject of discussion in scholarly circles (D'Arcy and Lowry 2019; Johnson 2009; Kowalski and Kowalski 1990; Pemberton 1998), ISS research may have merely scratched the surface when it comes to moral considerations and how appealing to a user's sense of morality affects their ISS decisions. In this light, further understanding of moral considerations in ISS decisions to account for the role of IT characteristics seems crucial in order to justify and drive approaches that accommodate users' difficulty in extending their sense of morality to ISS. Therefore, in the next section, we focus on IT characteristics and conceptualize the potential role of such characteristics in moral considerations of ISS decisions.

3 CONCEPTUALIZING IT CHARACTERISTICS IN MORAL CONSIDERATIONS

As reported in the previous section, the literature review revealed a number of IT characteristics examined in research models in relation to moral considerations of users. In this section, with the aim of conceptualizing the role of IT characteristics in moral considerations of ISS decisions, qualities of IT artifacts, and qualities of interaction with IT artifacts are examined. Furthermore, the potential difficulties that IT-induced experiences might create for moral considerations of users are outlined. In doing so, the aim is not to introduce new IT characteristics —in fact all of the characteristics and IT-induced experiences discussed in this section have been known in some capacity in the extant literature— but to draw attention to their potential significance in moral considerations of users.

Figure 1 demonstrates our conceptualization of the role of IT in moral considerations of users. In this model, it is suggested that perceptions of qualities of IT artifacts, perceptions of IT interaction, as well as IT-induced experiences challenge users' moral considerations. They do so by having an impact on the processes that underlie moral considerations, both cognitive such as moral reasoning as well as affective such as emotional engagement.

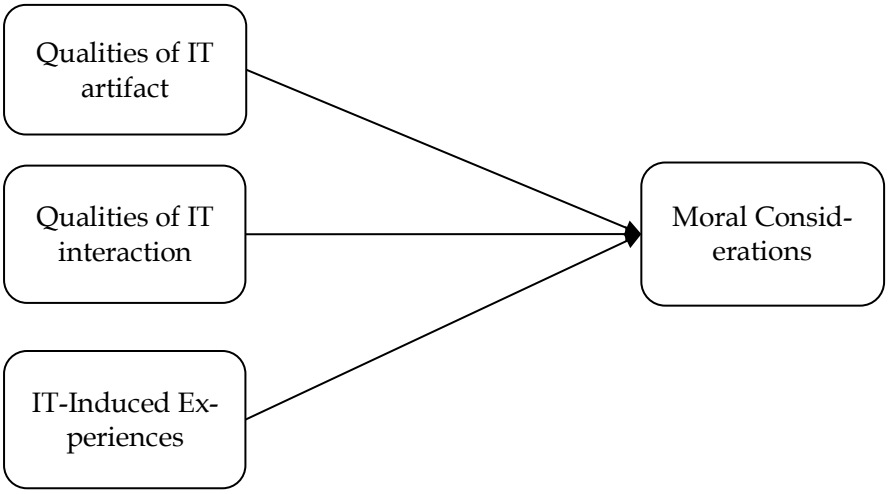

FIGURE 1 Model of the role of IT in moral considerations in ISS

3.1 Qualities of the IT artifact

Reproducibility refers to the quality of an artifact, such as a file, that allows it to be copied or taken away without inflicting damage to the artifact itself or to its ownership (Johnson 2009). Perceptions of reproducibility have been shown to affect users' justifications, evaluations, and understanding concerning privacy violations (Friedman 1997). Perceptions of reproducibility could obscure the infliction of harm as users may not recognize that their ISS-compromising acts may have victims. For instance, consider an act of ISS policy violation where an employee downloads customer personal information from a database in order to promote his own services. Such an act could lead to an ISS breach revealing personal information of many and inflicting harm. However, the employee might not understand the potential harm in this act if they perceive the database records to be reproducible. In this case, the employee may perceive the database records to be reproducible since taking them does remove their employer's ownership of the database records and does not damage the records themselves. Therefore, the employee's perceptions of reproducibility in this example could challenge them in understanding and interpreting the moral relevance of their copying of the database records. Some individuals need to "see blood flowing" before they realize there is a moral issue involved (Rest 1986), and the reproducible quality of IT artifacts, such as database records in the example, could mask the potential harm involved in ISS decisions.

In a similar vein, non-excludability is another quality that has been attributed to IT artifacts (Sinha and Mandel 2008). IT artifacts are non-excludable insofar as their consumption by one party does not remove access from others who wish to use the same artifact (Sinha and Mandel 2008). Similar to reproducibility, non-excludability could challenge users' understanding of harm in ISS decisions. In the example above, the employee might perceive database

records non-excludable since using it to promote their own services does not block their employer's access to the same records. The employee's perceptions of non-excludability of IT artifacts, therefore, could mask the potential harm to the employer as a result of revealing trade secrets, leading the employee to believe their action is harmless and morally irrelevant.

Reproducibility and non-excludability of IT artifacts are often associated with their intangibility (Weckert 1997). The quality of intangibility as the culprit in introducing difficulties for users have been touched upon by numerous scholars albeit often with respect to intellectual property and actions such as software piracy (Chiou et al. 2005; Lysonski and Durvasula 2008; Siponen and Vartiainen 2005, 2007). However, the intangibility quality may be important in an ISS context (Harrington 1996). Perceptions of intangibility of IT artifacts as mediums for transferring, accessing and storing information might transform the moral qualities of ISS actions. For instance, since database records are transferred on an intangible file, the employee might have difficulty understanding the volume of the information taken, and, therefore, the seriousness of exposing hundreds of customers' personal information.

Therefore, perceptions of reproducibility, non-excludability, and intangibility of IT artifacts could challenge the notions of damage and harm. By potentially disrupting users' understanding of the seriousness of the consequences, victims, and ownership, these qualities could make situations involving IT artifacts appear morally uninteresting, unimportant or harmless. This chain of events could, therefore, lead to users' difficulty of understanding the moral relevance of ISS decisions. Furthermore, since perceptions of qualities such as reproducibility and non-excludability could challenge users' considerations of harm and damage, ISS decision-making situations may not engage users emotionally. Individuals could become emotionally engaged in a situation if moral emotions such as empathy or guilt are stimulated (Decety et al. 2011, 2012; Morton et al. 2006; Silfver-Kuhalampi 2009). In the absence of emotional engagement, users might have difficulty in extending their sense of morality to ISS.

3.2 Qualities of IT interaction

In addition to IT artifacts, some of the IT characteristics that emerged in our review seemed to qualify interaction between a user and an artifact. One such quality was non-traceability/anonymity. The perception of non-traceability/anonymity of use may produce a change in the moral character of actions in cyber environments (Johnson 2009). This change concerns the possible role of sanctions or expectations of others in informing moral considerations of users. In anonymity, users might feel secure to engage in activities that violate ISS procedures since their identification as perpetrators and subsequently suffering from sanctions may seem unimaginable. Given evidence from several studies that sanctions could inform moral considerations of users in ISS decisions

(D'Arcy and Devaraj 2012; Myyry et al. 2009), perceptions of anonymity and thus experiencing a (possibly false) sense of security that there is no possibility for sanction may challenge users' moral considerations. For instance, in anonymity, the moral reasoning of the employee in the previous example might not be informed by the levels of moral reasoning that concern punishment avoidance and, therefore, the employee might not see any moral wrongdoing in downloading database records for his own purposes. Such an impact may explain findings that show the increasing effect of perceiving non-traceability on one's perceived ability to engage in IT misuse and subsequently intention to do so (Chatterjee et al. 2015) and the impact of anonymity on encouraging users to misuse internet resources in cases such as using P2P software at work (Zhang et al. 2006).

Distance from others is another quality of IT interaction emerging from our review. When using IT, users are typically away from those who could be affected by their actions. This distance could make it difficult to feel for the plight of those who could be affected (Dorantes et al. 2006; Friedman 1997; Peslak 2008; Siponen and Vartiainen 2002). Individuals are more likely to care for those close to them (Jones 1991). Greater distances from potential victims has been shown to affect the justifications, evaluations, and understanding of adolescents concerning privacy violations (Friedman 1997). This distance could make an action seem unimportant and uninteresting to require further attention and could distort the perception of victimhood and sense of damage. For example, the employee, in the afore-discussed example, might be uninterested in the difficulty that customers in another part of the world might endure if their personal information ends up in the wrong hands. As a result of greater distance, a harmful action using IT may not alarm users and may not engage them emotionally. Consequently, users may struggle with moral considerations toward that action.

A closely relevant quality of IT interaction to far distance is interconnectedness. Interconnectedness in using IT (Chatterjee et al. 2015) underscores the large scale of possible consequences of simple IT operations. Interconnectedness introduces a challenge insofar as an action could have harmful consequences for many in an operation that takes no more than a split second. For example, a simple action such as downloading an email attachment could result in the dissemination of malware and viruses on a mass scale. A lack of understanding of this quality when interacting with IT artifacts could make it hard for users to perceive the ramifications of their actions. In the case of the employee who downloads database records consisting of personal information of customers, a lack of understanding of the interconnected nature of IT use might create difficulties for the employee to see how their ISS violation exposes database records to threats that could disseminate private personal information rapidly and widely. Thus, lack of understanding of the interconnected nature of IT interaction could distort one's interpretations, emotional engagement and deliberations regarding the moral qualities of the action.

Lastly, interaction with IT is often characterized as morally ambiguous (D'Arcy et al. 2014; McMahon and Cohen 2009). IT use has often been described as lacking codes of behavior (Harrington 1997; Moor 2001) which some scholars have attributed to cultural lag (Peslak 2006; Roberts and Wasieleski 2012; Stylianou et al. 2013); that is a lag that occurs when material culture such as technology advances more rapidly than the non-material culture such as moral norms and code of behavior (Ogburn 1957). As such, moral ambiguity can create an environment in which users are left with conflicting ideas about what is considered acceptable behavioral norm. Users often draw on cues from their social environment in order to regulate their emotions, deliberations and behavior (Deci and Ryan 1985; Ryan and Deci 2000). In cases of moral ambiguity, however, such cues may not exist or may result in conflicting views which pull the user in different directions. Pierce and Henry (2000) reported such conflict when they observed inconsistencies between users' moral judgments, their perceptions of their coworkers' moral judgments, and the perceptions of company norms. Consequently, moral ambiguity challenges users' sense of morality and creates difficulties for their moral considerations.

3.3 IT-induced experiences

While, as noted, interaction with IT might represent qualities that introduce challenges to users' moral considerations, this interaction might induce experiences such as deindividuation, security-related stress, and moral stress that could challenge users as well. Moral stress is one such IT-induced experience observed by Pierce and Henry (2000). The moral ambiguity in interaction with IT may lead to conflicting moral considerations, such as conflicting personal, social and organizational moral judgments (Pierce and Henry 1999, 2000) that could induce an experience of moral stress (Pierce and Henry 2000). In a state of moral stress, it is possible that users would have difficulty with moral decision-making (Pierce and Henry 2000). In such a state, users might opt for a strategy whereby they can liberate themselves from feelings of self-blame and downplay their moral motivations.

A rather similar stress-related IT-induced experience is security-related stress, that is, stress induced by ISS requirements (D'Arcy et al. 2014, 2018). D'Arcy et al. (2014) argued that overload, complexity, and uncertainty of ISS requirements can induce stress. D'Arcy et al. (2014) suggested that users tend to cope with security-related stress using techniques of moral disengagement (Bandura 1991). Such techniques could challenge moral considerations insofar as they provide users with a mechanism to deprioritize a moral decision in favor of others.

In addition to experiencing stress, interaction with IT artifacts might leave a user in a state of isolation and alienation, particularly due to perceptions of anonymity in IT interaction. This feeling of isolation could manifest itself in experiencing deindividuation (Loch and Conger 1996). Deindividuation reflects

a state of lowered self-awareness and self-monitoring (Diener 1979). It represents the sense of losing self-identity and becoming immersed into group norms, particularly in antisocial behavior (Zimbardo 1969). An individual experiencing deindividuation might not rely on personal principles and ideologies but prefer to conform to group norms (Diener 1979).

For instance, members of a sales team who work remotely and deem ISS procedures as an impediment to their work might experience deindividuation as they might feel isolated from other teams and colleagues. In the ISS context, deindividuation has been shown to be linked to exhibiting less concern for protecting the information privacy of others (Hsu and Kuo 2003) and to reading others' emails (Loch and Conger 1996). Consequently, experiencing deindividuation induced by interactions with IT artifacts might challenge users' moral considerations by lowering their reliance on moral principles and ideologies and increasing their reliance on group norms with which they identify. One should note, however, that group norms may not be congruent with conventional social norms. Considering that the interaction with IT is often described as one lacking established guidelines (Harrington 1996), it is likely that any potential conflict between these two sets of norms may be resolved by bypassing the conventional norms. Previous research in ISS has provided evidence that indicates such an outcome. For instance, D'Arcy and Hovav (2009) showed that any effect of ISS education, training, and awareness programs in discouraging unauthorized access to information could be diminished if an individual was a remote worker who was more likely to experience deindividuation (D'Arcy and Hovav 2009). ISS education, training, and awareness programs are means for communicating conventional norms; therefore, their reduced impact among remote workers could be a sign of the challenging impact of deindividuation. In a similar vein, the reported decrease in the deterring effect of computer monitoring in discouraging unauthorized modification of data among employees who spend more time working remotely (D'Arcy and Hovav 2009) could also be due to deindividuation. In this case, computer monitoring could be viewed as enforcement of conventional norms which the user bypasses.

4 EMPIRICAL STUDY OF MORAL SENSITIVITY

In the absence of moral sensitivity in an ISS decision-making situation, users may not understand the moral relevance of their decision, thus, may not engage their moral schemata (Rest 1986). Prior ISS research on moral considerations of users has often presupposed or inadvertently triggered moral sensitivity. A common approach in prior ISS research is to ask users whether they find an act such as ISS policy violation in a given scenario "morally right", "ethically right", or "acceptable". In doing so, it is assumed that users are able to perceive the act as morally relevant, and that they are able to understand the potential ramification of that act on the welfare of others. However, in organizational settings, users may be on their own to interpret an ISS decision-making situation and may not be able to identify potential victims of their ISS decisions (Siponen and Vance 2010). Furthermore, the use of moral language such as "morally right", "ethically right", or "acceptable" in such questions provides users with cues indicating the presence of a moral problem, in turn, instructing them to reflect on the scenario in moral terms and triggering their moral sensitivity. Unfortunately, the few studies that examined moral sensitivity as a matter of recognition of "moral content" in prior research may have unintentionally triggered users' sensitivity due to use of such moral language (Dorantes et al. 2006; Goles et al. 2006). Against this backdrop, this dissertation zeroes in on moral sensitivity as a moral consideration that is crucial to users' moral decisions-making in ISS and examines how the moral sensitivity process unfolds.

In examining moral sensitivity, this dissertation looks into users' understanding of harm and means to prevent harm in ISS decisions, by investigating their interpretation of ISS decision-making situations without making any reference to the moral relevance of the situation. Additionally, the dissertation examines the potential impact of IT characteristics on moral sensitivity in ISS decision-making. As conceptualized previously (Figure 1), some IT artifact qualities, IT interaction qualities and IT-induced experiences could mask the potential harm and damage in ISS decisions. This could introduce challenges to users' moral sensitivity making it difficult for them to extend their sense of morality to ISS decisions.

Furthermore, the role of affect in the process of moral sensitivity in ISS decisions is examined. Examination of affect is of interest bearing in mind that IT characteristics can mask potential harm in ISS decisions, leading to reduced emotional engagement among users. Given recent findings regarding the importance of affective responses such as experience of moral emotions to moral considerations of individuals (Blasi 1999; Haidt 2003; Tangney et al. 2007), particularly, their conducive role to moral sensitivity (Decety et al. 2011, 2012; Morton et al. 2006) reduced emotional engagement in ISS decisions could lower users' moral sensitivity. The following are the research questions examined in the empirical study.

1) How morally sensitive are users in ISS decision-making situations?
2) What is the role of IT characteristics in users' moral sensitivity and understanding of harm in ISS decision-making situations?
3) What is the role of emotions in users' moral sensitivity and understanding of harm in ISS decision-making situations?
4) How does the moral sensitivity process unfold in ISS decisions?

By attending to these research questions, this dissertation addresses some of the aforementioned areas in prior ISS research on moral considerations that may need further attention. Firstly, study of moral sensitivity shifts the focus from moral judgment component in the four-component model of moral behavior to moral sensitivity that could precede moral judgment. Secondly, this dissertation highlights the role of IT characteristics in moral considerations of users insofar as moral sensitivity is concerned. As discussed, attention to the role of IT characteristics has been largely absent in prior research. Furthermore, in examining affect in moral sensitivity, the dissertation highlights the roles of both affect and cognition, while prior research has been predominantly focused on cognition.

4.1 Method

In order to study moral sensitivity in ISS, a scenario approach is employed where respondents would listen to audio recordings of conversations between a protagonist and another user involving a morally relevant ISS dilemma. Respondents are then asked to imagine themselves in the shoes of the protagonist and answer a few questions. In each scenario, the protagonist is asked for a favor which could potentially lead to an ISS violation. To increase practical relevance, each scenario is developed based on the ISS policies where the study is conducted, and is delivered in two episodes. In episode one of each scenario, per guidelines provided by Vance and Siponen (2014), respondents receive information about a specific ISS activity and are informed that the activity in question would be a violation according to their ISS policy. In doing so, the stage is set for the dilemma itself in episode two.

This method is deemed suitable for several reasons. First, use of scenarios for examining ISS decision-making is common in the extant literature (Vance et al. 2015; Warkentin et al. 2011) as it allows contextualization of a situation and requires minimum effort from respondents (Guo et al. 2011; Vance et al. 2012). Additionally, respondents are required to take the role of the protagonist in the scenario which is particularly of value since moral sensitivity is known to be associated with one's role-taking abilities (Myyry and Helkama 2002). Interpretation of the scenarios and the moral issues therein is left to the respondents as the dilemmas are not characterized as hypothetical moral situations, but practically relevant ISS situations. Lastly, audio recordings have been shown to elicit sufficient data to allow examination of moral sensitivity (Bebeau et al. 1985; Volker 1984).

4.1.1 Development of scenarios

In order to develop the scenarios[1], first the ISS policies of the two large Nordic universities at which the study was conducted were examined. With due attention to the terms of the policies and the roles of the potential respondents within these settings, seven distinct scenarios relevant to each role were developed. Given the characteristics of the research settings, three different roles were considered for the potential respondents, namely, researchers, administration staff, and students. Scenarios were developed with due consideration of the IT resources available to, and the job descriptions and assignments of an individual in each role and situations that could lead to exposure of such resources. Realism of the scenarios were examined when audio recordings were in development. For each role a unique password sharing scenario, and an access sharing scenario was developed. For the researcher role, an extra email security scenario was also developed, as according to their role researchers in research settings had to frequently handle emails from unknown sources outside the organization that they could not simply ignore. This was not the case for the student and the administration staff roles, therefore, a corresponding email scenario was not developed for them. A brief synopsis of each of the scenarios is provided in Table 3.

TABLE 3 Summary of developed scenarios

Respond-ent Role	**Scenario type {ISS Property}**	**Synopsis**
Research-ers	Access sharing {Availability, Confidentiality, Integrity}	Pekkonen is a researcher with access to a server for pro-cessing large datasets. Permission to use the computa-tional resources of the server are provided to Pekkonen based on their project proposal. Another researcher who also works with large datasets but does not have access to the server offers a potential collaboration opportunity if Pekkonen can upload a dataset and run a script on the server.

[1] Audio recordings are available from https://kyberper.github.io/kyberper/

	Password sharing {Confidentiality, Integrity}	Smith is a researcher who is also responsible for grading students in a university course before a deadline set by the faculty. Smith has access to student personal information and data from research participants on their laptop. In an incident, Smith injures their back and has to leave their laptop at the office. Smith receives a call from the faculty office asking her to either submit the grades or find another way. One suggestion is to share their password with the faculty office.
	Email security {Confidentiality, Integrity}	Williamson is a researcher at the university whose position requires them to supervise potential doctoral candidates. Williamson has access to student personal information as well as research data collected from participants. Williamson gets an email that looks like it is from a good doctoral candidate, however, the attached documents are sent in an unfamiliar format and the email address is a pseudonym.
Administration staff	Access sharing {Confidentiality, Integrity}	Pekkonen is a member of administration staff at the university who does a lot of remote work from home. Pekkonen is working on their laptop when a colleague arrives to pay them a housewarming visit. Pekkonen leaves the laptop to go prepare coffee when the colleague asks to use their laptop to show them a video about remote working.
	Password sharing {Confidentiality, Integrity}	Smith is a member of administration staff at the university whose responsibilities involve assisting lecturers with study matters such as grading. In an incident, Smith injures their back and has to leave their laptop at the office. A lecturer contacts Smith and asks for assistance with modifying student grades as it is only Smith who has access privileges for modification. One suggestion is to share their password and allow the lecturer to modify the grades.
Students	Access sharing {Availability}	Williamson is a student at the university and is provided with one of a few licenses available for a development tool in order to work on a project. A friend of Williamson's could use the tool for delivering her course project but is not provided with a license as their work is considered low priority. The friend asks Williamson to allow them to use their license and access the tool.
	Password sharing {Confidentiality, Integrity}	Pekkonen is a Master's student who in preparation for their thesis has collected and stored data from research participants on their university cloud storage account. Pekkonen also keeps a group assignment file on the same cloud storage account and is supposed to send that file to their group-mates for submission before a deadline. An incident happens where as the deadline approaches, Pekkonen is stuck on the road without access to the cloud. A group-mate calls and asks for Pekkonen's share of the group assignment. One suggestion is to share the password to the cloud and allow the groupmate to take the file.

4.1.2 Development of audio recordings

In order to develop the audio recordings from the developed scenarios, we developed scripts of conversations between a protagonist and another user (a friend, a student, or a colleague). These scripts were read by English-speaking voice actors and recorded. None of the researchers were involved in voice acting in order to make sure that the respondents would not associate them with the characters in the audio recordings. The recordings were available only in English. This was deemed acceptable as the research settings represented highly international environments where English was commonly spoken by potential respondents.

Even though potential respondents in the research settings were required to know and comply with the their organizational ISS policies, in order to make sure that the respondents were aware of what counted as an ISS violation (Siponen and Vance 2014), we included the relevant terms of the policy in episode one of each audio recording. Moreover, considering the variation in the type of information and other resources accessible to different respondents based on their roles, in episode one we outlined examples of the type of information or resource that was at risk. For instance, in the password sharing scenario developed for the researcher role, it was mentioned that the protagonist had access to personal information of students and research participants.

Development of the audio recordings was done with due respect to (1) brevity, and understandability, (2) realism relative to the respondent's role, (3) absence of unintended moral issues and (4) absence of inadvertent tip-offs regarding the moral issues. These were considered according to a list of requirements laid out by Sparks (2015) for a scenario to be effective in investigating moral sensitivity. In order to evaluate whether the developed audio recordings satisfied the aforementioned requirements, ten experts on ISS, psychology, criminology and information systems consisting of professors, post-doctoral fellows and doctoral candidates were approached for evaluation. Evaluators considered the records sufficiently brief and understandable to avoid respondent fatigue. Scenarios were considered realistic and in some cases the evaluators reported their personal experiences of similar situations. Additionally, the evaluators confirmed the absence of unintended moral issues or inadvertent tip-offs. However, based on suggestions made by the evaluators, references to male/female pronouns and first names of the characters were removed from the scenarios in order to remove the possibility of potential gender bias.

4.1.3 Development of the scoring system

In order to examine moral sensitivity of the respondents for a given scenario, there was a need to develop a moral sensitivity scoring system. Several distinct moral sensitivity scoring systems have been reported in the literature based on theoretical conceptualization of moral sensitivity. Sparks (2015), for instance, summed up the number of moral issues identified by a respondent in a job-

hunting dilemma as the moral sensitivity score. Bebeau et al. (1985) developed a scoring system in the dentistry context based on sensitivity toward the characteristics of a patient and awareness of actions that serve the rights of others. Myyry and Helkama (2002), on the other hand, developed a scoring system in the professional social work context based on identification of special characteristics of the people involved, as well as their rights, and responsibilities.

With such scoring systems in mind and considering that in an ISS context —unlike the dentistry or the social work contexts— parties involved might not be easily identifiable (Siponen and Vance 2010), the scoring system for sensitivity toward moral issues in ISS was developed. This scoring system is based on two classes:

1) awareness of parties involved and their rights with respect to well-known ISS concerns, namely: availability, confidentiality and integrity (the Party and Consequences Class, PCC),
2) awareness of the courses of action that could protect ISS rights (the Course of Action Class, CAC).

Simply put, the PCC class addresses respondents' understanding of the potential harm associated with an ISS decision, while the CAC class addresses understanding of possible means to avoid that harm.

Since the focus of the dissertation is sensitivity toward moral issues in an ISS dilemma, this classification focuses only on parties involved in terms of ISS concerns. Incidentally, this means that awareness of the person asking for a favor in each dilemma was not scored as they were designed in the scenarios in a manner that their rights to availability, confidentiality and integrity were unharmed and they were not responsible for an ISS decision in any capacity. Furthermore, awareness of rights of the parties involved in each scenario was assessed in terms of awareness of ISS consequences. For instance, right to availability of computational resources was assessed as the awareness that misuse of computational resources would delay or impede authorized users from access to the same resources. In this dissertation, the term 'party' denotes parties involved in terms of ISS concerns and 'consequence' denotes ISS consequences unless otherwise specified.

Since each of the developed scenarios exhibited different characteristics, first a different set of items within each class was developed for each scenario, blind to data. This led to the development of a scoring template for each scenario. Table 4 reflects an example of such a scoring template for one of the scenarios. Each item in the PCC class consisted of an affected party and the consequence for that party and each item in the CAC class consisted of a course of action. In this manner, each item in the PCC class was assessed on a three-point scale (0 = no awareness, 1= awareness of the party but not the consequence, 2= complete awareness) and each item in the CAC class was assessed on a two-point scale (0 = no awareness, 1= complete awareness).

TABLE 4 A scoring template example

	Class 1: awareness of parties involved and their rights with respect to availability, confidentiality and integrity (the PCC class)		**Class 2: awareness of the party responsible and the course of action that could protect such rights (the CAC class)**	
Party involved	**Rights of parties involved**	**Scale**	**Course of action**	**Scale**
Oneself	Compromising personal account/data/ info	2	Refuse & accept responsibility	1
Institute	Exposing assets, IP, & infrastructure	2	Technical solution	1
Users in server queue	Delays/troubles other people's work	2	Launch an official collaboration	1
Server users	Reveal/manipulate private information	2	Get IT support (such as necessary equipment)	1

The moral sensitivity of a respondent for a given scenario was then calculated as the ratio of the sum of their scores for each item to the overall score possible in that scenario. Assessing the moral sensitivity score as a standardized ratio between 0 and 1 allowed standard assessment of scores between different scenarios as each scenario enjoyed a unique set of characteristics and, subsequently, a distinct overall score. In addition to moral sensitivity scores, each respondents' average score for each class (the average PCC score and the average CAC score) was also calculated as the sum of their scores for each item in that class divided by the overall number of items to allow examination of respondents' sensitivity in either class. Table 5 shows how each respondent's scores for a given scenario was calculated based on a given template.

TABLE 5 Scoring formulas

Respondent score	**Calculation Formula**
Moral sensitivity score	(Sum of scores for all items)/(Total possible score)
Average PCC score	(Sum of scores for PCC items)/(Overall number of PCC items)
Average CAC score	(Sum of scores for CAC items)/(Overall number of CAC items)

4.1.4 Data collection

Moral sensitivity relies on the interpretation abilities of an individual and, therefore, any references to morality and ethics during data collection could prime respondents and trigger their sensitivity. This has led previous research to examine moral sensitivity using either interviews or open-ended written responses (Bebeau et al. 1985; Jordan 2007; Myyry and Helkama 2002; Sparks 2015; Sparks and Hunt 1998). Use of such methods allows the researcher to examine respondents' interpretation of a given scenario without instructing them to choose between parties, consequences or courses of action that might be

relevant in a scenario. In this respect, both methods were considered suitable for this study. However, since interviews involve interaction between an interviewer and a respondent, interview respondents may experience higher engagement with a given scenario, and, subsequently, they might examine the scenario in further detail than those who are less engaged. In order to account for and examine such potential engagement effect, in this study, data was collected from three groups. The no engagement group (N=17) who received all the questions in written form at once and were asked to return their answers in 1-2 pages in written form. The low engagement group (N=16) who participated in one-on-one interviews in which no questions were asked regarding the parties involved and consequences. And lastly, the high engagement group (N=7) who attended one-on-one interviews in which, in addition to questions answered by the other two groups, were specifically asked to identify parties involved and consequences.

In line with the design of the scenarios, respondents consisted of researchers, administration staff members and students from two large Nordic universities. Interview respondents (both low and high engagement groups) were from a variety of backgrounds and professional fields. Written responses were collected as a voluntary pre-course assignment from graduate management and business students who were also part-time working professionals.

Recruitment for interviews took place by posting study participation invitations in online newsletters as well as by reaching university networks via emails. Additionally, the snowballing technique was used whereby each respondent was asked to forward the participation invitation to their colleagues and friends. The participation invitations described the aim of the study as examination of users' perceptions of ISS dilemmas and avoided any terms related to moral notions such as ethics, fairness, and harm. After the interview, and upon request, the aim of the study was further explained to the respondents as examination of moral sensitivity in ISS dilemmas.

Since ISS could be a sensitive issue within an organization, a number of measures were taken to avoid potential bias. To this end, participation invitation for all respondents explicitly stressed that responses were anonymous, there were no correct/incorrect answers to the scenarios and that the researchers were not associated with the decision-making bodies at the research settings. Additionally, no personal data such as age, gender, field of work/study were collected from the respondents. Each respondent listened to one to three scenarios depending on the relevance of the scenarios to their role.

During data collection, all respondents were given the chance to listen to the audio recordings as many times as they wished. Furthermore, the transcript of the conversations in the audio recording were also provided to the respondents. Despite satisfaction with the understandability of the audio recordings, this measure was taken to make sure the audio recordings were fully understandable to non-native English speakers, or those with hearing problems. Respondents commonly made use of the transcripts. Overall, 88 responses to the scenarios were collected. As Table 6 shows, the highest share of the responses

went to the password scenario type, followed by the access scenario type and email scenario type, respectively.

All respondents were asked to first listen to episode 1 and then episode 2. After listening to audio recordings for a scenario, each respondent was asked to take the role of the protagonist and answer a number of probing questions. Data collection from interview respondents was conducted primarily online, with a total of seven interviews across both low and high engagement groups conducted in person at the premises of the research settings. Interviews in the low engagement group for a given scenario lasted between 7 to 21 minutes. In the high engagement group, interviews lasted between 5 to 13 minutes. Data collection from written respondents, on the other hand, was fully online and this group of respondents were given one week to return their responses.

Respondents in the no engagement group and low engagement group were asked, in order, to explain

1) what happened in the scenario,
2) how they felt about the situation,
3) what issues needed to be taken into consideration,
4) what could be done.

In addition to these probes, the high engagement group were asked to identify the parties involved, why they thought a course of action was appropriate and what arguments could be made against their decision. Specifically, the high engagement group was asked to explain

1) what happened in the scenario,
2) how they felt about the situation,
3) who were the parties involved,
4) what issues needed to be taken into consideration,
5) what could be done,
6) why they thought a course of action was appropriate,
7) what arguments could be made against their decision.

These questions were asked in the order outlined above from each group. However, in both the low engagement and high engagement groups, follow-up questions may have been asked to clarify responses. In the no engagement group, asking follow-up questions was not possible as responses were in written form. At no time during data collection was any reference to morality, IT artifacts, or any specific emotions made. In other words, there were no questions asked about morality, or perceptions of IT characteristics, and the one question about users' affective responses (i.e. how they felt) was open-ended without using a specific scale. However, if during an interview, a respondent addressed morality, IT artifacts, or specific emotions, further follow-up questions such as "Could you please elaborate what you mean by morality?" were asked.

TABLE 6 Data collected per group of respondents per scenario

Respondent role	Scenario type	No engagement	Low engagement	High engagement	Total
Researchers	Access sharing	0	10	0	10
	Password sharing	0	9	7	16
	Email security	0	9	7	16
Administra-tion staff	Access sharing	0	3	0	3
	Password sharing	0	3	0	3
Students	Access sharing	17	3	0	20
	Password sharing	17	3	0	20
Total per scenario type	Access sharing	17	16	0	33
	Password sharing	17	15	7	39
	Email security	0	9	7	16
Total	All scenarios	34	40	14	88

4.1.5 Analysis

Analysis of the responses consisted of the content analysis of text data (Lacity and Janson 1994) as well as analysis of elapsed time. Evaluation of the outcome of the content analysis and elapsed time analysis was performed using Kernel Density Estimation method (Silverman 1986) and correlation analysis (Pearson's r).

4.1.5.1 Content analysis

After transcription, interview responses as well as written responses were analyzed as text data using content analysis (Lacity and Janson 1994). First, a set of predefined code categories was developed which was primarily based on the items in the PCC and the CAC classes of the scoring system. These code categories consisted of parties involved, consequences, courses of action, IT characteristics, and affective responses. Each of these code categories consisted of several subcategories. For instance, the code category known as parties involved included subcategories such as the decision-maker, the institute or its representatives, and third parties such as the personal information owners, or the others users. The code category named Consequences consisted of the codes such as compromising personal accounts, exposing assets, intellectual property and IT infrastructure, revealing/manipulating personal/sensitive information, and delaying other users' work. Since the parties involved, consequences, and courses of action code categories and their subcategories were informed by the scoring system which was itself based on the theoretical conceptualization moral sensitivity, these code categories were instrumental in scoring moral sensitivity. In effect, these code categories provided the information to score respondents' moral sensitivity, average PCC and average CAC for a given scenario using the scoring template.

IT characteristics and affective responses were included as code categories in the content analysis in order to examine the role of IT and the role of affect in moral sensitivity. Subcategories considered for IT characteristics were based on

characteristics conceptualized in Section 4 such as non-excludability, reproducibility (Johnson 2009), interconnectedness (Chatterjee et al. 2015), anonymity (Zhang et al. 2006), and distance (Friedman 1997). As for affective responses, subcategories considered were moral emotions (Haidt 2003) such as empathy, and guilt. Empathy is known as an affective response congruent with that of another person that comes from understanding the other person's suffering, emotional state or condition (Eisenberg and Miller 1987). Guilt is closely related to empathy and is experienced due to moral transgressions (Tangney et al. 1996) particularly when others' welfare or suffering is of concern (Haidt 2003). Further subcategories for both categories, however, emerged from the data during coding. In order to evaluate the role of IT characteristics, and affective responses in understanding of harm in ISS scenarios, the relationship between expressions of IT characteristics and affective responses with expressions of parties involved, and/or consequences was examined, that is, the first time that a respondent recognized a party or a consequence. This analysis was then followed by the correlation analysis with moral sensitivity scores, average PCC scores and average CAC scores.

Content analysis also involved analysis of unrecognized categories and subcategories. The goal was to allow for new categories to emerge from the data if they were distinctly different from the predefined ones. New subcategories emerged as a function of recurring patterns with similar conceptualization after multiple readings of the data and the parts of the text that were coded as unrecognized. In this study, we only report the newly found subcategories that were mentioned by respondents at least five times. After careful analysis and comparison of subcategories, this exercise led to emergence of two new categories and several subcategories for IT characteristics and affective responses.

One category that emerged during the analysis was 'legal/contractual and reputational consequences'. This category marked respondents' expressions of the legal or contractual troubles (such as punishment) or the loss of reputation imposed on the parties involved due to a given ISS violation. This category was different from the consequences category that involved only ISS consequences. Another code category discovered was the 'immediate action' category. Immediate action emerged as a category distinct from the course of action category for two reasons. (1) Unlike the course of action category which could protect the rights of the parties involved while resolving the dilemma, immediate action appeared as the utterance of simple reject/accept reactions to the dilemma which could not in itself resolve the dilemma. These reject/accept decisions were sometimes followed up by a course of action to resolve the dilemma. (2) Immediate action category marked an immediate utterance of a decision that followed respondents' explanations of a given dilemma irrespective of the interviewer's questions. The new subcategories that emerged from the data recognized new IT characteristics and affective responses and will be discussed in their respective results sections.

In order to examine the reliability of the coding, the content analysis also involved inter-coder reliability analysis. After initial coding of the data, a second coder coded 12 random scenarios from five different respondents. The analysis included the code categories parties involved, consequences, and courses of action. The inter-coder reliability reflected an acceptable 80.9 % agreement, and a value of 0.861 for Krippendorff's Cu-α. This reliability analysis did not include IT characteristics or affective responses since these code categories mostly emerged from the data after the first round of coding. In order to test the reliability of these code categories, first the IT characteristics and affective responses that emerged from the data were defined and along with the expressions from the respondents were sent to a second coder. The second coder examined the codes and organized them according to the definitions. Overall, this analysis yielded an agreement of 90.4% between the two coders.

4.1.5.2 Elapsed time analysis

As discussed previously, the content analysis led to identification of immediate action as a code category marking a recurring pattern in which a respondent would provide an immediate reject/accept reaction to a dilemma. Initial examination of the data from interview respondents suggested that this immediate action occurred very early on in a given interview, and often preceded text data where most parties involved, consequences as well as legal and reputational consequences were identified. Furthermore, in a number of cases, respondents tended to change their preference for this immediate action by the time the interview was reaching its conclusion. Recurrence of this pattern appeared to suggest that there was an element of time involved in moral sensitivity, particularly in relation to one's ISS decision in a scenario. This matter led to examination of elapsed time in each interview.

To this end, all interview data were re-examined, and the times of utterance of immediate actions as well as every first utterance of a party involved, consequence, and legal, reputational consequence and expressions of IT characteristics were recorded for further analysis. In this manner, a time series was developed for each of the mentioned code categories, the starting point of which was the start of the interview for a given scenario. Utterances of affective responses were not included in this analysis since respondents were specifically asked during the interviews how they felt. This raised the issue that expressions of affective responses were biased to appear as a response to this question.

Elapsed time analysis was conducted only on interview responses and not on written responses as time could be irrelevant in writing and we could not ensure that written responses reflected immediate reactions, thoughts and observations of the respondents. Furthermore, the analysis was conducted on two groups of interviews: (1) the low engagement group where interviews tended to be longer and no direct questions regarding parties involved and consequences were asked and (2) the high engagement group where interviews tended to be shorter and questions were more direct. Distinguishing between these groups was necessary in the analysis as the structure of the interview and

questions asked tended to be slightly different (see Section 5.1.4). Evaluation of the time series was performed using the kernel density estimation method (Silverman 1986) with a bandwidth of 60 seconds and a Gaussian kernel.

4.1.5.3 Kernel Density Estimation (KDE)

KDE is a method that allows estimation of probability densities and produces the probability density curve of a variable (Silverman 1986). KDE was used in this study to evaluate the results of elapsed time analysis and moral sensitivity scores. In KDE, individual occurrences of a phenomenon (such as utterances of consequences in time or one's moral sensitivity score) are represented by a so called "kernel" (rectangular, Gaussian, etc.) along a line (for instance elapsed time or moral sensitivity scale). A KDE curve is produced when these kernels are stacked on top of each other according to a certain width on the given line. This width is known as the bandwidth (Silverman 1986).

The choice of the bandwidth has an impact on the smoothness of the produced curve. Too small a bandwidth could produce an under-smooth curve with too many data peaks, while too big a bandwidth could result in an over-smooth curve which provides little information about the phenomenon under investigation. KDE is considered ideal for investigation of mutual information between time series (Moon et al. 1995).

In this study, for the purposes of elapsed time analysis, a bandwidth of 60 seconds was chosen to represent respondents' utterances within one minute. As for the analysis of moral sensitivity scores, a bandwidth of 0.1 was chosen to represent an incremental scoring range for moral sensitivity ratio. The chosen bandwidths appeared to be suitable as they appropriately highlighted important peaks in the data without hiding valuable information. The peaks of the KDE curve in the elapsed time analysis conducted in this study represent times when respondents' expressions of a subcategory overlaps the most. The peaks of the curve in the analysis of moral sensitivity scores, on the other hand, represent the most likely scores.

4.2 Results

Analysis of the responses showed a positive skew in the distribution of moral sensitivity scores, that is, users' moral sensitivity scores tended to be relatively high. Furthermore, the results unearthed the IT characteristics that users tend to take into consideration in their examination of ISS decisions. In regards to affective responses, a standout discovery was the absence of expression of moral emotions toward individuals or entities whose information assets could be exposed. Furthermore, our results showed that moral sensitivity might be related to the time spent reflecting on a given scenario.

4.2.1 Moral sensitivity in ISS

In order to examine respondents' sensitivity toward moral issues in a given scenario, their understanding of moral issues in terms of parties involved, consequences for the parties involved and the courses of action that could protect those involved was investigated. This was achieved through content analysis of expressions of the respondents, and scored based on the scoring template for each given scenario. Doing so allowed us to examine sensitivity toward moral issues without relying on respondents' ability to consciously verbalize each dilemma in moral terms. However, in a few cases —both during the interviews as well as in written responses— respondents explicitly referred to notions such as "morality", "rightness", "ethicality", "fairness" and "harm". In one such case, for instance, a respondent underlined her concerns about sharing access to a development tool.

> *I can't really think of a circumstance that I would give [access to] the tool to her. Because, I take it very seriously that there are tools and platforms and that have information that can't just be accessed by anyone. And, I mean, it would get me in trouble and it would be morally incorrect to do that.*

While these cases seemed to indicate that at least some respondents were conscious about the moral relevance of a scenario, they were often hard pressed to explain what they meant and what the moral relevance of the scenario was. For instance, in interviews where we had the chance to probe the respondents with follow-up questions, one respondent backtracked on using the term ethical and explained "I think, I just used the word loosely". In other cases, interview respondents seemed to be lost for words and seemed confused. For example, the respondent who characterized sharing access to a development tool as morally incorrect, seemed unable to describe the moral issue.

> *Because I've been told not to and just because I feel some sort of compassion or something for the person, it's, hmmm, ok, well, morally, I guess you would feel like it's correct, but in reality that's not a valid reason for something like this.*

Such characterization indicated that even though some respondents may have been aware of an underlying moral issue in a given scenario, moral sensitivity in ISS decisions remained largely a nonconscious affair. In that respect, as Figure 2 and Table 7 show, when all scenarios were considered, moral sensitivity is normally distributed and respondents seemed to have relatively high sensitivity toward moral issues in the scenarios. As Table 7 indicates, there were negligible variations in respondents' moral sensitivity toward scenarios across scenario types (password, access, or email).

TABLE 7 Statistics for moral sensitivity scores

Scenarios	Descriptive statistics	Kolmogorov K-S test
All scenarios	Min=0.2, Max=0.9, N=88, mean=0.59, standard deviation=0.14	statistic=0.196, p=0.516
Password scenarios	Min=0.333, Max=0.9, N=39, mean=0.62, standard deviation=0.13	statistic=0.104, p=0.790
Email scenarios	Min=0.2, Max=0.9, N=16, mean=0.58, standard deviation=0.16	statistic=0.217, p=0.385
Access scenarios	Min=0.375, Max=0.875, N=33, mean=0.57, standard deviation= 0.13	statistic=0.161, p=0.325

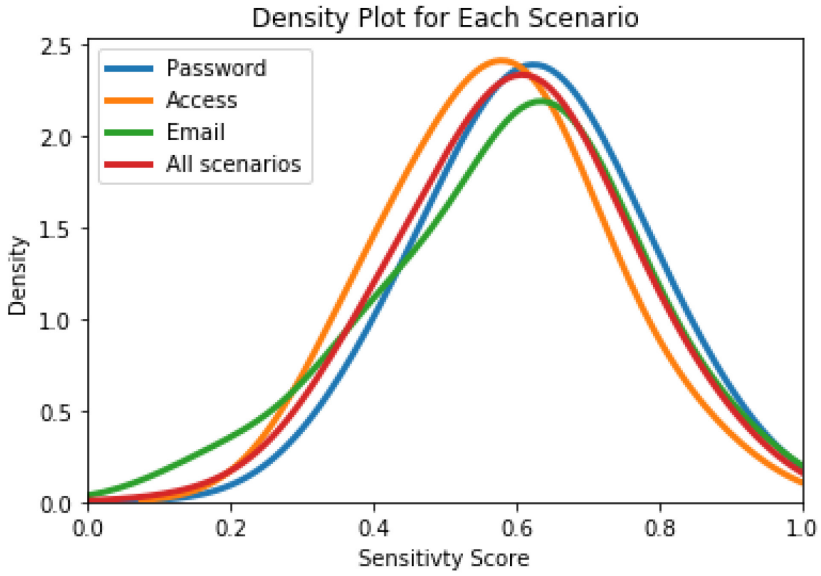

FIGURE 2 Density plot for moral sensitivity scores (all groups)

Given that the data collection method in this study consisted of three groups, namely: no engagement group (written responses), low engagement group (interviews), and high engagement group (interviews), we examined whether the distributions changed based on the level of engagement. Overall, the outcome of splitting the data based on the engagement groups (Figure 3, 4, and 5) did not indicate a notable shift in the distribution, even though the scores for the password scenarios in the no engagement group appear to be slightly higher than that of other groups. These results suggest that the method of data collection and the level of engagement did not trigger different levels of moral sensitivity in the respondents. However, considering that splitting the data reduced the number of observations in each group, some observations became more pronounced as in the email scenarios, for both low and high engagement.

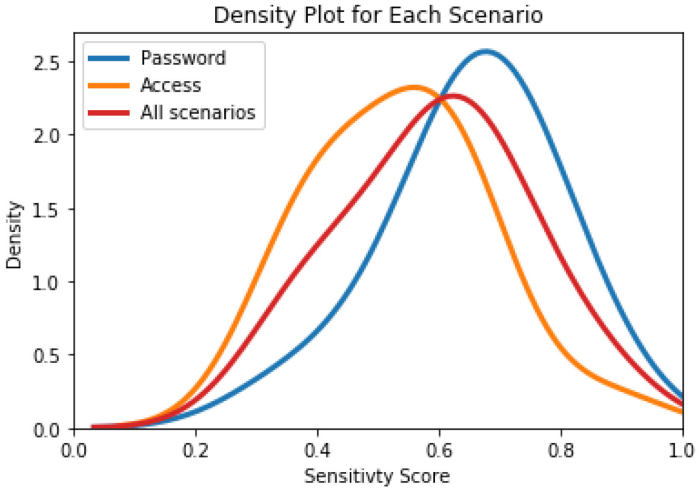

FIGURE 3 Density plot for no engagement group

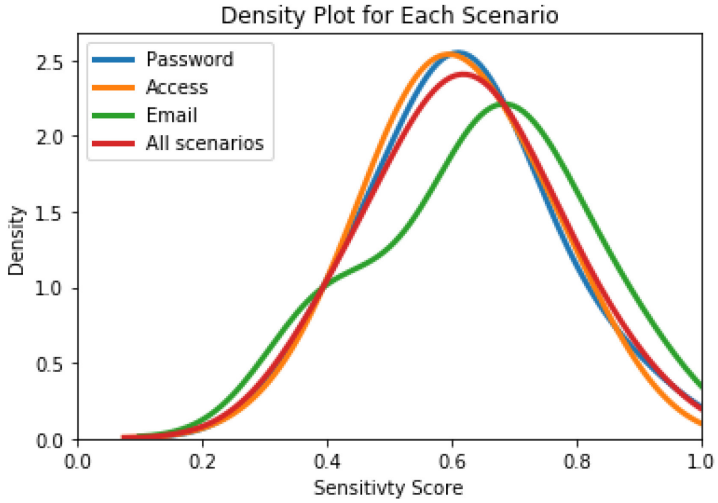

FIGURE 4 Density plot for low engagement group

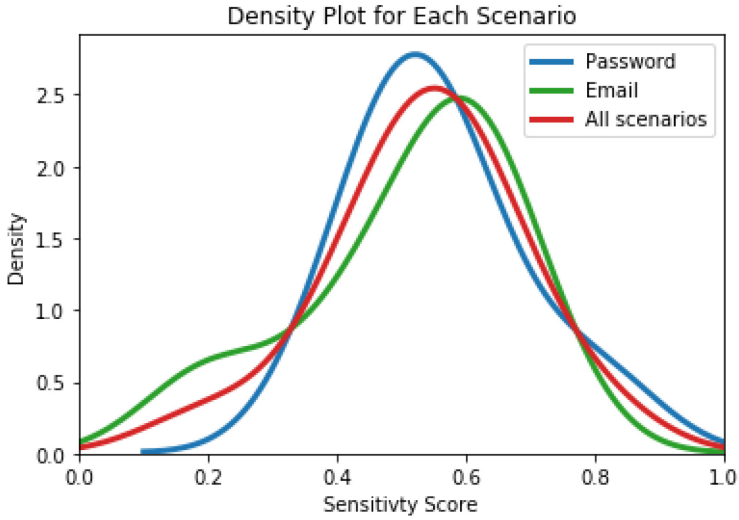

FIGURE 5 Density plot for high engagement group

4.2.2 Role of IT characteristics

Respondents referred to several IT characteristics both during the interviews as well as in written responses. Overall, respondents referred to IT characteristics in 48 instances: 33 instances in the low engagement group, 2 in the high engagement group and 13 in the no engagement group. Each instance represents a respondent's expressions of high or low perception of a single IT characteristic for a given scenario. In some cases, a respondent mentioned more than one IT characteristic for a given scenario, however, their perception remained constant for a given IT characteristic in a given scenario. Most instances referred to IT characteristics in the access scenarios (56%), followed by the password scenarios (40%) and the email scenario (4%). Expressions of IT characteristics referred to included the non-excludability, limitability and verifiability of IT artifacts, as well as the interconnectedness and anonymity of interaction with IT artifacts.

Table 8 shows the number of expressions of high and low perceptions for each IT characteristic. In order to examine whether perceptions of IT characteristics were related to respondents' understanding of harm in ISS scenarios, we examined whether such expressions led respondents to recognize new parties involved, and new consequences (the PCC class). This analysis was not performed on written responses as in such responses the occurrence of codes did not indicate immediacy between perceptions of IT and recognition of parties, consequences, or actions.

TABLE 8 Instances of expressions of IT characteristics

IT characteristic	Instances of high/low perception
Non-excludability	(high) 2, (low) 4
Limitability	(high) 13, (low) 3
Verifiability	(high) 1, (low) 4
Interconnectedness	(high) 13, (low) 0
Anonymity	(high) 3, (low) 5

4.2.2.1 Non-excludability

Known as the quality of an IT artifact whereby consumption by one party does not remove access of others who wish to use the same artifact (Sinha and Mandel 2008), non-excludability was often expressed by the respondents. Non-excludability was expressed solely in access scenarios regarding sharing access to a development tool with an organizational license or analyzing a dataset on an organizational server. Perceptions of high non-excludability coincided with statements of harmlessness while perceptions of low non-excludability in all cases led to recognition of new parties, and new consequences.

(High) An example of high non-excludability perceived by a respondent occurred with respect to a scenario of sharing access to a development tool. In this case, the respondent expressed their understanding of electronic resources as "unlimited" and argued that such a quality means their decision to share access would not carry "real-life" consequences. This example represents high

non-excludability as the respondent assumed sharing the access with another user would not remove access from other license users.

> *It would be unreasonable to not let her use [the license] only because of, not actual, not real life reasons or consequences, but out of like protocol, rules… If I was him, I probably would know, like, if it used up some bandwidth or some resources because usually (sic) electronical resources don't. They are basically unlimited… If you let her use this license, is it gonna cost one of those license users their bandwidth or something? Is it gonna take something away from them or not? But, I assume that it wouldn't.*

(Low) On the other hand, some respondents perceived the IT artifact as excludable (low non-excludability). For instance, in response to the same scenario, another respondent expressed their understanding of access to the tool as excludable "since the systems won't work" otherwise and it is reserved for specific groups of users. In this instance, the respondent's perception of low non-excludability led them to first-time recognition of other license users as a party in the dilemma as well as the potential delaying or troubling effect of sharing the access to the license for other authorized users.

> *What I understood is that they can't give access to everyone since, like, the system can't work if there are a lot of people using it. And, they also want, like, to give it to those who actually need it and can use it.*

4.2.2.2 Verifiability

This quality emerged during analysis of the data and refers to the possibility of inspecting, and understanding the nature and purpose of an IT artifact such as computer code or data. This quality was solely stressed upon in a scenario about access to organizational server resources. While perception of high verifiability led to statements of harmlessness, perceptions of low verifiability in all interviews led to recognition of new parties, and/or consequences.

(High) For instance, while discussing a scenario about running someone else's computer code and dataset on an organizational server, one respondent referred to the degree of understandability of the code, and implied harmlessness of the situation if the code was "layman" enough, and could be verified.

> *[I]f it's the kind of [code and dataset] that is easily trustable, it looks layman enough, I understand what it's all about, I'll probably just do it.*

(Low) On the contrary, discussing the same scenario, another respondent expressed low perception of verifiability when talking about the dataset and expressed concern that a dataset could be of ambiguous nature and from an unknown source. This expression of concern involved recognition of "scientists" and other organizational users who had not been identified up to that point in the interview.

*You can't have external people running their datasets through your piece of equipment, for scientists in your organization. Because, a dataset is, what the h**l is a dataset? It can be a lot of things, it be, you know, who knows what that is, it could be illegal information from an external source, it could not be, but it could be just nonsense.*

4.2.2.3 Interconnectedness

This quality stresses the networked nature of IT operations and the domino effect that IT could introduce to ISS decisions. Most expressions of interconnectedness took place in the password scenarios where respondents envisaged a network of systems that could be exposed. Respondents only expressed high perceptions of interconnectedness and no expression of low interconnectedness was observed. All expressions of high interconnectedness led to recognition of new parties, and/or consequences. One such case was a respondent who referred to the interconnections between their laptop and other databases and systems. The respondent went on to argue that sharing their laptop's password with another user could by consequence expose all these databases and systems and underscored their responsibility with regard to protection of such systems.

Well, on my laptop there are several, [anonymized] databases and all sorts that have very restricted access. And I use the save-password for many of those. So, if somebody could access my laptop, they could then access those databases and it's my responsibility to make sure that that doesn't happen.

Such concerns were expressed with respect to email security as well. One respondent highlighted the high interconnectedness of their email credentials to other systems due to the Single Sign-On technology and in doing so recognized the institute as a party and the potential exposure of other systems as consequence.

[As] I'm working at the university my passwords and the login information is for many other systems as well, not only email, and if those are distributed or sent back to the file sender, then all the other systems might be in danger as well.

4.2.2.4 Anonymity

Several respondents in different scenarios mentioned the (im)possibility of an ISS decision tracing back to them. Anonymity was expressed in all three scenario types. Those who expressed low perception for anonymity in all cases, except one, went on to identify a party, and/or a consequence they had not considered before. In the one exception, the respondent merely pointed out the legal consequence of running someone else's computer code on an organizational server. On the other hand, expressions of perceptions of high anonymity either coincided with statements of harmlessness or did not lead to recognition of any new parties, or consequences.

(High) For example, in one instance, a respondent characterized the act of sharing their password with another user as anonymous and therefore, a fairly harmless decision.

> *It's a very delicate thing that I would have to share my password, which is uncomfortable. It is specially (sic) uncomfortable because it is possible! No one will notice, and probably, if I fairly trust in this other person that I give the password [to], probably, nothing will go wrong.*

(Low) On the other hand, in response to a scenario about email security, another user perceived low anonymity in opening suspicious attachments and expressed their wish to do "right". This wish to do "right" involved identification of people whose personal information they had access to.

> *I do handle information that involves people… I kind of feel like there's a genuine issue out there [with opening email attachments from unknown sources] and that I can possibly be caught. Not necessarily that it might be about to be happening but I think if, there is an audit, and I get caught then I'm in trouble. So, it's more about covering my tracks. So, I'm worried about me doing things rightly.*

4.2.2.5 Limitability

Limitability was another quality of IT artifact that emerged from the data. It refers to perceptions of respondents regarding the possibility of limiting the extent of access privileges granted to another user for a specific IT artifact. Limitability was expressed in both password as well as access scenarios. This quality was often expressed when respondents tried to compare sharing access to an artifact with sharing password to that artifact. In doing so, multiple respondents stressed the possibility to limit access privileges to another user if instead of password only access was shared: "Sharing the login seems very risky, as he does not know what she will do with the tool. Instead, he could let her use the tool under his supervision".

Limitability was also expressed when respondents stressed the possibility of setting restrictions for different groups of users of an IT artifact. In such cases, respondents stressed that an IT artifact such as a "system" is limitable insofar as no extra privileges are granted to another user with similar access privileges upon sharing the password or access. In one such case, a respondent argued "[i]f it's a colleague that does the similar things as I do, they would have access to the same systems. It wouldn't be an issue".

(High) Perceptions of high limitability in all cases led to statements of harmlessness. An example of high limitability was when a respondent mentioned that allowing someone to use her computer would be less of an issue compared to sharing their password since access would be more limited. In this case, the respondent perceived their computer system as highly limitable as the other user would not be able to access their "files" or "systems". This case did not lead to identification of any parties, or consequences; rather, it implied that

since action would be limited, letting someone use one's computer would be relatively harmless.

> *I mean using my computer wouldn't require as much trust as revealing my password but still it would require some trust at least. And also if I knew that I had closed all my files and systems and information on the computer and it would be like a blank screen, that would lower my threshold of [sharing access for] using my computer.*

(Low) Perceptions of low limitability in one case (out of three) led to recognition of a new consequence. In this case, the respondent argued that they would not share their password with another user unless there was a system that made it possible to limit the access privileges granted using that password. In doing this the respondent underlined that the extent of access privileges granted to another user would not be limitable in the current system. This statement led the respondent to specify a consequence for the decision-maker as sharing one's password would reveal their highly personal way of creating passwords in general.

> *I have my own way how I create the passwords and if I share some examples of them, the whole system the whole formula might be known… if the system will allow us to have a second temporal password and if I really trust the person and really decide to allow the access for a limited period of time then the second password could work but no other way for me. At least I don't see [it].*

In other two cases, respondent's perception of low limitability did not lead to recognition of a new party, or a new consequence. However, in one such case the respondent reiterated a previously mentioned consequence and in doing so, emphasized that the extent of harm would be higher when the IT artifact is not limitable. In this case, the respondent compared the case of sharing their password to a cloud storage which they perceived as relatively highly limitable as opposed to their laptop, which they deemed to have low limitability.

> *[I]t's on the laptop [as opposed to cloud]! … No, no, no. It has to be super extreme [for me to share my password]… the quality of the information is different. So accessing the, my computer, could have more extensive damage in the worst case.*

4.2.2.6 Overview

Analysis of interview responses showed that low or high perceptions of IT characteristics could lead to one's recognition of parties involved and consequences. Expressions of low IT characteristics (LITC), consisting of low anonymity, low limitability, low verifiability, low non-excludability, and high interconnectedness, in almost all cases led to recognition of new parties involved, and/or new consequences for parties involved. On the other hand, utterances of high IT characteristics (HITC), consisting of high anonymity, high limitability, high verifiability and high non-excludability coincided with statements of

harmlessness, or did not lead to recognition of new parties and consequences. Given that moral sensitivity involves recognition of parties involved, consequences for the parties and possible courses of action, these results suggest that perceptions of IT characteristics could be related to one's average PCC score, and, subsequently, their moral sensitivity: the more likely the users are to perceive LITC, the higher their moral sensitivity score.

This relationship was examined by performing a correlation analysis between IT characteristics scores and moral sensitivity scores. To do so, the IT characteristics score for each respondent who mentioned an IT characteristic for a given scenario was calculated according to their expressions of LITC and HITC. Positive values of IT characteristics scores indicated that a respondent mentioned at least one LITC, while negative values indicated that the respondent mentioned at least one HITC. A value of zero indicated that a respondent expressed an equal number of LITC and HITC. Furthermore, we analyzed the correlation between IT characteristics scores and the average PCC scores and the average CAC scores.

Table 9 shows the outcome of the correlation analysis. The correlation between IT characteristics scores and moral sensitivity scores was non-significant, providing no evidence of a relationship between perceptions of IT characteristics and moral sensitivity. However, as the results indicate, the average PCC scores were positively and significantly related to IT characteristics scores (at the $p = 0.1$ level). The more likely the respondents were to express LITC, the more likely they were to recognize parties involved and consequences for those parties. Furthermore, the correlation between IT characteristics scores and the average CAC scores indicates a significant negative relationship. The more likely the respondents were to express LITC, the less likely they were to recognize possible courses of action.

TABLE 9 Correlations for IT characteristics

	Moral sensitivity score	**Average PCC score**	**Average CAC score**
IT characteristics score	(r = -0.039, p = 0.81)	(r = 0.28, p = 0.10)+	(r = -0.34, p = 0.04)*

These results indicate that the absence of a correlation between perceptions of IT characteristics and moral sensitivity scores could be due to respondents' consideration of (or lack thereof) possible courses of action. After further examination and readings of the responses, it appeared that respondents who expressed at least one LITC predominantly made an immediate reject decision in response to a given dilemma (65%) and were rather fixated on that decision. For instance, when responding to a scenario about sharing access to an organizational server, a respondent who perceived datasets to be non-verifiable (low verifiability) started the interview by rejecting the request.

> *I wouldn't feel that much if I'm honest with you. I mean, you can't do it. You just can't do it, so I wouldn't sweat over it too much.*

Later on in the interview, when the interviewer asked how they would resolve the situation, the respondent repeated the same response without considering other possible courses of action.

> *How would I handle it? Just write just explain, I would explain to them. I would think that if they're my good friends and colleagues, they're probably as aware of the guideline as I am. So, I'd make that clear, and if they are my good friend they would understand that I would have to say no.*

This fixation, therefore, seemed to have resulted in lower average CAC score for the participant which would subsequently also lower the moral sensitivity score. Appendix 2 provides further examples of expressions of IT characteristics.

4.2.3 Role of affect

Respondents never expressed any emotions towards parties whose information assets could be at risk such as the institute, other users or personal information owners, in any scenario. However, they commonly expressed empathy, and in some cases anger toward the individual asking for a favor in a given scenario. Expressions of feelings emerged primarily in access scenarios (81%) followed by password (12%) and email scenarios (8%). In only a single case did these expressions lead to recognition of new parties and/or consequences. In addition to their feelings toward the person asking for a favor, some respondents expressed their frustration, and anxiety regarding the dilemma in a given scenario. Feelings of frustration, and anxiety emerged mostly in password scenarios (49%), followed by access (38%) and email scenarios (13%).

4.2.3.1 Empathy

Empathy is known as an affective response congruent with that of another person that comes from understanding the other person's suffering, emotional state or condition (Eisenberg and Miller 1987). Feelings of empathy were expressed when respondents put themselves in the shoes of the person asking for a favor in each scenario. Expressions of empathy emerged primarily in access scenarios (90%). In their expressions, respondents imagined the contextual details of the situation and examined alternative explanations that led a colleague, friend, acquaintance or student to ask for a favor. For instance, while discussing the email scenario one respondent noted that an email sent from a strange email address might not pose an ISS threat and considered the context in which an "unfortunate" student without the privileges of institutional affiliation was looking for an opportunity.

> *I was thinking what if it's not a scam. What if it's just an unfortunate person that needs supervision and who doesn't have an institutional address? That's also possible.*

Another respondent highlighted a context in which a "desperate" colleague who does not have access to an organizational server due to bureaucratic issues could be helped out.

> *[I]f it was only the matter of access then I would probably still say no. But, it might be more, hmmm, it would depend on the context as well, like how desperate that person is for example. Is it really, because it can happen, I guess, in certain situations…. Because, I think that in any university and any company, it can happen that due to some bureaucratic issue you might end up not having access to whatever you need.*

4.2.3.2 Anger

Anger is considered an emotion that may involve feelings such as irritation and annoyance to fury and rage (Lomas 2019). While anger is often viewed in a negative light, it is considered a moral emotion insofar as it is rooted in perceived transgressions and a demand for justice, particularly when the self is involved (Haidt 2003; Hutcherson and Gross 2011; Lomas 2019). Expressing anger towards the person asking for a favor occurred in both password and access scenarios. In these cases, respondents described the request as "selfish" or "inappropriate" and said such requests should not take place to begin with. It was in one such case that a respondent's feeling toward the person asking for a favor led to recognition of new parties and consequences as the respondent explained why they felt the request was inappropriate. However, this pattern did not apply to other respondents who expressed their anger.

> *[I would feel] rather irritated to be honest. I think, I would feel that it's inappropriate to ask for username password and my details…. [the system] will have saved all sorts of passwords for other systems. Definitely student records that are not open for everybody but open for a certain number of people.*

4.2.3.3 Frustration

Frustration could be characterized as an event-triggered emotion for which the cause of a goal-blocking event may be unknown and the circumstances may be beyond one's control (Kuppens and Van Mechelen 2007; Roseman et al. 1990). Frustration is considered central to feeling anger (Kuppens and Van Mechelen 2007).

A few respondents expressed their frustration with the need to comply with ISS rules and requirements. These expressions of frustration seemed to indicate an underlying sense of alienation as respondents seemed to frame the problem as a matter of "us versus them". For instance, one respondent stressed their frustration by questioning the "over-emphasis" on security in an access sharing scenario before concluding that "sometimes it causes more problems to people than benefits". Another respondent showcased similar sentiments towards policies that prohibit sharing access with someone in need of help when they provided a "cynical" interpretation of access limitations, adding "it's important

that not everyone can have access, because it helps to keep up the hierarchies". The sense of alienation due to frustration was visible when a respondent lamented the skeptical perspective associated with email security, stressing how it made them feel as if there is everybody else and "then there's you".

> *[T]aking the very, very skeptical perspective means that you probably have, you probably lose a lot, and it just means that you miss the opportunity to trust somebody you should've trusted and you would've done really great things with. Yeah, so, it sort of makes everybody else them and then there's you, and then there is constantly this not trusting the person on the other side.*

4.2.3.4 Anxiety

Anxiety is a state of mind characterized by the notion of threat, the goal to avoid the threat and the goal to know whether the threat would materialize (Miceli and Castelfranchi 2005). Anxiety is often associated with stress and uncertainty (Miceli and Castelfranchi 2005) and it is regarded as a function of outcome expectancy (Pekrun 2006). Several respondents expressed anxiety regarding the decision in the scenarios when asked about their feelings and described the situation as awkward, stressful, uncertain and uncomfortable. Expressions of anxiety towards the dilemma seemed to be induced by concerns about violation of rules and policies (55%), ISS threats (18%), or consequences of ISS violations (27%).

(Concern for rule/policy violation) Some expressions of anxiety highlighted surface level concerns about policy violation. In such expressions, the respondents stressed the importance of the policy for its own sake. In other words, these responses did not specify an ISS threat, or potential harm associated with an ISS threat. An example of concerns regarding policy violation was a respondent who pointed out that they might be willing to share their password with another trustworthy user to get the job done but they would still feel "uneasy" because it is a violation of the "instructions".

> *Somebody who I trust 100 percent, then, maybe I would share my password. But I wouldn't share it easily. Not at all! And. even if it was somebody who I trusted completely and I gave them my password, I think it would still leave me feeling a bit uneasy like: 'Should I have done that?', 'Why did I do that?', 'Was it wise?', 'Should I change my password now?'... Perhaps the uneasiness comes from me knowing that it's against the instructions. I guess I believe in data security authorities.*

(Concern for ISS threats) Another group of respondents expressed anxiety in relation to the ISS threat involved in a decision. These cases went further than surface level concerns to acknowledge the presence of ISS threats, but stopped short of considering the potential harm of such threats. In one such case, a respondent outlined the threat of an email received from an unknown source and how it could throw them off as it would lead to a missed opportunity to

collaborate and do research, but did not go any further to consider the harm associated with the threat.

> *[T]hings like an email address that looks weird, it's almost like, I'm expecting trouble. So, such a thing would already be such a tick for me that I would not necessarily go on with it… I guess the dilemma would throw me off a little bit because it's legit that you want opportunity and you don't wanna miss an opportunity because you've been over-careful.*

(Concern for ISS consequences) Lastly, some expressions of anxiety drew attention to the potential harm associated with an ISS dilemma, that is, they underlined other parties involved in each scenario and the consequences for them. These deep level responses were the only cases where expressions of feelings led to recognition of other parties and/or consequences (the PCC class). For example, one respondent exhibited distress as a decision to share their credentials with another team member could either lead to undesirable ramifications for their teammates or revealing their research participants' confidential information.

> *I guess [this is about] confidential information regarding data collection from participants for a study … Man, this would be a terrible decision to have to make. You know, because, like, because when you are working in a group, I guess things change a little bit. Because you are not just responsible for your own part but also for the group success or failure in that sense.*

4.2.3.5 Overview

Analysis of the responses revealed a lack of experience of moral emotions such as empathy, anger and guilt toward parties that stand to lose in a given ISS dilemma. Instead, respondents seemed to be emotionally concerned about the person with whom they were in contact and expressed feelings of empathy and anger toward the person asking them for a favor. These results suggest that respondents are only emotionally engaged with those close to them, rather than parties who might be affected by their ISS decisions. This closeness, however, was not a matter of geographical distance, as feelings such as empathy were expressed in the email scenario as well, where a potential student sent an email asking for supervision. Overall, expressions of empathy and anger rarely led to recognition of parties involved or consequences. Furthermore, the correlation analysis did not indicate a notable relationship between expression of feelings toward the person asking for a favor in the scenarios and the moral sensitivity score, the average PCC score, or the average CAC score. The outcome of the correlation analysis is presented in Table 10.

TABLE 10 Correlations for affective responses

	Moral sensitivity score	Average PCC score	Average CAC score
Empathy	(r= -0.05, p = 0.61)	(r = -0.09, p= 0.35)	(r = 0.06, p = 0.56)
Anger	(r= 0.16, p = 0.13)	(r = 0.07 , p = 0.47)	(r = 0.18, p = 0.08)+
Frustration	(r= -0.10, p = 0.34)	(r = -0.17, p = 0.09)+	(r = 0.10, p = 0.32)
Anxiety	(r= -0.09, p = 0.35)	(r = -0.15, p = 0.14)	(r = 0.06, p = 0.56)

In addition to feelings of empathy and anger toward the person asking for a favor, the analysis of the responses showed that in some cases, respondents experienced feelings of frustration toward the dilemma. Expressions of frustration reflected an undesirable sense of alienation from the respondents' point of view. As the correlation analysis (Table 10) shows, there was a negative and significant relationship (at the p = 0.1 level) between the expression of frustration and average PCC score.

In regards to expressions of feelings of anxiety, most of all, respondents seemed to be concerned with ISS violations for the sake of the policies and rules rather than their potential harmful effects. In fact, less than one third of expressions of anxiety appeared to be informed by potential harmful effects of ISS violations (the PCC class). In line with these findings, the outcome of the correlation analysis did not show any notable relationship between expressions of anxiety and moral sensitivity. Appendix 3 provides further examples of expressions of affect.

4.2.4 Elapsed time

Emergence of a recurrent pattern related to mentions of immediate action during content analysis suggested that there might be an element of time involved in moral sensitivity in ISS decisions. This recurrent pattern emerged in first readings of the text data when, in most interviews, after explaining the problem in a given scenario, respondents made an immediate, almost reactionary accept/reject decision, followed by a preferred course of action. These immediate decisions, notably, preceded most mentions of parties involved and consequences in the majority of interviews and in some cases, they were overturned by the end of the interview in favor of another course of action. For instance, one respondent after listening to a scenario about password sharing stressed their unwillingness to share and continued to suggest delivery of the device as their preferred course of action. However, by the end of the interview, the respondent seemed to change this preference and advocated sharing the password with a trustee.

> *Early on into the interview: I would not share the password. It would be better, if the laptop is in the workplace and that someone from there would deliver the laptop to wherever I am.*

Late on into the interview: [S]he could call directly to some person that she trusts and give that information needed to that person who [is] known and can handle the situation and give the data to the people needing it.

The frequency with which this pattern seemed to emerge led to an examination of elapsed time. This examination was, however, only possible in interview responses and in cases where the structure of the interviews remained relatively similar. Since this study was conducted using two slightly different interview structures (low engagement group and high engagement group), elapsed time analysis was performed separately for each group.

As Figure 6 demonstrates, in low engagement interviews, respondents were most likely to mention an immediate action within about 100 seconds of the start of the interview. As the figure shows, this immediate utterance in some cases coincided with an initial understanding of parties involved and consequences. However, this initial understanding seemed to be rather limited, and further recognition of parties involved, and consequences (for oneself, the institute, or third parties) occurred later when a resolution was already offered by the respondent. In particular, recognition of consequences was most likely to take place at about 250 seconds into the interview. As the figure shows, changing the preferred action was most likely to take place at 500, and 800 seconds after recognition of parties and consequences.

Overall, recognition of parties involved and consequences in the low engagement group seemed to follow an upward trend from the time that the interview starts up to about 250 seconds into the interview, at which point such recognition was most likely across all scenarios. However, recognition of legal consequences did not seem to follow this pattern. Understanding of legal consequences seemed to follow a bi-modal distribution where it was most likely after 150 seconds and about 400 seconds into an interview. As Figure 6 shows, recognition of legal consequences seems to drop at 250 seconds when the respondents were most likely to recognize parties involved and consequences. In fact, in regards to the distributions for recognition of parties involved and consequences, the distribution for recognition of legal consequences seems to represent an overlapping distribution with non-coincidental peaks. In other words, at times that respondents paid the most attention to parties and consequences, they were less likely to pay attention to legal consequences.

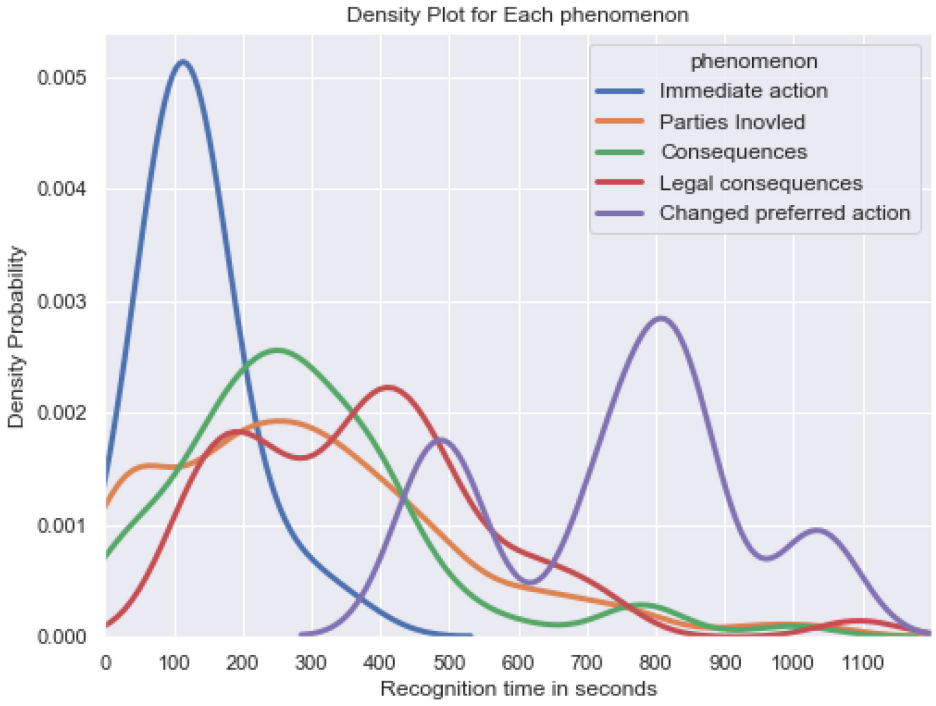

FIGURE 6 Time analysis of low engagement group

As Figure 7 shows, patterns observed in analysis of high engagement interviews are in accordance with those of low engagement interviews, in that respondents uttered a solution quickly after the start of the interview. However, as opposed to low engagement interviews where recognition of parties and consequences were most likely between 200-300 seconds into the interview, in high engagement interviews, such recognition was most likely to occur earlier at about 50-100 seconds. Furthermore, recognition of consequences as well as legal consequences both represented bi-modal distributions. However, in both low and high engagement interviews, the two distributions represented overlapping curves with non-coincidental peaks. In regards to change in the preferred course of action, the pattern seems to be relatively similar in high and low engagement interviews, as the change seems to take place after recognition of parties and the initial peak in recognition of consequences. Overall, while it seems the general trends are relatively similar between high and low engagement interviews, the timing is more compact in high engagement interviews.

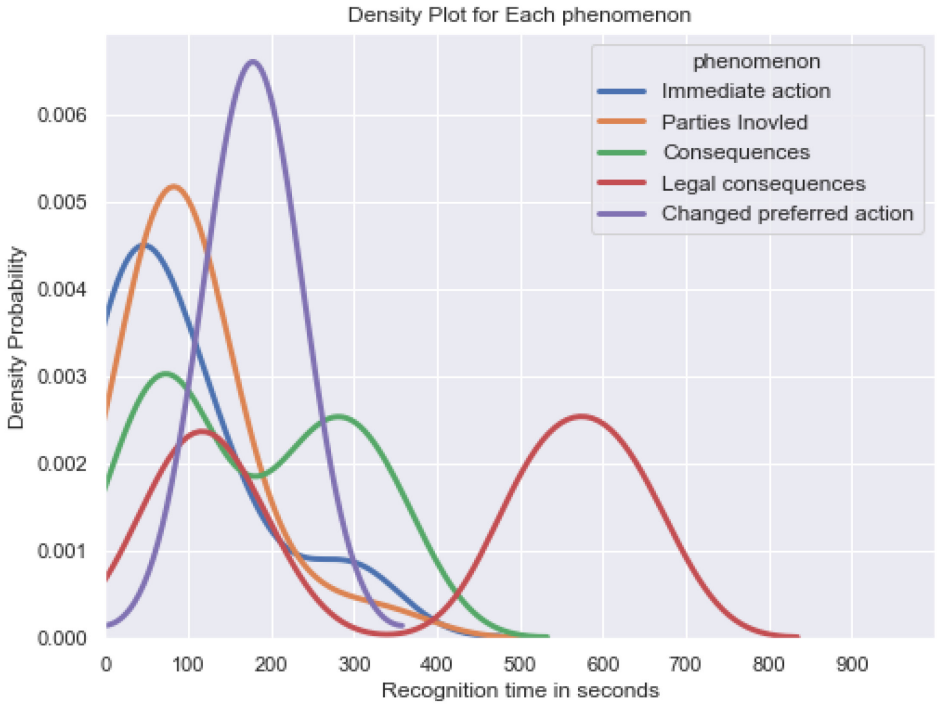

FIGURE 7 Time analysis of high engagement group

In regards to expressions of IT characteristics, as Figure 8 shows, among respondents of the low engagement group who mentioned IT characteristics, expressions of LITC follow an upward trend, coinciding with expressions of parties involved and consequences. This trend continues until 450 seconds into the interviews where LITC expressions reach their peak. On the other hand, the curve for expressions of HICT seem to have a downward trend. As expressions of parties and consequences increase with time, expressions of HITC decrease. Expressions of IT characteristics in the high engagement group (Figure 9) were limited and did not allow for detailed analysis, as only one respondent in this group mentioned any IT characteristics. There were no HITC expressions among this group and only two LITC expressions, which coincided with expressions of consequences.

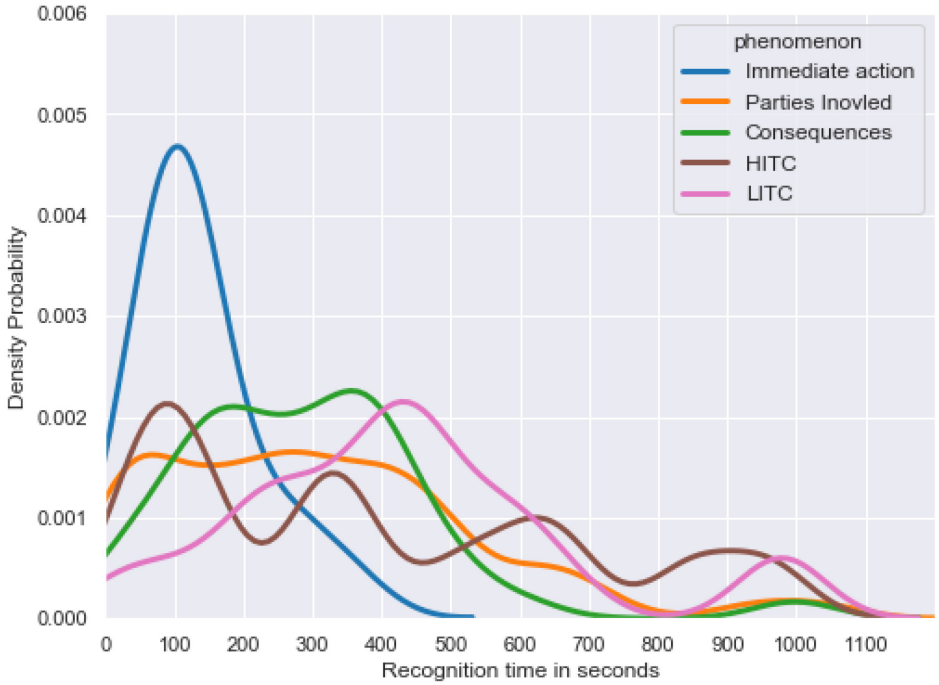

FIGURE 8 Time analysis of IT characteristics in low engagement group

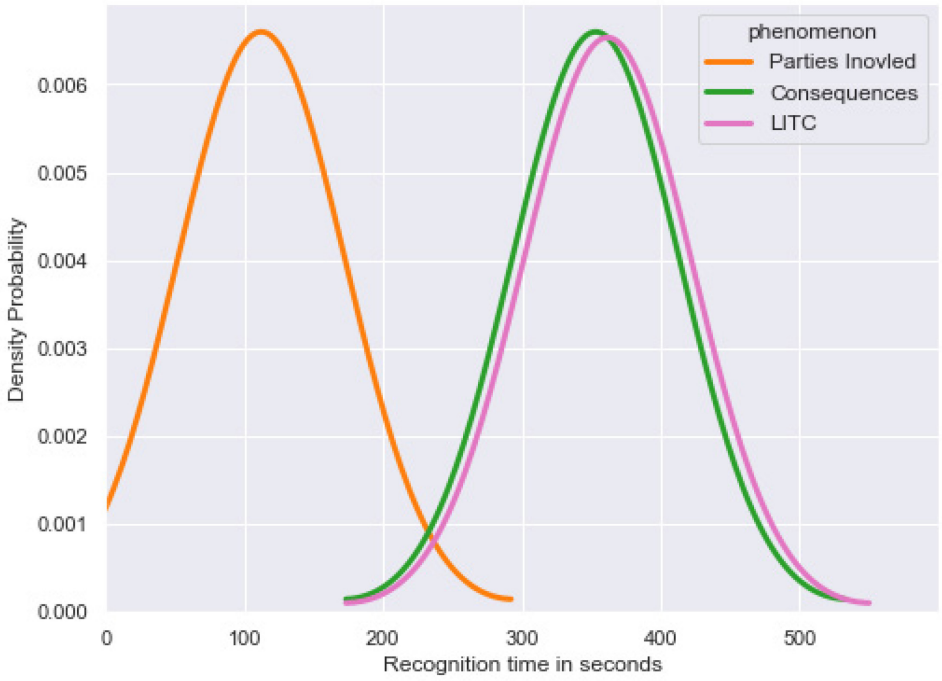

FIGURE 9 Time analysis of IT characteristics in high engagement group

Overall, the observed patterns and relative times observed for recognition of parties and consequences compared to the time of making an immediate decision suggests that moral sensitivity among the respondents took place in two stages. The first stage represents low moral sensitivity, with a limited understanding of parties involved and consequences. This stage seemed to have informed

respondents' immediate decisions and their preferred courses of action. The second stage occurred gradually after that decision. As the time passed and the respondents became further involved in a given scenario, they became more morally sensitive, as reflected in their recognition of parties involved and consequences. This increased sensitivity may have led to the respondents' change of preferred course of action which occurred predominantly after the second stage of recognition of parties and consequences.

Furthermore, the patterns that emerged regarding recognition of legal consequences suggests that attention to legal consequences may distract users from recognizing parties involved and consequences in an ISS decision-making situation. However, recognition may not be mutually exclusive, that is, attention to legal consequences could take place at the same time as recognition of parties involved and consequences.

Regarding IT characteristics, the patterns that emerged suggest that as respondents increasingly expressed LITC, they identified further parties involved and consequences. Meanwhile, as time passed by there were less expressions of HITC. Expressions of HITC seemed to be most likely when the interview started and respondents made an immediate decision.

Lastly, results from the analysis of high engagement interviews seemed to agree with that of low engagement interviews albeit over a shorter time frame. It seems that higher engagement and more direct questions may have acted as cues for respondents to recognize parties and consequences more quickly than when questions did not directly ask for parties and consequences. However, as was reported, this did not seem to affect overall sensitivity of the respondents.

5 DISCUSSION

Findings regarding the state of moral sensitivity in ISS decisions indicated a largely nonconscious and high sensitivity toward moral issues among users. However, elapsed time analysis showed that at the time of making an initial decision, users may not have been as highly morally sensitive than was shown. Particularly, users' understanding of harm - that is, recognition of parties involved and consequences of ISS decisions - seemed to be low when they first made an initial decision. As time passed, however, users became increasingly aware of the harm associated with ISS decisions and recognized further parties and consequences, hence, increased their moral sensitivity. This increased sensitivity after the initial decision could be attributed to reflection and reasoning according to a class of theories known as the dual process theories (Evans and Stanovich 2013; Greene et al. 2001; Kahneman 2011; Sloman 1996).

Dual process theories commonly posit that reasoning and decision-making involve two types of processes: type1 processes are intuitive, fast, and autonomous while type2 processes are reflective, slow and resource demanding (Evans and Stanovich 2013; Kahneman 2011). Dual processing has been shown to be relevant to individuals' moral considerations, in particular, moral judgments (Greene et al. 2001; Paxton et al. 2012). According to the dual process theory of moral judgments (Greene 2009; Greene et al. 2001, 2004), automatic and intuitive moral judgements are largely informed by affective responses and deontological judgments (judgments based on the nature of the act), while controlled and thoughtful judgments are commonly informed by cognitive and utilitarian judgments (judgments based on the cost-benefit evaluations of the outcome of the act).

In ISS research, scholars have suggested that users' ISS decisions could be subject to dual processing (Chu et al. 2015; Dennis and Minas 2018), with Dennis and Minas (2018) suggesting that ISS decisions are on autopilot, that is, made largely based on type1 processing. From this viewpoint, respondents' immediate initial decisions in this study could be viewed as type1 decisions made intuitively with little reflection. Increased sensitivity after the decision, on the other hand, signals type2 processing, through which users engaged in reflection and

reasoning. Users' engagement in type2 processing in this study could be due to the research instructions such as questions asked and the time available to the respondents, both of which have been shown to impact the extent of engagement in type2 processing (Pennycook et al. 2015). Findings of this study, therefore, seem to indicate that not only moral judgments could be subject to type1 and type2 processing (Greene et al. 2001; Paxton et al. 2012), but, at least as ISS decisions are concerned, also moral sensitivity. If ISS decisions are immediate, and instantaneous, users may not be as highly morally sensitive as when they can bide their time and reflect on their decisions. On that note, whether users' ISS decisions are morally informed or not may rely on availability of time and other social cues that trigger type2 processing.

Additionally, findings of this study highlighted the role of perceptions of IT characteristics in moral sensitivity. In particular, the findings showed that expressions of LITC perceptions (low anonymity, low verifiability, low limitability, low non-excludability and high interconnectedness) could lead to identification of parties involved and consequences (higher average PCC score), while expressions of HITC perceptions (high anonymity, high verifiability, high limitability, high non-excludability and low interconnectedness) could lead to statements of harmlessness or lack of recognition of parties and consequences (lower average PCC score). However, elapsed time analysis of expressions of IT characteristics showed that expressions of LITC mostly occurred after the initial immediate decision and increased as users identified further parties and consequences. Meanwhile, expressions of HITC were highest at about the same time when users made their initial immediate decisions. These trends suggest that perceptions of LITC may be mostly reflective and depend on type2 processing while perceptions of HITC may be mostly intuitive and rely on type1 processing. Therefore, in quick and instantaneous ISS decisions, perceptions of LITC may be absent, ineffectual and they might not inform users' understanding of the potential harm in ISS decisions. In such situations, perceptions of HITC could lead users to think of ISS violations as harmless.

The findings also showed a negative and significant relationship between one's perception of LITC or HITC for a given scenario and their average score for recognition of possible courses of action. As reported, further examination of these results showed that this negative relationship could be due to the relative fixation of some respondents with their initially stated immediate decisions. Specifically, respondents who expressed their perceptions of LITC seemed more likely to be fixated on rejecting the favor asked in a given scenario to the extent that they did not entertain the idea of looking for other possible courses of action. Those who expressed their perceptions of HITC, on the other hand, were more open to the idea of resolving the situation, thus, examined other possible courses of action. These observations could indicate that respondents' type2 processing may have been biased by their type1 decisions, that is, their immediate initial decisions, when they considered other possible courses of action may have biased their reflection and reasoning about a given scenario. Indeed, despite on-going debates regarding the interaction between type1 and type2 processing, previous

literature on dual processing such as proponents of parallel processing theories (Sloman 1996) as well as non-parallel processing theories (Evans and Stanovich 2013) have acknowledged that type2 processes could be biased by the outcome of the type1 processes (Pennycook et al. 2015).

Examination of users' affective experiences in this study indicated their lack of experience of moral emotions such as empathy or guilt toward those who stand to lose in ISS scenarios. These findings suggested that no affective processing took place when users considered ISS scenarios. One reason for this lack of affective processing among the respondents may have been perceptions of far distance and distance that is often associated with IT interactions (Dorantes et al. 2006; Friedman 1997). Further analysis showed that affective processing in ISS decisions took place after all, but it was focused on those who were directly in contact with the users. The findings showed that users experienced feelings of empathy or anger toward the person asking for a favor in a given scenario. Interestingly, these expressions of emotions were despite far geographical distance between the person asking for a favor and the decision-maker. For instance, users expressed their feelings of empathy toward a student who sent an email, another researcher whom they met in person, as well as a colleague with whom they had a phone call (albeit with less frequency for the email sender). This discrepancy in experience of affect suggested that far distance was not merely a matter of geographical distance. Instead, it could be related to perceptions of psychological distance and construal levels (Trope and Liberman 2010).

Psychological distance according to construal level theory represents ones' perception of an event or object as close or removed from the self, here and now in terms of (1) time, (2) space, (3) social relationships, and (4) hypotheticality (Trope and Liberman 2010). Perceptions of psychological distance influence formation of mental images or abstractions known as construals which allow individuals to understand, evaluate, speculate and imagine objects or events that cannot be experienced here and now (Trope and Liberman 2010). The farther the perception of psychological distance, the more abstract the construals. The higher level the construals, the more decontextualized and general the information that the individual will consider in understanding an event or object as opposed to contextualized, detailed and concrete (Trope and Liberman 2010). Construal levels have been shown to be related to affective processing and experience of feelings (Han et al. 2014; Schwartz et al. 2018) and recent ISS research has outlined the potential link between construal levels and ISS appraisals (Orazi et al. 2019).

Indeed, in this study, as reported in the findings, the respondents tended to contextualize the situation of the person asking for a favor in their expressions of feelings and tried to imagine alternative explanations that led the person to ask for the favor. This tendency, however, was not on display when users discussed parties involved in the ISS decisions. Given this tendency, and the characterization of construal levels, it is possible that users' feelings of empathy and anger toward the person asking for a favor as opposed to lack of experience of such feelings for those parties who stand to lose in ISS decisions might be due

to perceived psychological distance between the decision-maker and parties involved in the scenarios.

Given that the interaction with the person asking for a favor in most scenarios was immediate (temporal distance), was with one of the peers of the decision-maker (social distance), was very likely (hypothetical distance) and was taking place near the users (spatial distance), it was likely that users perceived low psychological distance with this person. Even in the email scenario where a student contacted a researcher via email, psychological distance might have been perceived to be low as findings regarding computer-mediated communication such as email interaction suggests that communication via IT could reduce perceived psychological distance between remote users (Oh et al. 2008). Such low perceptions of psychological distance, in turn, may have led to lower level construals which provided the respondents with detailed, concrete and contextualized information about the person asking for a favor and therefore allowed affective processing of their situation. In comparison, interaction with parties that might be affected by ISS consequences may have been considered far in terms of time, space, hypotheticality and social relations which may have led to higher level construals and therefore insufficient details to allow affective processing.

Findings of this study also revealed feelings of frustration among some respondents toward the dilemma in the scenario. These feelings seemed to reflect an underlying sense of alienation and isolation marked by framing of responses as "us versus them". Previous research has suggested that such a sense of isolation among users could lead to experience of deindividuation (Loch and Conger 1996). However, further examination of the responses did not indicate any sign of lowered self-awareness and control, or preference for group norms which could mark the experience of deindividuation (Diener 1976, 1979). Therefore, users' sense of alienation in this study may have been unrelated to experience of deindividuation. However, the findings showed a negative correlation between expressions of frustration and users' understanding of harm in ISS decisions. Given that expressions of frustration reflected an underlying sense of alienation among the respondents, this negative relationship could signal that either a lack of understanding of the harm in ISS scenarios led to a sense of alienation and subsequently expression of frustration or that it was the sense of alienation manifesting through feelings of frustration that led to a lack of understanding of the harm in ISS scenarios. Unfortunately, further readings of the responses and examination of the data did not indicate the direction of this relationship.

Lastly, in this study, users expressed anxiety when discussing their feelings. This finding is in line with previous studies conducted on security-related stress that emphasize the stress experienced by users in ISS compliance situations (D'Arcy et al. 2014; D'Arcy and Teh 2019). However, whereas the literature on security-related stress (D'Arcy et al. 2014; D'Arcy and Teh 2019) consider overload, complexity and uncertainty of ISS requirements as elements that induce stress, in this study, users' experience of uncertainty, stress and

awkwardness signaled experience of feelings of anxiety as an affective response that revolves around the notion of an ISS threat.

Anxiety has been characterized as an emotional state of mind that has to do with uncertainties regarding potential threats and that of goals being thwarted (Miceli and Castelfranchi 2005). Some scholars have suggested that anxiety is an achievement emotion that is a function of uncertainty about the outcome of an activity (Pekrun 2006). Experience of anxiety in an IT use context has been reported and studied with respect to computer-related anxiety (Thatcher and Perrewé 2002), technology-related anxiety (Ormond and Warkentin 2015) and internet-related anxiety (Moody et al. 2017). In such studies, anxiety is often characterized as a matter of concern for losing important data or making mistakes (Thatcher and Perrewé 2002), or a general uneasiness toward the online environment (Moody et al. 2017).

From this standpoint, findings of this study regarding experience of anxiety extends previous research and suggests that in ISS decisions, users may experience ISS anxiety. ISS anxiety is an emotional state that revolves around the notion of an ISS threat and the potential outcome of such a threat. According to the findings, this threat may be experienced at three different levels. At the surface level, an anxious user may be concerned about an ISS violation for the sake of ISS policies and rules. At the mid-level, an anxious user may be concerned about the presence of ISS threats. at the deep level, the anxiety might be due to concerns for the potential harm caused by ISS violations. Nevertheless, findings of this study showed that experiences of anxiety were unrelated to moral sensitivity. This was expected given the rarity of deep level concerns as the only source of anxiety where users considered the parties involved and consequences.

5.1 Research contributions

The findings of this study contribute to the current state of research on morally relevant ISS decisions by revealing the potential dual processing of moral sensitivity. Previous research has shown the value of incorporating moral considerations in models of ISS decision-making (Cram et al. 2019). Specifically, previous studies have shown that moral considerations could play an inhibitory role and prevent users from engaging in ISS violations (D'Arcy et al. 2009; D'Arcy and Devaraj 2012; D'Arcy and Lowry 2019; Vance and Siponen 2012; Xu and Hu 2018). Furthermore, studies on the use of neutralization techniques and moral disengagement mechanisms in ISS decisions have suggested that users may take a 'moral holiday' in ISS decisions by neutralizing insecure decisions or morally disengaging from ISS decisions (D'Arcy et al. 2014; Silic et al. 2017; Siponen and Vance 2010). This study, however, suggests that if users make ISS decisions instantaneously and on auto-pilot (Dennis and Minas 2018), they may not be morally sensitive enough for their decisions to be morally informed. Moral inhibition, neutralization or moral disengagement may not occur if users do not

perceive the situation as morally relevant and do not engage their moral schemata.

Another contribution of this study concerns the role of IT characteristics. Our results unearthed several IT characteristics, perceptions of which could inform users' understanding of harm in ISS decisions. Moral concerns in ISS situations take place in the context of IT use. In this study, we conceptualized that IT artifact qualities, qualities of interaction with IT artifacts, and IT-induced experiences could be influential in moral considerations of users, and should be accounted for in examination of such considerations. Such an examination has been largely missing in ISS research despite calls for attention to the role of IT (Lowry et al. 2017; Orlikowski and Iacono 2001). The empirical findings showed that high or low perceptions of specific IT characteristics could indeed lead to recognition of parties involved and consequences and could, therefore, inform users of the potential harmful implications of ISS decisions.

Additionally, IT characteristics were found to be relevant to the affective responses of users in morally relevant ISS decisions. Despite recent interest in affective models in ISS research (D'Arcy and Lowry 2019; Ormond et al. 2019), and despite the important role granted to affective processing in moral psychology (Blasi 1999; Greene 2009; Haidt 2003; Hofmann and Baumert 2010; Moll and de Oliveira-Souza 2007; Tangney et al. 2007), affective processing of moral considerations has not been a subject of much scholarly attention in morally relevant ISS decisions. Findings of this study indicated not only that perceptions of IT characteristics are intertwined with understanding of harm in ISS decisions, but that perceptions of distance as a quality of interaction with IT artifacts might be conditioning users' affective processing. This study showed that perceptions of far psychological distance may suppress feelings of moral emotions such as empathy toward potential victims of ISS decisions. This study, therefore, provides valuable insights into users' understanding of IT characteristics as far as moral considerations are concerned and therefore allow contextualization and development of context-specific theories (Hong et al. 2014) regarding such considerations in ISS research.

Lastly, this study contributes to research on users' experience of technology-related anxiety and security-related stress (D'Arcy et al. 2014; D'Arcy and Teh 2019; Ormond and Warkentin 2015; Thatcher and Perrewé 2002). Previous research has suggested that users may experience security-related stress when they are expected to comply with ISS requirements , and that coping with this stress by means of moral disengagement could lead to ISS policy violation (D'Arcy et al. 2014; D'Arcy and Teh 2019). In line with prior research, this study showed that users may experience anxiety in terms of feeling awkward, stressful, uncertain or uncomfortable in ISS decisions. In doing so, this study takes a step further and characterizes users' experience of anxiety as a matter of concerns regarding violation of ISS rules and policies, presence of ISS threats, and the potential harm in ISS threats. As such, security-related stress (D'Arcy et al. 2014; D'Arcy and Teh 2019) in ISS research seems to address users' experience of anxiety in ISS dilemmas at the surface level insofar as it deals with users stress

and uncertainty regarding compliance with a given set of requirements, and the potential threat of violating the policies and rules. In this respect, therefore, this study extends the literature on security-related stress and suggests that ISS anxiety as an experience could be more suited for capturing users' experience of negative emotions in ISS decisions.

The characterization of ISS anxiety in this study provides a nuanced understanding of anxiety in an ISS context. This is of value, particularly given that characterization of technology-related anxiety in the extant literature has been rather high -level. Examination of technology-related anxiety as a matter of fear of data loss and making mistakes - while suitable for examination of computer technology adoption and use (Thatcher and Perrewé 2002) does not provide a detailed enough frame of reference for examining how ISS specifically induces anxiety among users. The three levels of concerns regarding ISS threats, however, provide such a frame of reference and point toward an ISS specific understanding of anxiety.

5.2 Practical contributions

Moral interventions have long been suggested as a solution to moral concerns in ISS (Banerjee et al. 1998; Cook 1986; Li et al. 2014; Loch and Conger 1996; Moores and Chang 2006; Siponen 2001; Stahl 2012; Vance et al. 2019). This study contributes to the development of moral interventions by outlining the process of moral sensitivity. Understanding the underlying processes of moral decision-making is necessary if we are to develop sensible solutions to moral concerns in ISS (Gattiker and Kelley 1999; Lowry et al. 2014) and moral sensitivity is one such process (Rest 1986). In this regard, given users' rudimentary understanding of parties involved and consequences while they make fast and intuitive ISS decisions, one solution to moral concerns in ISS is to aim at triggering type2 processing. For instance, users could be instructed to take their time and evaluate the situation when they face an ISS decision. To do so, moral interventions could educate users and provide them with a template or clearly defined procedures to examine the parties involved, consequences and possible courses of action in a given situation.

Furthermore, given the potential influence of one's perceptions of IT characteristics on their ability to identify parties involved and consequences, moral interventions could be developed that challenge strongly held perceptions of IT characteristics. For instance, a moral intervention could target perceptions of high verifiability of computer code and underline the complexities of computer code and possibilities that running someone else's computer code could bring about an ISS breach.

Lastly, in this study, there was evidence that perceptions of far psychological distance could have suppressed users' feelings of moral emotions such as empathy for potential victims of ISS violations. Therefore, one solution to address moral concerns in ISS is to design and develop moral interventions

that challenge perceptions of far psychological distance and provide detailed contextual information regarding the potential victims and consequences of ISS violations for them. To do this, one could develop context-specific personas of potential victims according to the organizational setting where the moral intervention is to be delivered and the information asset that is to be protected. Given such personas, perceptions of psychological distance could be reduced across its constituent elements of temporal, spatial, hypothetical, and social distance. For instance, users could be shown how quickly and likely an ISS breach could inflict harm on a given persona.

5.3 Future research and limitations

Given the findings of this study and the relevance of experience of emotions, IT characteristics and dual processing to moral sensitivity of users, we propose a number of research directions that could address potential areas of interest. In these recommendations, we suggest future research to further investigate the confluence of IT and morality. We highlight the limitations of this study and the opportunity for future research in that regard.

5.3.1 Moral considerations and dual processing

According to the findings, moral sensitivity might be subject to dual processing and users may be more morally sensitive in type2 processing, which is more reflective and slower than type1 processing. However, the results did not indicate what could trigger type2 processing in ISS decisions. In this study, we suspect that the interview questions as well as the time available to respondents may have triggered type2 processing as previous research has shown that both these factors could be in contention. Future research could therefore examine this matter, as factors that trigger type2 processing could be cultivated to enable users to consider the potential harm involved in ISS decisions. In studying the potential role of time in triggering type2 processing, for instance, one approach could be to design an experiment with different groups of respondents who have different time limits to discuss a given ISS scenario.

If time is a trigger for type2 processing, future studies that examine moral considerations could distinguish between instantaneous ISS decisions and prolonged decisions in their research designs. Furthermore, given that users may not be sensitive when making quick and instantaneous decisions, future research that aims to study moral considerations such as moral beliefs, moral obligations and personal norms - or research that examines morally relevant behavior such as use of neutralization techniques - should clearly specify the moral problem to the users (Barlow et al. 2013; Haag et al. 2015; Siponen and Vance 2010). Otherwise, users may misunderstand or misinterpret the moral relevance of a study which would throw a study's findings into doubt. For instance, in a study of neutralization techniques, respondents may not understand the activity under

study as a moral wrongdoing in order to deploy techniques of neutralization to begin with (Sykes and Matza 1957).

Additionally, future research could compare moral sensitivity across different respondent groups. In this study, three respondent groups were examined, namely, students, researchers and administration staff. However, one of the limitations of this study was that the number of respondents in each of these groups was not high enough to allow comparison between them. In particular, there were only a few responses to the scenarios from the administration staff. Since these groups represent different levels of professional relationships with an organization, future research could undertake such a comparison and examine whether groups of users such as administration staff reflect different understanding of harm and moral sensitivity compared to other groups such as subcontractors or students. Such a study could show whether different groups of users would require different moral interventions or whether one size fits all.

5.3.2 IT characteristics and emotions

In this dissertation, no questions were posed to the respondents regarding their perceptions of IT characteristics. This was a design decision made to allow elicitation and analysis of IT characteristics based on respondents' interpretation of the scenarios. However, this decision came with the downside of leaving the perceptions of respondents who did mention any IT characteristics in their responses unknown. Therefore, in order to further examine the potential effect of IT characteristics on awareness of harm or moral considerations, future research could directly inquire users to rate their perceptions of specific IT characteristics, and examine how high and low perceptions could impact moral considerations.

Similarly, in this study, only one question was posed to the respondents asking for their experience of affect. Specifically, respondents were asked how they felt after listening to the scenarios and explaining the problem in the scenarios. While this method allowed examination of the potential emotional experiences of the respondents in their interpretation of the situation without any previous priming, it did not allow for examination of specific moral emotions. Therefore, future research could pose more specific questions regarding users' experience of moral emotions such as empathy, guilt and anger in order to study their impact on awareness of harm or moral considerations.

On that note, IT characteristics and emotions could be embedded in the scenarios in a factorial design where different variants of the scenarios are developed with high, or low expression of emotions or IT characteristics. Such a factorial design could allow examination of moral considerations under different conditions such as conditions of high emotional load. The relevance of such a method was visible in some of the responses where the respondent outlined a set of conditions for their decisions. For example, one of the respondents who was very strict about not sharing their password outlined how they might do otherwise depending on how the other person would plead with them.

[I]t would really depend on how the other person appeals to me as well. If the other person calls me again and [says] 'Hey man, really, this would change my life!' maybe I would come to some sort of agreement that I will share the username or password.

Furthermore, another limitation of this dissertation is the lack of distinction between dispositional and situational experience of emotions. While situational emotions refer to one's immediate affective responses to a given situation, dispositional emotions correspond to one's tendency to experience specific emotions across different situations (Eisenberg et al. 1994; Larsen and Ketelaar 1991). Since this study only presented one question regarding users' experience of affect, it was not possible to distinguish whether affective arousal was rooted in individual user's dispositional tendencies or their situational examination of the situation (Eisenberg et al. 1994). However, given that in the scenarios users' were given contextual information regarding a specific situation, it is likely that affective arousal was driven by the specific situation in the scenario. Nevertheless, future research may investigate this matter further to see whether those who are more likely to experience dispositional affective arousal - such as those who are more likely to experience dispositional empathy - are more likely to feel for potential victims of ISS violations.

5.3.3 Frustration and experience of alienation

In several instances, respondents expressed frustration toward ISS decisions. Expressions of frustration in such cases reflected a sense of alienation which seemed to be negatively related to respondents' understanding of harm. In this study, however, it was not possible to determine the nature of this relationship: whether lack of understanding of potential harm in ISS scenarios led to expressions of frustration and experience of alienation or vice versa. If users' experience of frustration is considered as instances of disgruntlement, this marks a potential valuable opportunity to examine disgruntlement in ISS. As prior research has indicated, disgruntlement among organizational users as a motivation for IT misuse is a valuable yet relatively unexplored area (Holton 2009; Willison and Warkentin 2013). If users' frustrations and experience of alienation are due to their lack of understanding of potential harm, moral interventions that communicate such harm can prevent user frustrations and prevent disgruntlement.

5.3.4 Desirable versus undesirable behavior

Cram et al. (2019) have previously reported on the significance of moral considerations in ISS decisions, albeit they argued that moral considerations seem to be better explaining avoidance of undesirable ISS behaviors such as ISS policy violation, rather than desirable behaviors such as ISS policy compliance. Based on their meta-analysis review of 95 empirical studies on ISS policy compliance - which showed in particular that moral considerations were more

relevant to undesirable behaviors than desirable behaviors - Cram et al. (2019) posited that undesirable ISS behaviors are conceptually dissimilar to desirable ISS behaviors. On the back of this, Cram et al. (2019) suggested that future research focus on user behavior by distinguishing between desirable and undesirable ISS behaviors. In terms of moral considerations, that could mean that such considerations and the role of IT characteristics thereof could differ based on whether the independent variable is desirable or undesirable ISS behavior. However, we believe such an approach in studying moral considerations could be misleading since rather than representing any conceptual difference, the difference observed in the meta-analysis could be due to a framing effect.

Framing effect was introduced by Tversky and Kahneman (1981) and refers to a change in (risk) decisions when decision-makers are faced with identical choices that are described differently, for instance using positive frame versus negative frame. Moral decisions such as famous trolley dilemmas are known to be subject to framing effect (Cao et al. 2017; Gonzalez et al. 2005). For instance, in a moral dilemma, negative framing such as "[if you decide to pull] the lever, one worker will be killed; otherwise, five workers will be killed on the main tracks" significantly affects one's moral considerations whereas an equivalent statement framed positively such as "[if you decide to pull] the lever, five workers will be saved on the main tracks; otherwise, one worker will be saved" would not (Petrinovich and O'Neill 1996).

Given that ISS policy violation and compliance could be interpreted respectively as negative and positive framing, there is a possibility that a framing effect rather than a conceptual difference between desirable and undesirable ISS behavior could explain the findings reported by Cram et al. (2019). Therefore, we suggest that future research investigate the role of IT in moral considerations of both desirable and undesirable ISS behavior with due attention given to any potential framing effect. Particularly, experiments with positively and negatively framed messages in awareness campaigns and moral interventions could be of interest as they could reveal evidence for delivering effective campaigns.

6 CONCLUSIONS

This dissertation conceptualized the role of IT characteristics in moral considerations of users. Specifically, IT artifact qualities, IT interaction qualities, and IT-induced experiences were outlined as potential IT-related characteristics that could have an impact on the moral considerations of users. When examined with respect to moral sensitivity - a moral consideration whereby users realize the moral relevance of ISS decision-making situations - high or low perceptions of IT characteristics could lead to recognition - or lack thereof - of parties involved and consequences. The IT characteristics uncovered in this dissertation concerned the non-excludability, limitability, and verifiability as IT artifact qualities, as well as anonymity, and interconnectedness as IT interaction qualities.

Furthermore, in this dissertation, the distance between two parties in an ISS decision-making situation as an IT interaction quality was further contextualized as psychological distance. In this respect, perceptions of far psychological distance may lead to emotional disengagement of users from potential victims of ISS decisions. Regarding IT-induced experiences, a sense of alienation was observed when users expressed their frustration with ISS requirements, however, no evidence was found that this alienation was reflecting experience of deindividuation. On the other hand, this dissertation found that previous research on security-related stress as an IT-induced experience may be extended to examine users' experience of uncertainty, stress and awkwardness as ISS anxiety.

Lastly, findings regarding the unfolding of moral sensitivity process suggest that moral sensitivity might be subject to dual processing. In quick, intuitive and autonomous type 1 processing, users could end up with decisions that are not morally informed. Meanwhile the slower, more reflective and more resource demanding type 2 processing, may be more informed by the potential harm in ISS decisions and more morally informed. Overall, these findings could contribute to further disentanglement of the relationship between IT and morality in ISS decisions and to the design and development of effective moral interventions.

REFERENCES

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., and Aleassa, H. 2013. "Information Security Policy Compliance: An Empirical Study of Ethical Ideology," *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 3018–3027.

Baab, D. A., and Bebeau, M. J. 1990. "The Effect of Instruction on Ethical Sensitivity," *Journal of Dental Education* (54:1), p. 44.

Bandura, A. 1991. "Social Cognitive Theory of Moral Thought and Action," in *Handbook of Moral Behavior and Development* (Volume 1:, Vol. 1), W. C. Kurtines and J. L. Gewirtz (eds.), Hillsdale, NJ: Lawrence Erlbaum Associates, pp. 45–103.

Banerjee, D., Cronan, T. P., and Jones, T. W. 1998. "Modeling IT Ethics: A Study in Situational Ethics," *MIS Quarterly* (22:1), pp. 31–60.

Bansal, G., Green, W., Hodorff, K., and Marshall, K. 2016. "Moral Beliefs and Organizational Information Security Policy Compliance : The Role of Gender," *Proceedings of the Eleventh Midwest United States Association for Information Systems*.

Barlow, J. B., Warkentin, M., Ormond, D., and Dennis, A. R. 2013. "Don't Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation," *Computers and Security* (39:PART B), pp. 145–159.

Bauer, S., and Bernroider, E. W. N. 2017. "From Information Security Awareness to Reasoned Compliant Action : Analyzing Information Security Policy Compliance in a Large Banking Organization," *The Data Base for Advances in Information Systems* (48:3), pp. 44–68.

Bebeau, M. J., Rest, J. R., and Yamoor, C. M. 1985. "Measuring Dental Students' Ethical Sensitivity," *Journal of Dental Education* (49:4), pp. 225–235.

Beck, L., and Ajzen, I. 1991. "Predicting Dishonest Actions Using the Theory of Planned Behavior," *Journal of Research in Personality* (25:3), pp. 285–301.

Benbasat, I., and Zmud, R. W. 2003. "The Identity Crisis within the Is Discipline: Defining and Communicating the Discipline's Core Properties," *MIS Quarterly* (27:2), pp. 183–194.

Blasi, A. 1999. "Emotions and Moral Motivation," *Journal for the Theory of Social Behaviour* (29:1), pp. 1–19.

Cao, F., Zhang, J., Song, L., Wang, S., Miao, D., and Peng, J. 2017. "Framing Effect in the Trolley Problem and Footbridge Dilemma: Number of Saved Lives Matters," *Psychological Reports* (120:1), pp. 88–101.

Chang, C. L.-. 2011. "The Significance of a Suitable Information Ethical Code," *Journal of Information Ethics* (2:1), pp. 54–85.

Chatterjee, S., Sarker, S., and Valacich, J. S. 2015. "The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use," *Journal of Management Information Systems* (31:4), pp. 49–87.

Chatterjee, S., Valacich, J. S., and Sarker, S. 2011. "Unethical Use of Information Technology: A Two-Country Study," *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 3071–3080.

Chiou, J. S., Huang, C. Y., and Lee, H. H. 2005. "The Antecedents of Music Piracy Attitudes and Intentions," *Journal of Business Ethics* (57:2), pp. 161–174.

Chu, A. M. Y., Chau, P. Y. K., and So, M. K. P. 2015. "Explaining the Misuse of Information Systems Resources in the Workplace: A Dual-Process Approach," *Journal of Business Ethics* (131:1), pp. 209–225.

Clarkeburn, H. 2002. "A Test for Ethical Sensitivity in Science," *Journal of Moral Education* (4), pp. 439–454.

Colby, A., Kohlberg, L., Gibbs, J., Lieberman, M., Fischer, K., and Saltzstein, H. D. 1983. "A Longitudinal Study of Moral Judgment," *Monographs of the Society for Research in Child Development* (48:1), pp. 1–124.

Cook, J. M. 1986. "What C.S. Graduates Don't Learn About Security Concepts and Ethical Standards Or-Every Company Has Its Share of Damn Fools. Now Every Damn Fool Has Access to a Computer," in *ACM SiGCSE Bulletin*, pp. 89–96.

Cram, W. A., D'Arcy, J., and Proudfoot, J. G. 2019. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance," *MIS Quarterly: Management Information Systems* (43:2), pp. 525–554.

Cronan, T. P., Leonard, L. N. K., and Kreie, J. 2005. "An Empirical Validation of Perceived Importance and Behavior Intention in IT Ethics," *Journal of Business Ethics* (56:3), pp. 231–238.

Culnan, M. J., and Williams, C. C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches," *MIS Quarterly* (33:4), pp. 673–687.

D'Arcy, J., and Devaraj, S. 2012. "Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model," *Decision Sciences* (43:6), pp. 1091–1124.

D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285–318.

D'Arcy, J., Herath, T., Yim, M.-S., Nam, K., and Rao, H. R. 2018. "Employee Moral Disengagement in Response to Stressful Information Security Requirements: A Methodological Replication of a Coping-Based Model," *AIS Transactions on Replication Research* (4:June), pp. 1–18.

D'Arcy, J., and Hovav, A. 2009. "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures," *Journal of Business Ethics* (89:SUPPL. 1), pp. 59–71.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79–98.

D'Arcy, J., and Lowry, P. B. 2019. "Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study," *Information Systems Journal* (29:1), pp. 43–69.

D'Arcy, J., and Teh, P.-L. 2019. "Predicting Employee Information Security Policy Compliance on a Daily Basis: The Interplay of Security-Related Stress, Emotions, and Neutralization," *Information & Management* (56:7), p. 103151.

Decety, J., Michalska, K. J., and Kinzler, K. D. 2011. "The Developmental Neuroscience of Moral Sensitivity," *Emotion Review* (3:3), pp. 305–307.

Decety, J., Michalska, K. J., and Kinzler, K. D. 2012. "The Contribution of Emotion and Cognition to Moral Sensitivity: A Neurodevelopmental Study," *Cerebral Cortex* (22:1), pp. 209–220.

Deci, E. L., and Ryan, R. M. 1985. "The General Causality Orientations Scale: Self-Determination in Personality.," *Journal of Research in Personality* (19), pp. 109–134.

Dennis, A. R., and Minas, R. K. 2018. "Security on Autopilot: Why Current Security Theories Hijack Our Thinking and Lead Us Astray," *Data Base for Advances in Information Systems* (49:s1), pp. 15–37.

Diener, E. 1976. "Effects of Prior Destructive Behavior, Anonymity, and Group Presence on Deindividuation and Aggression," *Journal of Personality and Social Psychology* (33:5), pp. 497–507.

Diener, E. 1979. "Deindividuation, Self-Awareness, and Disinhibition," *Journal of Personality and Social Psychology* (37:7), pp. 1160–1171.

Dorantes, C. A., Hewitt, B., and Goles, T. 2006. "Ethical Decision-Making in an IT Context: The Roles of Personal Moral Philosophies and Moral Intensity," *Proceedings of the Annual Hawaii International Conference on System Sciences* (8).

Eisenberg, N., Fabes, R. A., Murphy, B., Karbon, M., Maszk, P., Smith, M., O'Boyle, C., and Suh, K. 1994. "The Relations of Emotionality and Regulation to Dispositional and Situational Empathy-Related Responding," *Journal of Personality and Social Psychology* (66:4), pp. 776–797.

Eisenberg, N., and Miller, P. A. 1987. "The Relation of Empathy to Prosocial and Related Behaviors," *Psychological Bulletin* (101:1), pp. 91–119.

Ellis, T., and Griffith, D. 2001. "The Evaluation of IT Ethical Scenarios Using a Multidimensional Scale," *The DATA BASE for Advances in Information Systems* (32:1), pp. 75–85.

Evans, J. S. B. T., and Stanovich, K. E. 2013. "Dual-Process Theories of Higher Cognition: Advancing the Debate," *Perspectives on Psychological Science* (8:3), pp. 223–241.

Forsyth, D. R. 1980. "A Taxonomy of Ethical Ideologies.," *Journal of Personality and Social Psychology*, pp. 175–184.

Friedman, B. 1997. "Social Judgments and Technological Innovation: Adolescents' Understanding of Property, Privacy, and Electronic Information," *Computers in Human Behavior* (13:3), pp. 327–351.

Gattiker, U. E., and Kelley, H. 1999. "Morality and Computers: Attitudes and Differences in Judgments," *Information Systems Research* (10:3), Linthicum: Institute for Operations Research and the Management Sciences, pp. 233–254. (http://search.proquest.com/docview/208161762?accountid=11774).

Goles, T., White, G. B., Beebe, N., Dorantes, C. A., and Hewitt, B. 2006. "Moral Intensity and Ethical Decision-Making: A Contextual Extension," *The DATA BASE for Advances in Information Systems* (37:2&3), pp. 86–95.

Gonzalez, C., Dana, J., Koshino, H., and Just, M. 2005. "The Framing Effect and Risky Decisions: Examining Cognitive Functions with FMRI," *Journal of Economic Psychology* (26:1), pp. 1–20.

Grace, W. 2013. "How Did Ethical Evaluation Work As a Mediator between Moral Intensity and Decision Making?," *International Journal of Business, Humanities and Technology* (3:1), pp. 58–68.

Greene, J. D. 2009. "Dual-Process Morality and the Personal/Impersonal Distinction: A Reply to McGuire, Langdon, Coltheart, and Mackenzie," *Journal of Experimental Social Psychology* (45:3), Elsevier Inc., pp. 581–584.

Greene, J. D., Nystrom, L. E., Engell, A. D., Darley, J. M., and Cohen, J. D. 2004. "The Neural Bases of Cognitive Conflict and Control in Moral Judgment," *Neuron* (44), pp. 389–400.

Greene, J. D., Sommerville, R. B., Nystrom, L. E., Darley, J. M., and Cohen, J. D. 2001. "An FMRI Investigation of Emotional Engagement in Moral Judgment," *Science* (293), pp. 2105–2108.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems* (28:2), pp. 203–236.

Haag, S., Eckhardt, A., and Bozoyan, C. 2015. "Are Shadow System Users the Better IS Users ? – Insights of a Lab Experiment," *2015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015*, pp. 1–20.

Haidt, J. 2003. "THE MORAL EMOTION," in *Handbook of Affective Sciences*, R. J. Davidson, K. R. Scherer, and H. H. Goldsmith (eds.), Oxford: Oxford University Press, pp. 852–870.

Haines, R., and Leonard, L. N. K. 2007. "Situational Influences on Ethical Decision-Making in an IT Context," *Information and Management* (44:3), pp. 313–320.

Han, D., Duhachek, A., and Agrawal, N. 2014. "Emotions Shape Decisions through Construal Level: The Case of Guilt and Shame," *Journal of Consumer Research* (41:4), pp. 1047–1064.

Hansen, J., and Walden, E. 2013. "The Role of Restrictiveness of Use in Determining Ethical and Legal Awareness of Unauthorized File Sharing," *Journal of the Association for Information Systems* (14:9), pp. 521–549. (http://search.proquest.com/docview/1470087231?accountid=11774).

Hardy, S. A. 2006. "Identity, Reasoning, and Emotion: An Empirical Comparison of Three Sources of Moral Motivation," *Motivation and Emotion* (30:3), pp. 205–213.

Hardy, S. A., and Carlo, G. 2005. "Identity as a Source of Moral Motivation," *Human Development* (48:4), pp. 232–256.

Harrington, S. J. 1996. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3), pp. 257–278.
Harrington, S. J. 1997. "A Test of a Person – Issue Contingent Model of Ethical Decision Making in Organizations," *Journal of Business Ethics* (16:4), pp. 363–375.
Harris, A. L., Yates, D., Quaresma, R., and Harris, J. M. 2010. "Information System Ethical Attitudes: A Cultural Comparison of the United States, Spain, and Portugal," *16th Americas Conference on Information Systems 2010, AMCIS 2010* (3), pp. 1886–1895.
Higgins, G. E., and Wilson, A. L. 2006. "Low Self-Control, Moral Beliefs, and Social Learning Theory in University Students' Intentions to Pirate Software," *Security Journal* (19:2), pp. 75–92.
Hinduja, S., and Ingram, J. R. 2008. "Self-Control and Ethical Beliefs on the Social Learning of Intellectual Property Theft," *Western Criminology Review* (9:2), pp. 52–72. (http://wcr.sonoma.edu/v09n2/index.html).
Hofmann, W., and Baumert, A. 2010. "Immediate Affect as a Basis for Intuitive Moral Judgement: An Adaptation of the Affect Misattribution Procedure," *Cognition and Emotion* (24:3), pp. 522–535.
Holton, C. 2009. "Identifying Disgruntled Employee Systems Fraud Risk through Text Mining: A Simple Solution for a Multi-Billion Dollar Problem," *Decision Support Systems* (46:4), pp. 853–864.
Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., and Dhillon, G. 2014. "A Framework and Guidelines for Context-Specific Theorizing in Information Systems Research," *Information Systems Research* (25:1), pp. 111–136.
Hovav, A., D'Arcy, J., and D'Arcy, J. 2012. "Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea," *Information and Management* (49:2), Elsevier B.V., pp. 99–110.
Hsu, M.-H., and Kuo, F. Y. 2003. "The Effect of Organization-Based Self-Esteem and Deindividuation in Protecting Personal Information Privacy," *Journal of Business Ethics* (42:4), pp. 305–320.
Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?," *Communications of the ACM* (54:6), p. 54.
Hunt, S. D., and Vitell, S. 1986. "A General Theory of Marketing Ethics," *Journal of Macromarketing*, pp. 5–16.
Hutcherson, C. A., and Gross, J. J. 2011. "The Moral Emotions: A Social-Functionalist Account of Anger, Disgust, and Contempt," *Journal of Personality and Social Psychology* (100:4), pp. 719–737.
Johnson, D. G. 2009. *Computer Ethics*, (4th ed.), USA: Prentice Hall Press.
Jones, T. M. 1991. "Ethical Decision Making by Individuals in Organizations : An Issue-Contingent Model," *The Academy of Management Review* (16:2), pp. 366–395.

Jordan, J. 2007. "Taking the First Step toward a Moral Action: A Review of Moral Sensitivity Measurement across Domains," *Journal of Genetic Psychology* (168:3), pp. 323–359.

Kahneman, D. 2011. *Thinking, Fast and Slow.*, New York: Macmillan.

Khazanchi, D. 1995. "Unethical Behavior in Information Systems: The Gender Factor," *Journal of Business Ethics* (14:9), Dordrecht: Springer Science & Business Media, p. 741. (http://search.proquest.com/docview/198084319?accountid=11774).

Kim, J., Park, E. H., and Baskerville, R. L. 2016. "A Model of Emotion and Computer Abuse," *Information and Management* (53:1), Elsevier B.V., pp. 91–108.

Kohlberg, L., Levine, C., and Hewer, A. 1983. *Moral Stages: A Current Formulation and a Response to Critics.*

Kowalski, S. 1990. "Computer Ethics and Computer Abuse: A Longitudinal Study of Swedish University Students.," in *IFIP TC11 6th International Conference on Information Systems Security.*

Kowalski, S., and Kowalski, H. 1990. "Computer Ethics and Computer Abuse: A Study of Swedish and Canadian University Data Processing Students.," *Information Age* (12:4), pp. 206–212.

Kuo, F., Lin, C. S., Sun, H.-I., Lee, M.-H., and Huang, Y.-F. 2010. "A Study of the Effect of Anger on Immoral Judgment of Internet Privacy Invasion," *PACIS 2010 Proceedings*, pp. 1649–1655.

Kuppens, P., and Van Mechelen, I. 2007. "Interactional Appraisal Models for the Anger Appraisals of Threatened Self-Esteem, Other-Blame, and Frustration," *Cognition and Emotion* (21:1), pp. 56–77.

Lacity, M. C., and Janson, M. A. 1994. "Understanding Qualitative Data: A Framework of Text Analysis Methods," *Journal of Management Information Systems* (11:2), pp. 137–155.

Ladd, J. 1982. "Collective and Individual Moral Responsibility in Engineering: Some Questions," *IEEE Technology and Society Magazine* (June), pp. 3–10.

Lankton, N. K., Stivason, C., and Gurung, A. 2019. "Information Protection Behaviors: Morality and Organizational Criticality," *Information and Computer Security* (27:3), pp. 468–488.

Lapsley, D. K., and Narvaez, D. 2004. "Moral Development, Self, and Identity," *Moral Development, Self, and Identity.*

Larsen, R. J., and Ketelaar, T. 1991. "Personality and Susceptibility to Positive and Negative Emotional States," *Journal of Personality and Social Psychology* (61:1), pp. 132–140.

Lee, Y., Lee, Z., and Kim, Y. 2007. "Understanding Personal Web Usage in Organizations," *Journal of Organizational Computing and Electronic Commerce* (17:1), pp. 75–99.

Leonard, L. N. K., and Cronan, T. P. 2001. "Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences," *Journal of the Association for Information Systems* (1:1), pp. 1–31.

Leonard, L. N. K., and Cronan, T. P. 2005. "Attitude toward Ethical Behavior in Computer Use: A Shifting Model," *Industrial Management & Data Systems* (105:9), pp. 1150–1171.
Leonard, L. N. K., Cronan, T. P., and Kreie, J. 2004. "What Influences IT Ethical Behavior Intentions - Planned Behavior, Reasoned Action, Perceived Importance, or Individual Characteristics?," *Information and Management* (42:1), pp. 143–158.
Li, H., Sarathy, R., Zhang, J., and Luo, X. 2014. "Exploring the Effects of Organizational Justice, Personal Ethics and Sanction on Internet Use Policy Compliance," *Information Systems Journal* (24:6), pp. 479–502.
Li, H., Zhang, J., and Sarathy, R. 2010. "Understanding Compliance with Internet Use Policy from the Perspective of Rational Choice Theory," *Decision Support Systems* (48:4), Elsevier B.V., pp. 635–645.
Liao, Q., Luo, X., Gurung, A., and Li, L. 2009. "Workplace Management and Employee Misuse: Does Punishment Matter?," *Journal of Computer Information Systems* (50:2), Stillwater: Taylor & Francis Ltd., pp. 49–59.
Loch, K. D., and Conger, S. 1996. "Evaluating Ethical Decision Making and Computer Use," *Communications of the ACM* (39:7), pp. 74–83.
Loch, K. D., Conger, S., Oz, E., Lock, K. D., Conger, S., and Oz, E. 1998. "Ownership, Privacy and Monitoring in the Workplace: A Debate on Technology and Ethics," *Journal of Business Ethics* (17:6), Dordrecht: Springer Science & Business Media, pp. 653–663. (http://search.proquest.com/docview/198022814?accountid=11774).
Lomas, T. 2019. "Anger as a Moral Emotion: A "bird's Eye" Systematic Review," *Counselling Psychology Quarterly* (32:3–4), Routledge, pp. 341–395.
Lowry, P. B., Dinev, T., and Willison, R. 2017. "Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda," *European Journal of Information Systems* (26:6), pp. 546–563.
Lowry, P. B., Posey, C., Roberts, T. L., and Bennett, R. J. 2014. "Is Your Banker Leaking Your Personal Information? The Roles of Ethics and Individual-Level Cultural Characteristics in Predicting Organizational Computer Abuse," *Journal of Business Ethics* (121:3), pp. 385–401.
Lysonski, S., and Durvasula, S. 2008. "Digital Piracy of MP3s: Consumer and Ethical Predispositions," *Journal of Consumer Marketing* (25:3), pp. 167–178.
McMahon, J. M., and Cohen, R. 2009. "Lost in Cyberspace: Ethical Decision Making in the Online Environment," *Ethics and Information Technology* (11:1), pp. 1–17.
McNeel, S. P. 1994. "College Teaching and Student Moral Development," *Moral Devvelopment in the Professions: Psychology and Applied Ethics*, pp. 27–49.
Merhi, M. I., and Ahluwalia, P. 2019. "Examining the Impact of Deterrence Factors and Norms on Resistance to Information Systems Security," *Computers in Human Behavior* (92:October 2018), Elsevier, pp. 37–46.

Miceli, M., and Castelfranchi, C. 2005. "Anxiety as an 'Epistemic' Emotion: An Uncertainty Theory of Anxiety," *Anxiety, Stress and Coping* (18:4), pp. 291–319.

Moll, J., and de Oliveira-Souza, R. 2007. "Moral Judgments, Emotions and the Utilitarian Brain," *Trends in Cognitive Sciences* (11:8), pp. 319–321.

Moody, G. D., Galletta, D. F., and Dunn, B. K. 2017. "Which Phish Get Caught? An Exploratory Study of Individuals' Susceptibility to Phishing," *European Journal of Information Systems* (26:6), Taylor & Francis Ltd., pp. 564–584.

Moody, G. D., Siponen, M. T., and Pahnila, S. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly* (42:1), pp. 285–311.

Moon, Y. Il, Rajagopalan, B., and Lall, U. 1995. "Estimation of Mutual Information Using Kernel Density Estimators," *Physical Review E*.

Moor, J. H. 2001. "The Future of Computer Ethics: You Ain't Seen Nothin' yet!," *Ethics and Information Technology* (3), pp. 89–91.

Moores, T. T., and Chang, J. C.-J. 2006. "Ethical Decision Making in Software Piracy: Initial Development and Test of a Four-Component Model," *MIS Quarterly* (30:1), pp. 167–180.

Morton, K. R., Worthley, J. S., Testerman, J. K., and Mahoney, M. L. 2006. "Defining Features of Moral Sensitivity and Moral Motivation: Pathways to Moral Reasoning in Medical Students," *Journal of Moral Education* (35:3), pp. 387–406.

Myyry, L., and Helkama, K. 2002. "The Role of Value Priorities and Professional Ethics Training in Moral Sensitivity," *Journal of Moral Education* (31:1), pp. 35–50.

Myyry, L., Siponen, M. T., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18:2), pp. 126–139.

Ogburn, W. F. 1957. "Cultural Lag as Theory," *Sociology & Social Research* (41), pp. 167–174.

Oh, H., Curley, S. P., and Subramani, M. R. 2008. "The Death of Distance?: The Influence of Computer Mediated Communication on Perceptions of Distance," in *ICIS*, pp. 1–14. (http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1068&context=icis2008).

Orazi, D. C., Warkentin, M., and Johnston, A. C. 2019. "Integrating Construal Level Theory in the Design of Fear Appeals in IS Security Research," *Communications of the Association for Information Systems* (45:1).

Orlikowski, W. J., and Iacono, C. S. 2001. "Research Commentary : Desperately Seeking the ' IT ' in IT Research — A Call to Theorizing the IT Artifact," *Information Systems Research* (12:2), pp. 121–134.

Ormond, D., and Warkentin, M. 2015. "Is This a Joke? The Impact of Message Manipulations on Risk Perceptions," *Journal of Computer Information Systems* (55:2), pp. 9–19.

Ormond, D., Warkentin, M., and Crossler, R. E. 2019. "Integrating Cognition with an Affective Lens to Better Understand Information Security Policy Compliance," *Journal of the Association for Information Systems* (20:12), Association for Information Systems, pp. 1794–1843.

Park, E. H., Kim, J., and Park, Y. S. 2017. "The Role of Information Security Learning and Individual Factors in Disclosing Patients' Health Information," *Computers & Security* (65), pp. 64–76.

Paxton, J. M., Ungar, L., and Greene, J. D. 2012. "Reflection and Reasoning in Moral Judgment," *Cognitive Science* (36:1), pp. 163–177.

Pekrun, R. 2006. "The Control-Value Theory of Achievement Emotions: Assumptions, Corollaries, and Implications for Educational Research and Practice," *Educational Psychology Review* (18:4), pp. 315–341.

Pemberton, J. M. 1998. "'Through a Glass Darkly': Ethics and Information Technology," *Information Management Journal* (32:1), pp. 76-84+. (http://search.proquest.com/docview/227693385?accountid=28180%5Cnhttp://xt6nc6eu9q.search.serialssolutions.com/?SS_Source=3&amp%5Cngenre=article&amp%5Cnsid=ProQ:&amp%5Cnatitle=%22Through+a+glass+darkly%22%3A+Ethics+and+information+technology&amp%5Cntitle=Information).

Pennycook, G., Fugelsang, J. A., and Koehler, D. J. 2015. "What Makes Us Think? A Three-Stage Dual-Process Model of Analytic Engagement," *Cognitive Psychology* (80), Elsevier Inc., pp. 34–72.

Peslak, A. R. 2006. "An Exploratory Investigation of Information Technology Ethics Factors," *Issues in Information Systems* (VII:2), pp. 339–343.

Peslak, A. R. 2008. "Current Information Technology Issues and Moral Intensity Influences," *The Journal of Computer Information Systems* (48:4), pp. 77–86. (http://search.proquest.com/docview/232570794?accountid=11774).

Peterson, D. K. 2002. "Computer Ethics: The Influence of Guidelines and Universal Moral Beliefs," *Information Technology & People* (15:4), West Linn: Emerald Group Publishing, Limited, pp. 346–361. (http://search.proquest.com/docview/222415542?accountid=11774).

Petrinovich, L., and O'Neill, P. 1996. "Influence of Wording and Framing Effects on Moral Intuitions," *Ethology and Sociobiology* (17:3), pp. 145–171.

Pierce, M. A., and Henry, J. W. 1999. "An Exploration of Differences in Judgements of Computer Ethical Behavior by Sex, Education, Age, and Other Demographic Factors," *Journal of International Information Management* (8:2), pp. 25–43.

Pierce, M. A., and Henry, J. W. 2000. "Judgements about Computer Ethics: Do Individual, Co-Worker, and Company Judgements Differ? Do Company Codes Make a Difference?," *Journal of Business Ethics* (28:4), pp. 307–322. (http://search.proquest.com/docview/198028545?accountid=11774).

Rest, J. 1986. *Moral Development: Advances in Research and Theory.*, Praeger.

Rest, J., Narvaez, D., Thoma, S. J., and Bebeau, M. J. 2000. "A Neo-Kohlbergian Approach to Morality Research," *Journal of Moral Education* (29:4), pp. 381–395.

Rest, J. R. 1983. "Morality," in *Handbook of Child Psychology. Vol. III: Cognitive Development* (4th ed.), New York: John Wiley, pp. 556–629.
Rest, J. R. 1994. "Background: Theory and Research," in *Moral Development in the Professions: Psychology and Applied Ethics.*, Hillsdale, NJ: Lawrence Erlbaum Associates.
Rest, J., Turiel, E., and Kohlberg, L. 1969. "Level of Moral Development as a Determinant of Preference and Comprehension of Moral Judgments Made by Others," *Journal of Personality* (37:2), pp. 225–252.
Roberts, J. A., and Wasieleski, D. M. 2012. "Moral Reasoning in Computer-Based Task Environments: Exploring the Interplay between Cognitive and Technological Factors on Individuals' Propensity to Break Rules," *Journal of Business Ethics* (110:3), Dordrecht: Springer Science & Business Media, pp. 355–376.
Robin, D. R., Reidenbach, R. E., and Forrest, R. J. 1996. "The Perceived Importance of an Ethical Issue as an Influence on the Ethical Decision-Making of Ad Managers," *Journal of Business Research* (35), pp. 17–28.
Roseman, I. J., Spindel, M. S., and Jose, P. E. 1990. "Appraisals of Emotion-Eliciting Events: Testing a Theory of Discrete Emotions," *Journal of Personality and Social Psychology* (59:5), pp. 899–915.
Ryan, R. M., and Deci, E. L. 2000. "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions," *Contemporary Educational Psychology* (25:1), pp. 54–67.
Sacco, V. F., and Zureik, E. 1990. "Correlates of Computer Misuse: Data from a Self-Reporting Sample.," *Behaviour & Information Technology* (9:5), pp. 353–369.
Schwartz, A., Eyal, T., and Tamir, M. 2018. "Emotions and the Big Picture: The Effects of Construal Level on Emotional Preferences," *Journal of Experimental Social Psychology* (78:January 2017), pp. 55–65.
Schwartz, S. H. 1977. "Normative Influences on Altruism," *Advances in Experimental Social Psychology* (10), pp. 221–279. (http://content.apa.org/journals/psp/36/7/715).
Scilhavy, R. A. M., and King, R. C. 2009. "The Virtuous and the Vicious: The Effects of Professionalism and Machiavellianism on Ethical IT Decision Making," *Proceedings of the 15th Americas Conference on Information Systems*, pp. 1–9.
Silfver-Kuhalampi, M. 2009. "The Sources of Moral Motivation: Studies on Empathy, Guilt, Shame and Values," University of Helsinki.
Silic, M., Barlow, J. B., and Back, A. 2017. "A New Perspective on Neutralization and Deterrence: Predicting Shadow IT Usage," *Information & Management* (54:8), pp. 1023–1037.
Silverman, B. W. 1986. "Density Estimation: For Statistics and Data Analysis," *Density Estimation: For Statistics and Data Analysis*.
Sinha, R. K., and Mandel, N. 2008. "Preventing Digital Music Piracy: The Carrot or the Stick?," *Journal of Marketing* (72:1), pp. 1–15.

Siponen, M. T. 2001. "On the Role of Human Mortality in Information System Security: From the Problems of Descriptivism to Non-Descriptive Foundations," *Information Resources Management Journal* (14:4), pp. 15–23.
Siponen, M. T., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487–502.
Siponen, M. T., and Vance, A. 2014. "Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations," *European Journal of Information Systems* (23:3), Basingstoke: Palgrave Macmillan, pp. 289–305.
Siponen, M. T., and Vartiainen, T. 2002. "Teaching End-User Ethics: Issues and a Solution Based on Universalizability," *Communications of the Association for Information Systems* (8:29), pp. 422–443.
Siponen, M. T., and Vartiainen, T. 2005. "Attitudes to and Factors Affecting Unauthorized Copying of Computer Software in Finland," *Behaviour & Information Technology* (24:September), pp. 249–257.
Siponen, M. T., and Vartiainen, T. 2007. "Unauthorized Copying of Software: An Empirical Study of Reasons for and Against," *ACM SIGCAS Computers and Society* (37:1), pp. 30–43.
Sloman, S. A. 1996. "The Empirical Case for Two Systems of Reasoning," *Psychological Bulletin* (119:1), pp. 3–22.
Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. "Variables Influencing Information Security Policy Compliance," *Information Management & Computer Security* (22:1), pp. 42–75.
Son, J.-Y. Y., and Park, J. 2016. "Procedural Justice to Enhance Compliance with Non-Work-Related Computing (NWRC) Rules: Its Determinants and Interaction with Privacy Concerns," *International Journal of Information Management* (36:3), Elsevier Ltd, pp. 309–321.
Sparks, J. R. 2015. "A Social Cognitive Explanation of Situational and Individual Effects on Moral Sensitivity," *Journal of Applied Social Psychology* (45), pp. 45–54.
Sparks, J. R., and Hunt, S. D. 1998. "Marketing Researcher Ethical Sensitivity: Conceptualization, Measurement, and Exploratory Investigation," *Journal of Marketing* (62:April), pp. 92–109.
Stahl, B. C. 2004. "Responsibility for Information Assurance and Privacy: A Problem of Individual Ethics?," *Journal of Organizational and End User Computing* (16:3), pp. 59–77.
Stahl, B. C. 2012. "Morality, Ethics, and Reflection: A Categorization of Normative IS Research," *Journal of the Association for Information Systems* (13:8), Atlanta: Association for Information Systems, pp. 636–656. (http://search.proquest.com/docview/1039704452?accountid=11774).
Stylianou, A. C., Winter, S., Niu, Y., Giacalone, R. A., and Campbell, M. 2013. "Understanding the Behavioral Intention to Report Unethical Information Technology Practices: The Role of Machiavellianism, Gender, and

Computer Expertise," *Journal of Business Ethics* (117:2), Dordrecht: Springer Science & Business Media, pp. 333–343.
Sykes, G. M., and Matza, D. 1957. "Techniques of Neutralization : A Theory of Delinquency," *American Sociological Review* (22:6), pp. 664–670.
Tangney, J. P., Miller, R. S., Flicker, L., and Barlow, D. H. 1996. "Are Shame, Guilt, and Embarrassment Distinct Emotions?," *Journal of Personality and Social Psychology* (70:6), pp. 1256–1269.
Tangney, J., Stuewig, J., and Mashek, D. 2007. "Moral Emotions and Moral Behavior," *Annu Rev Psychol* (58), pp. 345–72.
Thatcher, J. B., and Perrewé, P. L. 2002. "An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficacy," *MIS Quarterly* (26:4), pp. 381–396.
Thoma, S. J., and Dong, Y. 2014. "The Defining Issues Test of Moral Judgment Development.," *Behavioral Development Bulletin* (19:3), pp. 55–61.
Thong, J. Y. L., and Yap, C.-S. 1998. "Testing an Ethical Decision-Making Theory: The Case of Softlifting," *Journal of Management Information Systems* (15:1), pp. 213–237.
Trope, Y., and Liberman, N. 2010. "Construal-Level Theory of Psychological Distance," *Psychological Review* (117:2), pp. 440–463.
Ugrin, J. C., and Michael Pearson, J. 2013. "The Effects of Sanctions and Stigmas on Cyberloafing," *Computers in Human Behavior* (29:3), pp. 812–820.
Vance, A., Fellow, S. J. B., Siponen, M. T., and Straub, D. W. 2019. "Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations across Cultures," *Information & Management* (57:4).
Vance, A., Lowry, P. B., and Eggett, D. 2015. "Increasing Accountability Through User-Interface Design Artifacts: A New Approach To Addressing the Problem of Access-Policy Violations.," *MIS Quartely* (39:2), pp. 345–366. (http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=102375755&site=ehost-live&scope=site).
Vance, A., and Siponen, M. T. 2012. "IS Security Policy Violations: A Rational Choice Perspective," *Journal of Organizational and End User Computing* (24:1), pp. 21–41.
Vance, A., Siponen, M. T., and Pahnila, S. 2012. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Information and Management* (49:3–4), Elsevier B.V., pp. 190–198.
Volker, J. M. 1984. "Counseling Experience, Moral Judgement, Awareness of Consequences and Moral Sensitivity in Counseling Practice," unpublished doctoral dissertation, University of Minnesota, MN.
Wall, D. S. 2010. "The Internet as a Conduit for Criminal Activity," *Information Technology and The Criminal Justice System* (March), pp. 77–98.
Walstrom, K. A. 2006. "Social and Legal Impacts on Information Ethics Decision Making," *The Journal of Computer Information Systems* (47:2), pp. 1–8. (http://search.proquest.com/docview/232576404?accountid=11774).

Warkentin, M., Willison, R., and Johnston, A. C. 2011. "The Role of Perceptions of Organizational Injustice and Techniques of Neutralization in Forming Computer Abuse Intentions," in *Proceedings Of The Americas Conference On Information Systems*, pp. 2822–2829. (http://aisel.aisnet.org/amcis2011_submissions/318/).

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review.," *MIS Quarterly* (26:2), xiii–xxiii.

Weckert, J. 1997. "Intellectual Property Rights and Computer Software," *Business Ethics: A European Review* (6:2), pp. 101–109.

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1–20.

Winter, S. J., Stylianou, A. C., and Giacalone, R. A. 2004. "Individual Differences in the Acceptability of Unethical Information Technology Practices: The Case of Machiavellianism and Ethical Ideology," *Journal of Business Ethics* (54:3), pp. 275–301. (http://search.proquest.com/docview/198093313?accountid=11774).

Xu, Z., and Hu, Q. 2018. "The Role of Rational Calculus in Controlling Individual Propensity toward Information Security Policy Non-Compliance Behavior," *Proceedings of the 51st Hawaii International Conference on System Sciences* (9), pp. 3688–3697.

Yazdanmehr, A., and Wang, J. 2016. "Employees' Information Security Policy Compliance: A Norm Activation Perspective," *Decision Support Systems* (92), pp. 36–46.

Yoon, C., and Kim, H. 2013. "Understanding Computer Security Behavioral Intention in the Workplace," *Information Technology & People* (26:4), pp. 401–419.

Zhang, D., Oh, L., and Teo, H.-H. 2006. "An Experimental Study of the Factors Influencing Non-Work Related Use of IT Resources at Workplace," *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (8), pp. 3688–3697.

Zimbardo, P. G. 1969. "The Human Choice: Individuation, Reason, and Order versus Deindividuation, Impulse, and Chaos.," *Nebraska Symposium on Motivation* (17), pp. 237–307.

APPENDICES

Appendix 1 Summary of reviewed studies and key findings

Study	Phenomenon	Method	Sample	Primary theory; Role of morality	Key relevant Findings
(Al-Omari, Deokar, El-Gayar, Walters, & Aleassa, 2013)a	Compliance with security policy	QNT/Cross-sectional/ Jordan	445 employees	TPB	Moral obligation, and formalism positively influenced intention to comply while ethical egoism, affected intention negatively.
(Banerjee, Cronan, & Jones, 1998)	Information technology misuse	QNT/Cross-sectional/scenario/US	139 employees	TRA	Intention to behave ethically was affected by personal normative beliefs, and organizational climate, while attitude* and level of moral development were not found to have a significant primary effect.
(Bansal, Green, Hodorff, & Marshall, 2016)	Security policy non-compliance	QNT/Cross-sectional/scenario	173 (online)	NA	Moral belief was found to negatively affect security policy non-compliance intentions.
(Bauer & Bernroider, 2017)	Compliant information security behavior	QLT+QNT/Cross-sectional	97 Employees	TRA; Part of self-regulatory process	The paper considered the use of neutralization techniques as a reflection of personal moral norms and found a negative relationship between neutralization and intention to comply.

Study	Phenomenon	Method	Sample	Primary theory; Role of morality	Key relevant Findings
(Chang, 2011)	Ethical IT use	QLT/interview/ China, Taiwan, Hong-Kong	89 Employees	Chinese morality	In mainland china, some individuals acknowledged they would violate access to customer data for self-interest while individuals in Hong Kong and Taiwan considered it immoral. Gunaxi was found important in decisions to violate privacy and to provide accurate information to customers in mainland china, Hong Kong, and Taiwan.
(Chatterjee, Sarker, & Valacich, 2015)	Unethical IT use	QNT/Factorial/scenarios	? Undergrad students	TPB	Moral intensity was found to negatively affect attitude toward unethical IT use. Technological idealism negatively influenced attitude toward unethical IT use when it was very high or very low. Technological relativism influenced attitude only when it was not strong.
(Chatterjee, Valacich, & Sarker, 2011)	Unethical IT use	QNT/Factorial/scenarios/ US, Finland	141+189 Undergrad students	TPB	Technological idealism and relativism beliefs were found to have no significant effect on attitude in either US or Finnish samples. Moral intensity negatively affected attitude toward unethical IT use in both US and Finnish samples.
(Chu, Chau, & So, 2015)	IS resource misuse	QNT/Cross-sectional	208 employees (online)	TPB	Intention and desire to misuse resources both affected behavior, however, the effect of intention was found to be larger.
(Cronan, Leonard, & Kreie, 2005)	Ethical IT use/misuse	QNT/Cross-sectional/scenario/US	429 students	TRA	Attitude* was found to affect intention to engage in ethical IT use. Perceived ethical importance of a scenario influenced intention in all scenarios (small effect size). Perceived importance of a scenario also affected attitude* in all but one scenario.

Study	Phenomenon	Method	Sample	Primary theory; Role of morality	Key relevant Findings
(D'Arcy & Devaraj, 2012)	IT Misuse	QNT/Cross-sectional/scenario/US	228 employees+273 MBA students	DT; Informal regulatory mechanism (informal sanction)	Formal sanctions had a positive effect on moral beliefs regarding misuse. Moral beliefs influenced misuse intention negatively and partially mediated the effect of formal sanctions and social desirability pressure on misuse intention.
(D'arcy & Hovav, 2009)	IS misuse	QNT/Cross-sectional/scenario/US	269 employees + 238 MBA students	DT	Moral judgement had the strongest effect on intention to access information without authorization and to modify information without authorization. Virtual status of the employee was found moderating the effect of SETA programs on intention to access information without authorization and the effect of monitoring on intention to modify information without authorization.
(D'Arcy, Herath, & Shoss, 2014)	Security policy violation	QNT/Cross-sectional/scenario	539 (online)	Moral disengagement theory; Self-sanction mechanism	Security-related stress was found to have an indirect effect on security policy violation intention via moral disengagement. Perceived sanctions was found to negatively affect moral disengagement.
(D'Arcy, Herath, Yim, Nam, & Rao, 2018)	Security policy violation	QNT/Cross-sectional/scenario/Canada	150 employees	Moral disengagement theory; Self-sanction mechanism	Security-related stress (overload, complex, uncertain requirements) was found to have an indirect effect on security policy violation intention via moral disengagement. Perceived sanctions was found to negatively affect moral disengagement.
(D'Arcy, Hovav, & Galletta, 2009)	IS misuse	QNT/Cross-sectional/scenario/US	269 employees	DT; A concern that could diminish the effect of sanctions	For those high on moral commitment, perceived certainty woks as a deterrent while perceived severity does not and for those low in moral commitment perceived severity works as a deterrent while perceived certainty does not.
(D'arcy & Lowry 2019)	Compliance with information security policies	QNT/Experience-sampling/US	77 Professionals (online)	TPB and RCT; A mechanism for resolving conflicting courses of action	. Moral beliefs as a between-individual measure positively influenced average daily compliance with security policy. Organizational deviance as a within-individual measure was negatively related to compliance.

Study	Phenomenon	Method	Sample	Primary theory; Role of morality	Key relevant Findings
(Dorantes, Hewitt, & Goles, 2006)	IT unethical behavior	QNT/Cross-sectional/scenario/US	318 students	ICM	Moral intensity influenced recognition of ethical situation, moral judgement and moral intentions but not for all scenarios. Recognition of moral situation positively affected moral judgement, and both recognition of moral situation and moral judgement negatively affected intention to behave unethically.
(Ellis & Griffith, 2001)	IS misuse	QNT/Cross-sectional/scenario	? Undergrad and grad students	Three dimensional model of ethics	Out of moral equity, contractualism and relativism only moral equity was found to be associated with moral judgement in all scenarios.
(Friedman, 1997)	Property and privacy issues in computer-mediated behavior	QLT/interview/US	64 adolescents	NA; A concern for other's welfare, justice, and/or rights.	Justifications of adolescent students permitting privacy acts (accessing a computer file, reading a letter, reading a diary) relied on welfare considerations (others not affected and that of the actor), personal choice and fairness and rights justifications. Reproducibility, intangibility, decoupling of access from misuse and far proximity to potential victims affected justifications of adolescents.
(Gattiker & Kelley, 1999)	Ethical computer use	QNT/Cross-sectional/scenario/US	120 (online) + 17 Professionals	Domain Theory of Moral Development; An impartial constraint on the pursuit of individual interests	Ratings of permissiveness was different for the three domains of morality under investigation: personal (encryption scenario), conventional (Virus scenario), and moral (banned game).
(Goles, White, Beebe, Dorantes, & Hewitt, 2006)	IS misuse	QNT/Cross-sectional/scenario/US	442 students	ICM	Moral intensity had an effect on intention to behave ethically via moral recognition.

Study	Phenomenon	Method	Sample	Primary theory; Role of morality	Key relevant Findings
(Grace, 2013)	IT misuse	QNT/Cross-sectional/scenario	280 employees	Theory of ethical decision making in marketing	Moral intensity was found to affect both deontological and teleological evaluations. Both deontological and teleological evaluations were found to affect intentions to behave ethically.
(Haines & Leonard, 2007)	Ethical IT use/misuse	QNT/Cross-sectional/scenario/US	167 students	FCM	Moral judgement affected moral intention in all scenarios and perceived ethical importance of an issue affected moral judgement in all scenarios. Moral obligation was found to affect moral intent in 2 out of 5 scenarios.
(Harrington, 1996)	Computer abuse	QNT/Cross-sectional/scenario/US	219 employees	FCM	Company specific-codes of ethics influenced those individuals high in responsibility denial.
(Harrington, 1997)	Computer misuse	QNT/Factorial/scenarios/US	83 students + 219 professionals	ICM	Individuals who are characteristically less rule-oriented or those who are less tending to deny responsibility were more likely to find spreading viruses immoral and were more likely to intend to behave ethically. Social consensus had an effect on moral judgement and moral intent.
(Harris, Yates, Quaresma, & Harris, 2010)	Ethical IT use/misuse	QNT/Cross-sectional/scenario/Spain, Portugal, US	537 students	PAPA model	Individuals' ethical profiles in all samples (US, Spain and Portugal) were found to be negatively related to their self-reported misuse in less than half of the reported scenarios. However, differences were observed between the samples with respect to specific scenarios such as software use, and programming abuse.
(Hovav & D'Arcy, 2012)	IS Misuse	QNT/Cross-sectional/scenario/US, South Korea	269+145 employees + 97+215 students	DT; Informal regulatory mechanism (informal sanction)	Moral beliefs were found to be very good predictors of IS misuse intentions in both US and Korean samples.

Study	Phenomenon	Method	Sample	Primary theory; Role of morality	Key relevant Findings
(Hsu & Kuo 2003)	Protecting personal information	QNT/Cross-sectional/scenario/Taiwan	212 employees	TPB	Attitude* and subjective norms were found to have an effect on encouraging protection of others' information privacy. Deindividuation was linked to exhibiting less concern for protecting information privacy of others.
(Hu, Xu, Dinev, & Ling, 2011)	Security policy violation	QNT/Cross-sectional/scenario/China	207 employees	RCT; An internal force against which economic costs and benefits are assessed	Moral belief had an effect on perceived intrinsic benefits (negatively), shame, perceived informal risk, and perceived formal risk (all positively)
(Khazanchi, 1995)	Ethical IT use/misuse	QNT/Cross-sectional/scenario	134 undergrad and grad students	NA	In only 3 out of 7 scenarios female respondents judged the moral wrongness of acts in the given scenarios related to disclosure, integrity and conflict of interest higher than males. The scores for both men and women were high.
(Kim et al. 2016)	IS abuse	QNT/Factorial/scenarios/US	193 employees	Theory of emotion process; An internal regulation mechanism	Morality of an individual was found to influence abuse-positive affect and abuse intent negatively.
(Kowalski & Kowalski, 1990)	Computer abuse	QNT/Cross-sectional/Sweden, Canada	135 + 158 students	NA; An internal control mechanism for preventing crimes	Most of the students in both Swedish and Canadian samples rated computer abuse situations as unethical.
(Kowalski 1990)	Computer abuse	QNT/Cross-sectional/Sweden	157 + 325 students	NA; The foundation of any control system containing human elements	A shift in attitude was reported from 1986 to 1990 toward a view that computer resources should not be owned by an individual or organization.
(Kuo, Lin, Sun, Lee, & Huang, 2010)	Privacy invasion	QNT/Factorial/scenarios/Taiwan	114 students	NA	Anger influenced moral judgements regardless of moral obligation and exposure to violent/non-violent stimulus.

Study	Phenomenon	Method	Sample	Primary theory; Role of morality	Key relevant Findings
(Lankton et al. 2019)	Information protection	QNT/Factorial/scenarios/US	216 professionals and students	ICM; A concern that produces self-approval, virtue, or pride	For behaviors of high criticality, temporal immediacy, proximity and social consensus are related to moral judgments. For low criticality behaviors, magnitude of consequences and social consensus were related to moral judgments. Moral judgments about the rightness of performing a protective security behavior was found to be related to intention.
(Lee, Lee, & Kim, 2007)	Personal web usage	QNT/Cross-sectional/US	426 employees	TPB; A constraining mechanism that ensures functioning in a society	No evidence was found as for the effect of moral obligation on intention to use internet for personal purposes.
(Leonard & Cronan, 2001)	Ethical IT use/misuse	QNT/Cross-sectional/scenario/US	423 students	TRA	Attitude*, personal normative beliefs, and moral development (D-score) were found to affect intention to behave ethically. Ego strength could moderate this effect.
(Leonard & Cronan, 2005)	Ethical IT use/misuse	QNT/Cross-sectional/scenario/US	422 students	Attitude model	Moral obligation was consistently related to attitude* in all scenarios.
(Leonard, Cronan, & Kreie, 2004)	Ethical IT use/misuse	QNT/Cross-sectional/scenario/US	423 students	TPB	Intention to behave ethically was found to be affected by attitude*, personal normative beliefs, perceived ethical importance, ego strength, and moral development level (D-score). This make-up changed when each scenario was examined individually.
(Li, Sarathy, Zhang, & Luo, 2014)	Internet use policy compliance	QNT/Cross-sectional/US	241 employees (online)	Organizational justice theory; An intrinsic self-regulatory mechanism.	Procedural and interpersonal justice influenced personal ethics. Personal ethics influenced compliance intention.

Study	Phenomenon	Method	Sample	Primary theory; Role of morality	Key relevant Findings
(Li, Zhang, & Sarathy, 2010)	Internet use policy compliance	QNT/Cross-sectional/US	246 employees (online)	RCT; A regulatory mechanism that is independent from economic cost-benefit evaluations	For those who highly believe personal internet use is wrong (high personal norms), perceived sanction severity reduces compliance intentions. Organizational norms and organizational identification both have a positive effect on personal norms.
(Liao, Luo, Gurung, & Li, 2009)	Workplace internet misuse intention	QNT/Cross-sectional/US	205 employees (online)	TPB and DT	Perceived ethical importance positively influenced favorable attitudes toward misuse avoidance.
(Loch & Conger, 1996)	Computer misuse	QNT/Cross-sectional/scenario/US	174 grad students	TRA	Attitude* affected all intention scenarios but the model fit was very low in general. Deindividuation was found to affect attitude* in one out of three scenarios.
(Lowry, Posey, Roberts, & Bennett, 2014)	Computer abuse	QNT/Cross-sectional/US	449 employees (online)	Theory of ethical decision making in marketing; A mechanism that prevents acting in one's self-interest	Collectivism moderated the negative relationship between formalism and computer abuse as well as the negative relationship between utilitarianism and computer abuse. Formalism was found to have a stronger negative effect on computer abuse than utilitarianism
(Mcmahon & Cohen, 2009)	Computer (mis)use	QNT/Cross-sectional/scenario/US	93 undergrad students	Machiavellianism; A societal concern for governance in a decentralized and borderless environment	No connection was found between Machiavellianism and moral judgement regarding computer usage behaviors.
(Merhi & Ahluwalia, 2019)	Resistance to Security policy	QNT/Cross-sectional/US	133 employees	DT; A mechanism for regulating compliance decisions	Descriptive norms (one's perceptions are what others are doing) was found to have an effect on moral norms (one's perception of what a given employee should do). Detection certainty was found to have an effect on moral norms and moral norms affect resistance to IS security

Study	Phenomenon	Method	Sample	Primary theory; Role of morality	Key relevant Findings
(Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009)	Compliance with security policy	QNT/Cross-sectional/scenario/Finland	97 employees + 66 grad students	Theory of Moral Development; Theory of Motivational Types of Value; A mechanism for resolving conflicting courses of action	Preconventional level of moral reasoning was related to compliance with security policy in both hypothetical and real-life scenarios. Openness to change value type was found to be negatively related to compliance with security policy in both hypothetical and real-life scenarios.
(Park, Kim, & Park, 2017)	Patient Health Information disclosure	QNT/Cross-sectional/South Korea	123 undergrad students	DT; A deterrent mechanism	Health information security awareness was found positively affecting personal norms. Personal norms, in turn, had a negative effect on intention to violate patient's health information.
(Peslak, 2008)	IT (un)ethical behavior	QNT/Cross-sectional/US	307 employees and students	ICM	Different moral intensity components were found to affect moral judgements about different IT issues. However, magnitude of consequences and social consensus were found to be more influential than others, respectively.
(Peterson, 2002)	Ethical use of company computers	QNT/Cross-sectional/US	285 employees	NA	For individuals highly believing in universal moral rules, misuse intentions remained the same with more ethics guidelines. However, misuse intentions of those who believed less in universal moral rules were affected highly by more clear ethics guidelines.
(Pierce & Henry, 1999)	Use of IT resources	QNT/Cross-sectional/scenario	356 employees	NA	Evidence shown that age, years in the profession, and position may affect personal moral judgements, perceptions of co-workers judgments and perceptions of what the company expects.
(Pierce & Henry, 2000)	Ethical computer technology use	QNT/Cross-sectional/scenario	356 employees	NA	Individuals' moral judgements, their perceptions of their coworkers' moral judgements, and perceptions of company norms were inconsistent in different scenario types.

Study	Phenomenon	Method	Sample	Primary theory; Role of morality	Key relevant Findings
(Sacco & Zureik, 1990)	Computer misuse	QNT/Cross-sectional/Canada	105 undergrad students	NA; A control mechanism	Moral judgements were found to negatively affect self-reported computer misuse.
(Scilhavy & King, 2009)	Unethical computer use	QNT/Factorial/scenarios	240 grad students	FCM	The more intense scenario led to a strong effect of moral recognition on moral judgement based on equity while the less intense scenario led to a strong effect of moral recognition on moral judgement based on relativism. Regardless of the intensity of each scenario, moral judgements based on equity were found to affect moral intentions. Meanwhile, professionalism and Machiavellianism were found to affect moral recognition.
(Son & Park, 2016)	non-work-related computing	QNT/Cross-sectional/South Korea	209 employees (online)	Organizational justice theory; A concern in fairness evaluations	No evidence of the effect of Moral commitment on intention to comply with non-work-related computing was found.
(Ugrin & Michael Pearson, 2013)	cyberloafing	QNT/Factorial/scenarios/US	81 employees + 69 students	DT; A mechanism that motivates rule-following	Sanctions influenced intention to cyberloaf in cases of social media and email usage (two types of cyberloafing) when detection is likely, and there have been instances of past sanction enforcement. This effect is likely when the cyberloafing activity in question (social media and email usage) is deemed to be less abusive (more acceptable).
(Walstrom, 2006)	Information ethics decision-making	QNT/Cross-sectional/scenario	308 students	NA; A mechanism to help reinforce benefits and prevent losses	Evidence showed that perceived legality and social acceptability were almost equally related to perceived ethical correctness.
(Vance & Siponen, 2012)	IS security policy violation	QNT/Cross-sectional/scenario/Finland	203 students	RCT; An overriding concern	Moral beliefs were found to negatively affect intention to violate security policy.

Study	Phenomenon	Method	Sample	Primary theory; Role of morality	Key relevant Findings
(Vance, Lowry, & Eggett, 2015)	Access policy violation	QNT/Cross-sectional/scenario	318 employees	Accountability theory	Moral intensity was found to have a positive effect on intention to violate access policy.
(Winter, Stylianou, & Giacalone, 2004)	Privacy and IP rights	QNT/Cross-sectional	290 employees	Machiavellianism	In general, Machiavellianists had more favorable attitudes* toward privacy violations. This effect was found to be stronger for those who work in R&D than those who did not. Idealists were found to hold less favorable attitudes* toward violating privacy rights.
(Xu & Hu, 2018)	Security policy non-compliance	QNT/Cross-sectional/scenario/China	207 employees	DT; A form of deterrence	Moral beliefs affect intention to commit security policy violation negatively in low risk and medium risk scenarios. In high risk scenario, moral beliefs do not have a direct effect on intention, instead it moderates the effect of self-control on intention. Level of risk seems to refer to punishment.
(Yazdanmehr & Wang, 2016)	Information security policy compliance	QNT/Cross-sectional/US	201 employees (online)	Norm activation theory; An internal self-rewarding and self-sanctioning mechanism	Personal norms were found to positively affect compliance with information security policy. Awareness of consequences and ascription of personal responsibility were found to affect personal norms. Injunctive norms and subjective norms positively affect personal norms.
(Yoon & Kim, 2013)	Computer Security Behavior	QNT/Cross-sectional/South Korea	162 employees	TRA; A self-control mechanism	Moral obligation was found to affect computer security behavioral intentions. Subjective norms, organizational norms, and existence of security policies were found to positively affect experience of moral obligation.

Study	Phenomenon	Method	Sample	Primary theory; Role of morality	Key relevant Findings
(Zhang, Oh, & Teo, 2006)	IT resource misuse	QNT/Factorial/scenarios	120 undergrad students	TPB	Attitude*, and personal norms affected intention to engage in IT resource misuse (porn & P2P). Perceived ethical importance was found to have an effect on attitude*. Anonymity was found to negatively affect intention to misuse IT resources.
*Denotes characterization of attitude construct as moral judgment					

Appendix 2 Examples of expressions of IT characteristics

IT characteristic	(High or Low perception) Quote
Non-excludability	(Low) If there are heavy resources at stake, he probably understands that sharing this very privileged access isn't *fair* for anyone, especially, the *other people in the queue*.
	(Low) [This server is] an exclusive piece of technology that has to be used for specific reasons. It's not an Xbox. It's not a PlayStation. It's a computer to analyze data that's exclusive to your contractual obligations… you can't have external people running their datasets through your piece of equipment for *scientisits* in your *organization*
	(Low) [I]t's meant for the use of the *university researchers or whoever* it is designated to, and I'm presuming that it's actually being used so there are no, it's not running idle, most of the time. So, *the resources should be used by the people who they are meant for*.
	(High) They might feel it is not so serious violation as there is no clear damage done.
Verifiability	(Low) [M]ost people can't really judge if the *code is malicious* or not. So, you don't really run other people's code without like probably reading it… Well, the supercomputer is an expensive thing and the *university* has probably *paid for it.*
	(low) I'm thinking that the data might have something, some s**t in it, some malware or something. Not that the researcher is a bad person, might be just *infected*, he might not know, you know, that type of thing. And then I would be responsible if something happens if suddenly the supercomputer explodes or something like that would be my concern. So, I wouldn't be sure so, I would ask the *specialists*. You know the *people that handle the actual machine.*
Interconnectedness	(High) Yeah, sure, and also you just adding onto sharing your password, if you share with someone your password, I think, and this is generalizing again but let's say a lot of people use the same password for so many different things, like, that's bananas, because you're giving someone potential *access to a lot of other accounts*.
	(High) It would also give *them access to all of your [anonymized] accounts*, because at least in [anonymized], you use the same username and password for the cloud storage that you used to log into other [anonymized] accounts.
Anonymity	(High) It's not that after you get the permission, from the context, I assume that there is nobody above her head like checking what you are on.
	(High) [N]ow I'm thinking, what if the dataset is really involved in some study that I'm doing, and no will ever notice that it's from someone else, because it looks very similar to what I'm researching, right?
	(Low) [The] secretary could have friends among the student body and some of the secretary's friends might want the secretary *to go and edit their grades in the system…* And, also, the system or login

	leaves like a paper trace, then, if the secretary used the lecturer password to login that would, it would put the blame on the lecturer, and the system would report the lecturer as the one who's *editing all those grades*.
	(Low) when I'm the one using the machine, it's definitely in the record that I used the machine at this time and this period of time and that kind of thing. And, so, every time I'm using the machine if something does happen, if something goes wrong, it falls on me… so picture a horrible scenario where it *wipes up the whole system* and then there is all these *other people who have information stored,* the things they do, *could be wiped, could be corrupted.*
Limitability	(High) If she's not just giving out the password and go run your stuff, then she can read the stuff and kind of be sure that it's nothing malicious.
	(High) [A]nother person could ask what do you need [this access] for, what kind of information, and, instead of like giving her the password, that person would go and find information for her, and then give it to her… I think, it's better than giving the whole password, the whole access to that person.
	(High) You log in to the system on your own computer and then let your friend use the tool. This would be safer.
	(High) It seems that the secretary has this information, so technically you are not telling them anything new.
	(Low) The best way to do this is to have [a system that allows] a guest account that can access some documents and maybe for people that you're not sure.

Appendix 3 Examples of expressions of affective responses

Affective response	Quote
Anger	I find it very selfish to make that kind of request in the first place. It puts the one with the license in a tough spot since you do not want to appear rude, and you want to help a friend out. This is selfish behavior and the university wants to prevent exactly this kind of behavior by requiring the license holder to read the security policy again
	I wouldn't appreciate it because someone is putting me into that situation. ... it wouldn't be a professional thing to do and it sound like something that puts someone else's work on you unless there is a very strong reason like you are also working with that person on that project which didn't sound to be the case then it's basically doing someone else's work
	[I would feel] a bit annoyed that someone is asking for my password.
Empathy	I think that the recognition with the other person, all researchers or for example if this person is let's say we're all doctoral students it's just the recognition of I see myself in your shoe and I would appreciate it if somebody would've helped me if it was the other way around.
	it's going to feel, pretty rough and you know what I think that a lot researchers and I'm gonna go out a limb here, I'm generalizing a lot but I think a lot of researchers tend to be on the more agrreable end of the personality spectrum so they're more agreeable and compassionate and so that would make them feel pretty rough when I have to say no to something like that but I have to say no
	[I]t's understandable that sometime people who do not have enough resources specially, you have a big data set, you are a master student and you don't have the right to go to the processor and you got this massive pile of data.
	What I considered is that well obviously I can't give it to her but it would be kinda selfish of me to say sorry I can't just give it to you and that's it and let her figure out what she is going to do next so that's why I came to the decision that maybe like suggest a way that she could still get it but just not through me cause I'm not allowed to give it to her but maybe there is a rightful way to get it so I would say why wouldn't you ask to get it from the faculty or whatever that you get the tool from coz I still think that there's nothing wrong with that
	But when I think about situations that I'm in my own field, because there are people who don't have funding but who are doing good research nevertheless so if she knew him well maybe she could help him out.
Frustration	Yes, but also it's frustrating, this security, like the over-emphasis on security is also frustrating, it causes, sometimes it causes more problems to people than benefits it seems, for example in my work I cannot receive material anymore by email, probably the same with everybody because the new regulation, we just can't receive that so I guess that is probably more harm than good
	Hmm that's very, and, it's also very annoying, because it puts me in a position of power to help them or not, and it's not very fair. If they are doing good research, anyway, and then, well, I would try to help them out if I could be certain that they are going to be doing good research and yeah.

	And, if I thought that they are being unfairly out funding at the moment and so on.
	I keep feeling that my answers are all about wanting a system that is a little bit, enough leeway for people to still be human while dealing with these very sensitive things. Like, don't put so much burden on me to be the one who I have to decide now. I have to share this password and feeling the guilt of I might cause some trouble by doing this, but I have to do.
	So, this is like a cynical interpretation of the [limitations on sharing access to the server in this] situation: It's important that not everyone can have access, because it helps to keep up the hierarchies.
Anxiety	I would turn down Smiths' proposal: it is more important for me to hold on my promises than fulfil a friend's request of help which she must know is against the policy. However, the closer the person is to me, the more difficult it is to decline such a request. For instance, if Smith would be my sister, spouse or mother and lived in the same household, I would feel rather agonized for making the decision.
	Very annoyed [that I forgot the deadline], like, almost a little panic, a little scare like was it was today! She would say, yeah. I thought it was tomorrow!
	I would feel really stressed out. Because, obviously we had to meet the deadline and I have to get the file, but it was made very clear that only I can have access to it. So, I would feel very, it would be a dilemma, it would be really bad to be in that situation.
	I'd feel under pressure, I'd feel stressed out, I'd feel probably anxious because my because I shouldn've submitted something and deadline's tomorrow. Who know what kind of impact that might have on my performance rating and my contract and things like that you it could have a lot of ramifications so yeah I'd feel stressed , anxious, under pressure.
	I'd be so stressed. It depends on the relationship I have with the person meaning that if it's a complete stranger it's easier to say no way if it's someone you really know I would still say no way ... Because umm I like to follow the policies of my employers, I know that I can use the system only under certain conditions and only I have the access to it or the people that are authorized to it so for someone coming that is not allowed to use it and asking me to do it on his behalf, I believe I'm going around the law or around the norm.
	I would sound horrible but I would ask this person if we can clearly talk about this with somebody like a superior or something. like can I go talk to my supervisor about this and see what he/she thinks that can we do it or not.
	To be honest, I find this situation quite tricky, in terms of trying to find a sufficient solution… Normally, I would let a friend that I trust to access my university cloud storage to get the file, and then I would change my password afterwards, when I would have access to it. However, in this situation there are some research data, so it makes it more complicated.
	So these two people, actually is an issue of trust, whether you trust the secretary person but it's also the responsibility of the lecturer that she has lots of students' data… Quite a difficult case to be honest.
	Even if the interview data is anonymous it's still confidential and giving other people access is a breach of that confidentiality and security. This is a tricky situation but I think quite a few people would actually give their login

	to their friend… I wouldn't want to be the one failing my group project by forgetting to send my part. I also wouldn't want to breach the confidentiality of my empirical thesis data. I really don't want to take a side here but I think it could be argued that for many people the lesser of two evils is to share access and not fail the group project if the deadline really is strict and it couldn't be negotiated
	I could probably be in the same situation, I could understand, I would be uncertain to some extent probably.., that you would be interested in collaborating so you wouldn't want to miss that opportunity but on the other hand if you have no, absolutely no way of confirming if that was a genuine email!
	I would be in the same problem as him… Well, one thing is that they say that they keep their participants' information, their study, data in their own laptops so I thought ok you don't want anything bad happening to that