TRADEOFFS IN SURVEILLANCE AND PRIVACY TECHNOLOGIES

LAN YIHONG
(B.Eng., University of Michigan)

**A THESIS SUBMITTED
FOR THE DEGREE OF DOCTOR OF PHILOSOPHY
DEPARTMENT OF INFORMATION SYSTEMS
NATIONAL UNIVERSITY OF SINGAPORE
2021**

Supervisors:
Associate Professor Hahn Jungpil, Main Supervisor
Professor Zhenhui (Jack) Jiang, Co-Supervisor

Examiners:
Associate Professor Tan Chuan Hoo
Assistant Professor Jin Chen

DECLARATION

I hereby declare that the thesis is my original work and it has been written by me in the entirety. I have duly acknowledged all the sources of information which have been used in the thesis.

This thesis has also not been submitted for any degree in any university previously.

Yihong Lan

08 November 2021

ACKNOWLEDGEMENTS

This thesis was made possible only with the help and support of those around me, to only some of whom it is possible to give particular mention here.

I owe my sincere gratitude to my supervisor, Professor Hahn Jungpil, who guided me in developing my thesis. I deeply appreciate all his contributions of time, ideas, and funding to my research, as well as his guidance in my academic pursuits. He encouraged me to pursue interesting research ideas with strong theoretical contributions. His dedication and passion for rigorous research were deeply motivational for me and kept me going even during tough times in the Ph.D. journey.

I am deeply indebted to my supervisor, Prof. Jiang (Zhenhui) Jack, who started me on my Ph.D. journey. I appreciate all his contributions of time, ideas, and funding to my research, without which, this thesis would not have been possible. He always challenges me with tough questions and motivates me to improve the quality of my work. He has been extremely gracious and understanding of my circumstances. I am thankful for the excellent example he has provided as a diligent, rigorous, and humble researcher.

I would also like to thank my committee members Professor Tan Chuan Hoo, Professor Jin Chen, and Professor Lim Shi Ying for their insightful comments, as well as their feedback at every stage of my thesis. Their feedback helped me position my research and motivated me to ponder better ways to deliver my research.

I also received help from faculty in the Department of Information Systems and Analytics, who have shared with us their knowledge and views on IS research in various research seminars. I am grateful to Dr. Lu Weiquan, who helped me develop my skills as an independent researcher.

Lastly, I would like to thank my family for their patience and support. For my parents who encouraged my academic aspirations. For my younger siblings who kept me motivated, knowing the example that I will be setting for them. For the unconditional love and encouragement of my wife. To them, I dedicate this thesis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1 INTRODUCTION

1.1 BACKGROUND AND MOTIVATION

Privacy was first identified by Mason (1986) as one of the 4 ethical issues of the information age. As information becomes increasingly important to both government and corporations in decision-making, these public and private entities will seek avenues to obtain such information even at the expense of invading another's privacy (Mason 1986; Zuboff 2019).

One of the key growth areas in information technology that threatens privacy is the enhanced capacity for surveillance (Mason 1986). Surveillance technology poses a particularly salient threat to privacy is since it allows a surveillant to observe that which a subject does not wish to be observed (Kearns 1998).

Surveillance technology proponents have made the case for its implementation in various contexts, such as progress towards efficient administration within large-scale bureaucratic organizations (Lyon 2008), employee safety and security within the workplace (Watkins Allen et al. 2007), increased physical security of people and property within a law enforcement context (Clarke 1988), and for the provision of deterrence and information to understand and prevent terrorist acts within a national security context (Reddick et al. 2015). However, critics have claimed that surveillance technology is sweeping up massive amounts of data without evidence of the technologies being effective in improving security (Cayford and Pieters 2018).

Despite this claim, the effectiveness of surveillance technology has been discussed in various contexts such as government surveillance (Cayford and Pieters 2018) transportation networks (Li and Ouyang 2012), pandemic control (Ng et al. 2020), and deterrence of deviant behaviors (Doumbouya et al. 2017). However, to the best of our knowledge, these effectiveness studies in the current surveillance literature have been contextual in nature, meaning that surveillance efforts, rather than surveillance technology, have been at the core of these studies.

Additionally, much of the debate that pertains to the tension between privacy and surveillance has been argued from a legal (Friedman and Reed 2007) or ethical (Fairweather 1999) perspective. As such, these discussions on the privacy-surveillance tradeoff rarely go beyond the rhetoric. Empirical studies conducted on the other hand, have been inconclusive with regards to how the tradeoff could be addressed to improve outcomes. Dinev et al. (2008) found that US respondents recognized the need for surveillance in general but raise concerns when surveillance might apply to them individually. The researchers noted that the resolution to this conflict was unclear. This was echoed in Cayford et al. (2019)'s finding that 'the public does not engage in trade-offs between the different (security and privacy) values involved, but rather, wants it all.'

Our thesis seeks a resolution to the said conflict by empirically investigating the IT artifacts central to the privacy-surveillance tradeoff in terms of their effectiveness in achieving both surveillance and privacy objectives. In centering this thesis around surveillance technology itself, we also respond to Benbasat and Zmud (2003)'s call to return to the IT artifact. This thesis comprises two studies: Study One explores the impact of surveillance technology on consumer behavior in an unmanned retail environment, and Study Two examines the effectiveness of privacy-preserving designs applied to digital contact tracing in a public health surveillance context.

In Study One, by investigating the impact of surveillance technology on behavioral outcomes, we hope to better understand if surveillance technologies live up to promises of delivering better security as well as their impact on economic outcomes. Specifically, in Study One, the objective of surveillance is the deterrence of theft, this is measured by theft rate. One of the objectives of privacy is to ensure that potential customers feel safe to approach and purchase from the unmanned retail stand, this is measured by approach and conversion rate. Hence, Study One shows how implementing surveillance technologies might have conflicting impact on surveillance and privacy, as measured by theft rate and approach/conversion rate.

In Study Two, we consider the practicality of surveillance technologies that aim to achieve surveillance objectives while preserving the privacy of its users by investigating the impact of privacy-preserving designs on user behavior. Specifically, in Study Two, we explore how the privacy-surveillance tradeoff might be mitigated through privacy-preserving design. That is, how system owners might be able to continue to benefit from the information obtained from surveillance technologies while mitigating privacy risks through the implementation of privacy-preserving features.

Taken together, this thesis explores the effectiveness of surveillance technologies as an avenue to better inform the privacy-surveillance tradeoff discussion.

The next two subsections will provide a more detailed, albeit high-level, overview of the two studies, including an overview of the study context and the general motivations, highlighting the growing impact of surveillance technology has on our lives.

1.1.1 Impact of Surveillance Technology on User Behaviors

Surveillance refers to any collection and processing of personal data, whether identifiable or not, for purposes of influencing or managing those whose data have been garnered (Dinev et al. 2008; Lyon 2001). George Orwell's depiction of Big Brother, the leader of the fictional totalitarian state Oceania, in his novel 1984, is perhaps the most widely used metaphor in the discussion of surveillance and information privacy (Solove 2004). While the metaphor is an incomplete representation of the information privacy problem in the modern context of dataveillance, the maxim ubiquitously on display across Oceania “BIG BROTHER IS WATCHING YOU” certainly captures the psychological impact that surveillance has on surveilled subjects.

A modern-day example of the adoption of surveillance technologies is the marked and sustained growth in the use of CCTVs to prevent crime in public places around the world, which resulted in a significant decrease in crime (Welsh and Farrington 2009). Another example is public health surveillance through the implementation of digital contact-tracing technologies. Both examples collect and process personal data (of different forms) for the purpose of managing those whose data have been garnered.

Researchers have argued about the social benefits and risks of surveillance – that is, about the Janus-like nature of surveillance in that it is both necessary and risky (Lyon 2001). For example, while people usually appreciate the sense of increased security brought about by video surveillance, they often fear the simultaneous loss of privacy. This legitimate concern often slows down the deployment of video surveillance (Dufaux et al. 2006). On one hand, surveillance can play an important role in ensuring the safety of the public’s activities and transactions (Dinev et al. 2006a). Dinev et al. (2008) pointed out the perceived beneficial component of surveillance makes users welcome it as a needed practice that will result in a variety of benefits such as security, social order, convenience, and ease. On the other hand, there is a growing consensus that surveillance systems pose a threat to privacy (Moncrieff et al. 2009) that should be debated and, ultimately, mitigated by legislative action (Lucky 2008). The very possibility of covert surveillance increases the information asymmetry between the surveillant and the surveilled. This increases the perceived risk that access and possible abuse of the private information obtained by the surveillant may occur (Dinev et al. 2008).

In Study One, we explore the impact of surveillance technology on behavioral outcomes in the context of an unmanned retail environment. We measure behavioral outcomes such as theft rate, customer approach rate, and sales conversion rates, which not only shed light on user behavior but also serve to further the discussion on the tradeoffs between social benefits and risks of surveillance (Dinev et al. 2006a; Lyon 2001).

1.1.2 Impact of Privacy-preserving Design on User Behaviors

The threat posed by surveillance to privacy is aptly summarized by a statement made by the Canadian supreme court, 'one can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance' (Taylor 2002). However, Cappello (2019) argued that the "all-or-nothing" character of the public debates on the trade-offs between surveillance and privacy had framed the problem incorrectly. Instead of forcing a choice between security and privacy, Cappello (2019) argued that the focus should have been on how privacy could be protected while simultaneously pursuing surveillance objectives such as security and corporate efficiency.

A report commissioned by The European Commission and undertaken by London Economics (2010) proposed that researchers should develop privacy protection methods in conjunction with advances in surveillance technology and that such methods should aim to maximize privacy while retaining the surveillance system's purpose. As such, a more explicit role for "privacy by design" had been considered in a review of the information privacy-related legislation in the European Union (London Economics 2010).

Designers have responded to this call by applying "privacy by design" principles to surveillance technologies such as CCTVs (London Economics 2010), and more recently, digital contact tracing (Bay et al. 2020). Sutanto et al. (2013) had validated a privacy-preserving architectural design in a digital marketing context. However, to the best of our knowledge, we found little research in a surveillance context that measures the impact of these design features on user behavioral outcomes. Hence, we explore the counterbalancing impact of implementing “privacy by design” into surveillance technology. An opportunity to conduct such a study was provided by the recent COVID-19 outbreak.

The recent COVID-19 pandemic was a global public health crisis that has urged governments and health authorities to take proactive actions to manage its outbreak, including work-from-home policies, social distancing, and even mandatory lockdowns. As pointed out by Rai (2020), from an IS perspective, a foundational aspect for a proactive strategy is a robust real-time public health surveillance system. Thus, the roll-out of digital contact tracing (DCT) by governments and Big Tech (Ahmed et al. 2020) can be understood as a supplement to current public health surveillance systems. Accordingly, information privacy concerns related to early implementations of DCT technologies have been thrust to the forefront of discussion (Li et al. 2020; WHO 2020). In response, technologists and app designers have come up with innovative solutions such as privacy-preserving features in terms of relative location data collection and decentralized data location storage for DCT technologies.

Hence, Study Two explores the impact of privacy-preserving features on user behavior in the context of COVID-19 digital contact tracing. We collect responses from subjects exposed to two different privacy-preserving features designed into a digital contact tracing app. We measure the perceived risk reduction associated with the implementation of these privacy-preserving features. We take an extended privacy calculus perspective to understand the risk-benefit tradeoff being considered by subjects concerning adoption.

1.2 RESEARCH FOCUS AND CONTRIBUTIONS

This thesis explores two aspects of surveillance from an IS perspective. Study One explores the impact of surveillance technology itself on behavioral outcomes, which reflect the perceived risks and benefits associated with the potential privacy invasion and security enhancement derived from the surveillance technology. Study Two focuses on potential mitigators to the perceived risks in the form of privacy-preserving design. By identifying what is lacking in the current literature, this thesis proposes frameworks to evaluate surveillance technology and privacy-preserving designs. Taken together, these two studies aim to uncover *if* and *how* surveillance technology should be implemented, given its strong privacy implications. This thesis contributes to existing surveillance literature by focusing on the surveillance artifact itself, instead of being limited to surveillance programs in the workplace (Ball 2010; D'Urso 2006; Watkins Allen et al. 2007) or government (Dinev et al. 2006a; Dinev et al. 2008; Reddick et al. 2015) contexts. The following two subsections discuss the contributions of the two studies individually.

1.2.1 Study I: Impact of Surveillance Technology in Unmanned Retail Environments

Study One studies the impact of surveillance technology in the context of an unmanned retail environment. It identifies and fills two research gaps in the current literature. First, while there is existing literature discussing the impact of surveillance on privacy, the discussion usually focuses on the societal level impact (Campbell and Carlson 2002; Moncrieff et al. 2009; Taylor 2002) or impact on the workplace (Ball 2010; Watkins Allen et al. 2007). This study attempts to quantify the individual level benefit of surveillance technology by measuring its impact on deviant behaviors such as the theft rate of individual retail shelves. We collect our empirical observations in an unmanned retail environment, which disentangles the impact of surveillance technology from other potential factors that may deter such deviant behavior. To the best of our knowledge, there has not been much empirical research with regards to surveillance on consumers evident in the IS literature (Dinev et al. 2006a). Second, we provide a framework to quantitatively evaluate surveillance technology from a tradeoff perspective. While past literature has often discussed the social benefits and risks of surveillance technology, the discussions are generally expository or anecdotal in nature (Campbell and Carlson 2002; Moncrieff et al. 2009; Taylor 2002). We extend the discussion on surveillance technology by evaluating the tradeoffs between positive impacts such as theft rate reduction and negative impacts such as customer approach rate and sales conversion rate reduction.

1.2.2 Study II: Digital Contact Tracing and Privacy-preserving Features

Study Two examines the effect of privacy-preserving features on user behaviors in the context of COVID-19 digital contact tracing. It makes the following contributions to the current literature. First, the existing literature focuses more on the individual characteristics (e.g., privacy self-efficacy) (Schade et al. 2018; Wang et al. 2017), contextual factors (e.g., compensation and regulation) (Kummer et al. 2018; Xu et al. 2011), cognitive and affective factors (e.g., perceived control and trust) (Dinev et al. 2016; Jiang et al. 2013; Shaw and Sergueeva 2019) as antecedents of privacy calculus. In comparison, there has not been much research on specific design features evident in the IS literature to the best of our knowledge. By examining the effect of privacy-preserving features, we fill this research gap. Second, the current privacy calculus literature mostly examined personal benefit, since it is a model primarily designed to understand individual's decision processes with regards to the disclosure of personal information required to complete a transaction (Dinev and Hart 2006). As such, benefits beyond personal benefit are rarely, if ever, considered. The COVID-19 public health crisis provides a unique context whereby public health authorities have called on ordinary citizens to make personal sacrifices to help contain the outbreak and keep the community safe (Fairchild et al. 2020). In the context of digital contact tracing, this means giving up personal information to help track infection clusters. Hence, we extend the current literature by considering the impact of community benefit in addition to personal benefit in the privacy calculus model. Third, we contribute to the literature of privacy-preserving design. Specifically, although there exists an objective tradeoff between privacy-preservation and functionalities such as accuracy and efficiency, we posit that this tradeoff is perceived differently for different types of users. For example, while technically inclined personnel might notice the marginal decrease in accuracy and efficiency, the general population might not perceive the decrease, even if the decrease did objectively occur. Hence, it is important to determine in the initial stages of the design process whether the goal is to maximize perceived or actual benefits. In addition, designers should be aware that benefits might not be perceived uniformly across demographics.

1.3 THESIS ORGANIZATION

The opening chapter has provided an overview of the study context and the general motivations based on the current research gaps. It highlights the importance of surveillance technology to modern life and raises the research questions that will be addressed in the studies as well as the potential contributions. The subsequent chapters of the thesis are organized as follows.

Chapter 2 describes Study One in detail. It first reviews the literature on surveillance, deterrence, assurance, and social presence. It then presents the hypotheses and compares the impact of formal and informal surveillance on behavioral outcomes. A 2×2 field experiment is conducted to test the proposed hypotheses. Discussions and implications are then reported.

Chapter 3 describes Study Two in detail. It first reviews the literature on privacy calculus and privacy preservation features, identifying the specific gaps in the literature. It then presents the hypotheses on the individual and joint impacts of two privacy-preserving features and existing user base on users' usage intentions for a digital contact tracing app. A 2×2×2 experiment is conducted to test the hypotheses. Discussions and implications are then reported.

Chapter 4 concludes this thesis by summarizing the findings and implications of the two studies, followed by a discussion of potential future research directions.

CHAPTER 2 STUDY I: WILL THEY STILL PAY? A STUDY OF CONSUMER BEHAVIOR IN AN UNMANNED RETAIL ENVIRONMENT

2.1 INTRODUCTION

Unmanned retail is a new retail format that has gained rapid interest amongst investors and technology companies. Its recent adoption by consumers had been made possible primarily by the proliferation of smartphones, mobile payments, and related technologies. The concept of unmanned retail has existed since the 19th century in the form of vending machines (Chandler et al. 2009). In the early 1990s, technologies such as barcode scanners and credit card payments have updated the format with the introduction of self-service checkouts in supermarkets, thereby reducing the number of staff required to man checkout counters. More recently, by integrating computer vision and deep learning on top of mobile internet and digital payments, retailers have managed to further automate the checkout process to the extent that onsite staff headcount can be reduced to the minimum. AmazonGo, one of the most high-profile examples, requires shoppers to only use a smartphone app to enter the store, and then walk out without stopping at a cash register. The unmanned checkout process relies on sensors and computer-vision technology to detect what the shoppers take and bill them automatically.

Beyond entire brick-and-mortar stores, there have also been other updated interpretations of unmanned retail concepts. Chinese technology companies such as Jing Dong have deployed unmanned vending shelf solutions (Lee 2017) which work like glorified vending machines that accept digital payment through either smartphones or facial recognition. This not only provides convenience to consumers, since cash is no longer required to purchase merchandise from the vending shelves, but also allows the retailer to match merchandise sales to each individual consumer. This customer surveillance allows the retailer to better understand the purchase habits of their customers while subjecting said customers to potential privacy risks.

Another Chinese technology company, Xingbianli, has deployed regular retail shelves that accept digital payments through a QR code. Also referred to as unmanned retail shelves, users can purchase snacks and beverages easily from these shelves through self-service and mobile payment. Unmanned retail shelves are inexpensive and can be quickly deployed since they do not require additional equipment such as gantry systems or facial recognition systems. This advantage allows startups such as Xingbianli to swiftly expand and compete against more established competitors such as Jing Dong.

However, the lack of a gantry system at unmanned retail shelf locations also means that potential customers can enter and exit the vicinity of the retail shelf with no restraint. With neither gantry systems nor onsite staff, unmanned retail shelves are left with no physical deterrents to deviant behavior such as theft. The lack of onsite staff also means an absence of customer service, thus removing a potential source of purchase stimulus. This could result in reduced sales conversion.

Higher opportunities for theft of merchandise due to the absence of surveillance by onsite staff, as well as a less pleasant shopping experience due to the lack of human interaction, are two major issues with unmanned retail shelf concepts. These two issues are highly relevant to retailers since they directly impact the profit generated by the retail shelf. For example, an incident of theft would represent a potential loss to the retailer since no revenue is generated on the goods that were stolen, resulting in a net loss. A lack of human interaction might lead to reduced revenues since human interaction such as customer service acts as a purchase stimulus by facilitating purchase decisions, whether it be answering specific questions about the merchandise or providing transaction security assurance for potential customers.

Both issues mentioned above directly result from the removal of onsite staff, since responsibilities such as checkout, customer service, and theft deterrence in traditional retail are fulfilled by onsite staff. However, since the reduction in onsite personnel cost was precisely why unmanned retail could have a cost advantage over traditional retail, simply reinstating onsite staff would defeat the purpose of adopting unmanned retail shelves in the first place. Therefore, we seek low-cost technological interventions to fulfill the responsibilities originally undertaken by onsite staff. To theorize how these technological interventions might deter theft behavior, we utilize the theory of Crime Prevention through Environmental Design (CPTED).

Hence, this study plans to measure the impact of low-cost technological interventions on our three dependent variables, theft rate, approach rate, and conversion rate to answer our research question as follows:

RQ: how would surveillance technology impact consumer behavior in an unmanned retail environment?

To directly deter potential deviant behavior, we identify CCTV as a possible option. CCTV is considered a form of **formal surveillance** under the CPTED framework, which aims to produce a direct deterrent threat to potential offenders (Lindblom and Kajalo 2011). The rapid reduction in the cost of CCTV surveillance cameras in addition to their ability to record any deviant behavior for future use by law enforcers makes it an ideal potential deterrent.

To counter the absence of customer service staff and indirectly discourage deviant behavior, we identify sensor greeting bells as a form of low-cost technology that could improve the shopping experience. A sensor greeting bell that plays a greeting message as a customer enters the vicinity of the retail shelf helps aurally simulate the simplest form of customer service – greeting the customer as he or she enters. By fostering positive social interaction and control, the sensor greeting bell could be considered as a form of **informal surveillance** under the CPTED framework (Lindblom and Kajalo 2011).

Thus, the two technological interventions, CCTV surveillance, and sensor greeting bells were chosen as our independent variables. We attempt to study the impact of these technological interventions on consumer behaviors in a retail environment that no longer includes onsite retail staff and cashiers as the default, as well as the extent that these technologies can fill the gap in manpower caused by the move towards an unmanned retail environment. Specifically, we are interested in finding out how these technological interventions perform as theft deterrents and purchase stimulants.

We measure theft rate, as this reflects the probability of shoplifting, which is what we seek to reduce in an unmanned retail setting through surveillance technologies. We measure approach rate, which reflects the probability of a subject walking by interacting with the shelf. Finally, we measure conversion rate, which reflects the probability of a subject paying for the merchandise. Both approach rate and conversion rate are important measures since they directly impact the sales generated by an unmanned retail shelf. Ideally, our two technological interventions should reduce theft rate, but not approach rate and conversion rate. However, this may not be the case due to potential privacy concerns resulting from the implementation of the two technological interventions.

By measuring the main effects and interaction effects of CCTV and sensor greeting bells on not just theft rate, but also approach and conversion rate, we developed a framework to evaluate the overall economic impact of implementing formal (CCTV) and informal (sensor greeting bells) surveillance. This framework can be applied during the design of future retail systems to specify the combination of technological interventions to improve economic outcomes for the retail system.

2.2 LITERATURE REVIEW

In this section, we develop our theoretical perspective on the underlying mechanisms driving the relationships between the independent and dependent variables in the context of unmanned retail. Firstly, with regards to customer theft rate, we begin by reviewing deterrence theory to understand the mechanisms underlying retail theft prevention. We then discuss ‘Crime Prevention through Environmental Design’ (CPTED), which provides us the framework with which to understand the deterrent qualities of our two independent variables, CCTV surveillance and sensor greeting bells. We then turn to CCTV surveillance related literature theory, to explore the psychological rationale behind how a technological artifact can effectively replace the function of a human staff for a surveillance task. Secondly, with regards to customer approach rate, we draw from information privacy literature to understand the impact of our technological interventions on the willingness of potential customers to approach the unmanned retail shelf from a privacy risk perspective. Thirdly, with regards to customer conversion rate, we apply assurance theory and social presence theory to understand the impact of these technological interventions on trusting intentions, perceived security risk, and correspondingly, purchase intentions and customer conversion rate.

2.2.1 Deterrence Theory

Deterrence theory applies a utilitarian philosophy to crime (Akers 1990) by assuming that individuals evaluate the costs and benefits associated with a situation, and then make rational decisions based on increasing pleasure (e.g., benefits) and decreasing pain (e.g., risks/costs) (Dootson et al. 2017). Kennedy (1983) defined deterrence as the “control or alteration of present and future criminal behavior which is affected by fear of adverse extrinsic consequences resulting from that behavior.”

The 18th-century founder of utilitarianism, Jeremy Bentham, was convinced that crime rose from the conscious, rational considerations of the individual (Andenaes 1974). Accordingly, a person contemplating unlawful behavior would undertake a cost-benefit analysis and would execute the act only if potential benefits sufficiently outweighed expected costs. It can then be argued that it is possible to influence the outcome of the cost-benefit analysis and deter the execution of the act by sufficiently increasing the perceived risks associated with unlawful behavior. Under this argument, the task of law enforcement personnel and lawmakers is clear: deterrents must be put in place through policies such that the risks, or costs, for a potential violator had to be so great that he would have far more to lose than to gain from unlawful behavior.

Bentham believed that the rate of commission of a particular offense varies inversely with the celerity, certainty, and severity of punishment for that crime (Gibbs 1968). Silberman (1976) noted that ‘studies on the effects of certainty and severity of punishment on crime rates consistently describe weak, although significant, negative association between certainty of punishment and crime rates.’

We can also infer from previously observed significant negative associations between the certainty of punishment and crime rate (Silberman 1976) that actors are deterred by potential punishment. It means that a potential violator would seek to avoid punishment, leading him or her to process the situation to search for perceived opportunities (with lower certainty of punishment) to commit theft or violence before simply acting. Perceived opportunities for crime commission are directly measured by the chances of which the violator could both commit a crime and escape punishment successfully. The extension of this logic would mean that the perceived perfect opportunity for crime commission would be a scenario where the violator has a 100% chance of escaping punishment. Indeed, Matsueda et al. (2006) found that for both theft and violence, a higher perceived chance of success at both commission and escaping punishment will substantially increase the likelihood of occurrence.

This study focuses on unmanned retail environments, which, in the process of replacing human cashiers with mobile payment technologies, have removed a major deterrent to theft from the retail shelf. The absence of a human cashier means that there is a much lower certainty of punishment for the potential violator since there is no one on site to observe, identify, and apprehend him or her. It follows that this reduced certainty of punishment leads to an increased perceived opportunity to commit theft and get away with it. This also explains why current unmanned retail shelf models suffer from extremely high levels of theft.

2.2.2 CPTED Framework

CPTED draws on ideas that argue that it is possible to use the built urban form to reduce opportunities for crime (Cozens and Love 2015). In *Defensible Space: Crime Prevention through Urban Design*, Newman (1973) argued that the environmental design of the buildings was a causal factor explaining the differing crime rates between two housing projects in New York that were compared and analyzed together with recorded crime rates.

Newman (1972) developed his hierarchy of defensible space, which is, in turn, made up of four design elements, territoriality, surveillance, image and milieu, and geographical juxtaposition (environment), which act individually and in combination to help create a safer urban environment. In our study, we focus on one of the four design elements of CPTED – surveillance. Surveillance refers to the capacity of the built form to provide opportunities for surveillance for residents and others using the building configuration and the design and placement of windows and building entrances (Cozens and Love 2015). Within the CPTED framework, surveillance can be further separated into formal and informal surveillance methods (Moffatt 1983).

Formal surveillance aims to produce a direct deterrent threat to potential offenders through the deployment of personnel whose primary responsibility is ensuring security (e.g., police, security patrols), or through the introduction of some form of surveillance technology, such as CCTV (Cozens and Love 2015; Reynald and Elffers 2009; Welsh and Farrington 2004). The presence of these interventions also presents the potential for action either immediately through active enforcement by security personnel; or by recourse, through collecting evidence from analyzing CCTV recordings.

The very active and visible way that CCTV systems exercise surveillance makes it a form of formal surveillance since subjects will know explicitly that they are under observation and that there is a high risk that they may be caught if they commit a crime (Kajalo and Lindblom 2016). In fact, CCTV surveillance systems are a very popular form of formal surveillance. Retail chains have been installing CCTV surveillance systems as part of increased spending on retail security (Yaniv 2009). It can be argued that investments in formal surveillance may be necessary to combat shoplifting, but at the same time, there is a major concern that these investments may make honest consumers feel less secure (Cox et al. 1993; Guffey et al. 1979; Overstreet and Clodfelter 1995). For example, a survey by Lin et al. (1994) found that formal surveillance devices were perceived to increase shoppers' sense of environmental hostility within the store. Another potential explanation could be an increase in perceived privacy threat due to the ability of surveillance equipment to invade individuals' privacy (Kearns 1998).

Informal surveillance indirectly deters crime by capitalizing upon the ‘natural’ surveillance provided by people going about their everyday business (Welsh and Farrington 2004). Informal surveillance is promoted by physical features and activities in a way that maximizes visibility and fosters positive social control. Some practical implementations include keeping stores well-lit and fostering positive social interaction between sales staff and customers (Lindblom and Kajalo 2011). By increasing subjects’ perception that they can be seen, a technological intervention would increase the subjects’ perceived apprehension risk and certainty of punishment. By fostering positive social control, it would increase the perceived seriousness of committing a crime, which could, in turn, increase the expected severity of punishment. Thus, even if a technological intervention’s primary goal is not surveillance, it could still have the desired effect of deterring crime through informal surveillance. Accordingly, even though the primary goal of a sensor greeting bell is not surveillance, by being ‘natural’ and fostering positive social control, it would be acting as a form of informal surveillance, thereby deterring crime.

Reynald and Elffers (2009) highlight social control as a crucial part of informal surveillance. Social control is the willingness of sales staff to be vigilant in preventing deviant behavior in the store environment. Nugier et al. (2007) define social control as any verbal or non-verbal communication by which individuals show disapproval of deviant (counter normative) behavior. Social control impacts deviant behavior by pressuring potential violators to abide more closely to societal norms. Under such a mental state, potential violators would assume a lower tolerance for deviant behavior, thereby increasing the expected severity of punishment should he or she proceed. In practice, social control in the store environment can be enhanced by bringing better-trained sales staff to the floor and fostering positive social interaction between sales staff and customers (Kajalo and Lindblom 2016; Reynald and Elffers 2009). Customer service provided professionally by sales staff to the floor will signal to customers that they are a part of a lawful and orderly shopping environment. Since deviant behavior would feel even more conspicuous in such an environment, this would heighten the subject's awareness of potential legal repercussions for even a petty crime such as shoplifting, which in turn increases their expected severity of punishment, thereby deterring them from any deviant behavior. Following this logic, the greeting message that would be played by our sensor greeting bells would simulate the initial social interaction between onsite staff and customers. This could foster social control even if there is no actual onsite staff.

In summary, our study is primarily interested in the impact of two technological interventions, CCTV surveillance, and sensor greeting bells, on consumer behavior in an unmanned retail environment. The deterrent qualities of these two technological interventions can be classified under formal and informal surveillance respectively within the CPTED framework as described above.

2.2.3 CCTV Surveillance

To better understand how CCTV surveillance technology influences subjects, we look into Foucault (1977)'s work on governmentality and disciplinary practice, which relies on the 'Panopticon' in depicting surveillance in society. The Panopticon has since been often invoked when discussing the theoretical and social significance of CCTVs in modern society (Norris 2005).

The Panopticon, designed by Bentham in the eighteenth century (Koskela 2000), is a model prison that utilizes an optical-mechanical technique that enables an unseen observer to observe any inmate in prison cells on the periphery of a circular building. Consequently, while it is still physically impossible for a single observer to observe all prison cells at once, the inmates are always, potentially, under the gaze of a warden in the central tower (Driver 1985). The spread of the CCTV has been described as the dispersal of an ‘electronic panopticon’. CCTVs, like Bentham’s Panopticon, presents power to the observed in a form that is ‘visible and unverifiable’ (Fyfe and Bannister 1996).

Visibility of the central tower refers to the fact that just as any inmate can see the central tower from which he is being spied upon at all times, so too anybody in a city with CCTVs deployed can see the cameras overhead and street signs proclaiming their presence. Unverifiability refers to the fact that inmates never know whether they are being observed at any moment, but are aware that they may always be so, just as anyone within the coverage of CCTV would never know if security personnel in the control room are looking at them at a given moment, but may always be so.

Visibility and unverifiability lie at the heart of how the surveillance gaze in Bentham’s Panopticon can effectively fulfill its purpose and control its subjects. Foucault had observed that the Panopticon’s main purpose is **“to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power”.** The CCTV, like Bentham’s Panopticon, is particularly effective at exerting surveillance as the CCTV is also a mechanism that 'automatizes and disindividualizes power' (Foucault 1977). This mechanism could cause subjects to enter a state of perceived constant surveillance. This state of perceived constant surveillance within the subject causes the CCTV’s role as a crime deterrent to always be functional, even when the individual is not consciously aware of the CCTV. Both CCTV proponents and Bentham claim that the result of such intensive surveillance is the deterrence of unlawful behavior through the possibility of rapid intervention at any moment.

Koskela (2000) observed that panoptic surveillance can be so effective such that there is no need for physical intervention. As Foucault (1980) puts it: ‘There is no need for arms, physical violence, material constraints. Just a gaze.' Being constantly aware of being controlled by invisible overseers leads to the internalization of control. While the Panopticon seemingly works by keeping the body entrapped, it is in fact targeted at the psyche. It is this control of the subject's psyche, that results in effective physical control. When successful, subjects regulate their behavior even when seemingly unnecessary due to the creation of a bad conscience within them. They became subject to this bad conscience, which effectively exercises power over their physical selves. The panoptic condition of video surveillance imposes self-vigilance. This internalization of control then results in an easy and effective exercise of power (Foucault 1980).

It is this proposition regarding the effectiveness of the panoptic surveillance put forth by Foucault that we seek to validate as part of our study on the impact of technological interventions on consumer behavior in an unmanned retail environment.

2.2.4 Technology and Privacy Concerns

Clarke (1999) identified four dimensions of privacy: privacy of a person, personal behavior privacy, personal communication privacy, and personal data privacy. Today, as most communications are digitized and stored as information, personal communication privacy and data privacy can be merged into the construct of information privacy (Bélanger and Crossler 2011).

Most studies have used one of two instruments to measure privacy concerns: concern for information privacy (CFIP) or internet user's information privacy concerns (IUIPC). Smith et al. (1996)'s CFIP construct identified four dimensions of information privacy: collection, unauthorized secondary use, improper access, and errors. A few years later, the IUIPC construct adopted the CFIP in the internet context and included three dimensions: control, awareness, and collection (Malhotra et al. 2004). IUIPC can be conceptualized as the degree to which a user is concerned about marketers' collection of personal information, the user's control over the collected information, and the user's awareness of how the collected information is used.

Information technology is driving many concerns (and some solutions) related to information privacy. Advances in the technical capabilities to collect, store and search large quantities of data concerning phone conversations, internet searches, emails, and location history, etc., have led to concerns about seemingly unbounded options for collecting, processing, distributing, and using personal information (Smith et al. 2011). Specifically, with the advent of advanced information and communications technologies, data can be collected, aggregated, and analyzed at a faster pace and in a larger volume than ever (Malhotra et al. 2004). Further, data can be collected without individuals' awareness (Soliman et al. 2006). This evolution has led to the emergence of data-centric business models, as exemplified by Big Tech (Google, Amazon, Facebook, Microsoft, Apple) and described in detail by Zuboff (2019) under the label "surveillance capitalism".

Surveillance technology invokes privacy concerns perhaps more directly than any other type of technology because surveillance equipment, by its very nature, is designed to enable a surveillant to observe that which the subject does not want to be observed (Kearns 1998). Furthermore, although privacy concerns stemming from surveillance activity traditionally involve government intrusion, private actors increasingly have access to surveillance equipment and the ability to invade individuals' privacy (Kearns 1998). Hence, we would expect that privacy concerns pertaining to surveillance technology would impact how consumers choose to interact with the unmanned retail shelves. For example, consumers could choose to avoid interacting with the unmanned retail shelves altogether due to privacy concerns caused by the presence of surveillance technology.

By definition, the surveillance technology discussed in the previous paragraphs would be classified under formal surveillance within the CPTED framework. Informal surveillance, by its definition, utilizes 'natural' aspects that would be much less likely to invoke privacy concerns.

2.2.5 Assurance Theory

Assurance implies a situation in which security is sound and the system provides trust and confidence in the organization's security and privacy practices (Spears et al. 2013). In a retail context, where assurance is geared towards winning consumer trust (Ray et al. 2011), the perception of the effectiveness of measures is as important as the actual effectiveness of the measures. In these specific contexts, assurance can be achieved through the implementation of safety nets such as legal recourse, guarantees, and regulations (McKnight et al. 1998; Shapiro 1987; Zucker 1986).

A key aspect of assurance is taking (and showing to take) measures to address all known vulnerabilities, either by removing them or counteracting them through various security tools and techniques (Flechais et al. 2005). An example of such a technique used in assurance is guarantees built into websites, such as a 1-800 number (Gefen 1997). The purpose of security tools and techniques employed by online service providers is not only to provide security, but it is also often argued that the very presence of security tools and artifacts is a form of assurance that promotes trusting beliefs in users (Nöteberg et al. 1999).

This impact of assurance on trusting beliefs is critical as establishing trust is one of the key challenges facing retail firms attempting to convert visitors to buyers. According to the conceptual framework developed by Schlosser et al. (2006), trusting intention is the behavioral aspect of trust that follows trusting beliefs, which is the cognitive aspect. To the extent that consumers are concerned about the risks of purchasing within an unmanned retail context through mobile payment, trusting intentions will impact purchase intentions and therefore conversion rate. For example, the unmanned nature of unmanned retail shelves could give rise to potential transaction security concerns such as disputes as to whether a subject took more merchandise than what he or she had paid for. Another potential concern could be acts of vandalism on the merchandise itself. As unmanned retail shelves primarily offer snacks and beverages, acts of vandalism could potentially have disastrous consequences. For example, consuming a beverage that was tampered with could threaten the physical well-being of the consumer. Through the CCTV, which provides an accurate video record of all interactions with the unmanned retail shelf, assurance can be achieved. This would mitigate the transaction and merchandise related concerns discussed above.

2.2.6 Social Presence Theory

Social presence refers to the degree to which a medium allows a user to establish a personal connection with other users (Short et al. 1976). It represents the capability of a medium to allow a user to experience others as being psychologically present (Fulk et al. 1987). Studies have identified the important role of social presence in the context of Internet shopping. For example, Gefen and Straub (2003) have found that social presence enhances consumers' trust, which in turn influences their purchase intentions.

Typically, trust is built gradually through extensive ongoing interpersonal interactions that enable individuals to create reliable expectations of what other persons or organizations may do (Blau 1964; Luhmann 1979). However, the lack of these interpersonal interactions happens to be a key defining characteristic of e-commerce, as well as unmanned retail. What makes social presence particularly relevant in building consumer trust in our study is its ability to be embedded into retail scenarios even when there is no actual interaction with other people. For example, many websites include pictures of smiling people to convey a sense of personal, sociable, and sensitive human contact (Gefen and Straub 2004). Argo et al. (2005) suggested that the presence of another person may satisfy the customer's need for association, resulting in a decrease in negative emotions when compared to situations where no other individuals were present.

According to Short et al. (1976), social presence is a subjective quality of the communication medium and relates to the social psychology concepts of intimacy (determined by physical distance, eye contact, smiling, and personal topics of conversation) and immediacy (determined by the medium's capacity in transmitting information). Therefore, social presence can be a function of both verbal cues (e.g., tone of voice) and nonverbal cues (e.g., facial expression, direction of gaze, posture, dress). Hence, the welcome greeting generated by the sensor greeting bell when approached by subjects could act as a verbal cue. This could induce social presence within approaching subjects.

2.3 RESEARCH MODEL AND HYPOTHESIS

This study examines the impact of two technological interventions, CCTV surveillance systems, and sensor greeting bells, on consumer behavior in an unmanned retail environment. In an unmanned retail environment, the lack of onsite human staff results in a lack of deterrent to customer theft for the retail shelf. Unmanned retail also results in a reduction of social interaction for customers as there is no longer any onsite staff to interact with. By introducing the two technological interventions, CCTV surveillance and sensor greeting bells, we are interested in the effectiveness of these two technological artifacts to fulfill tasks once performed by onsite staff and evaluate their impact on consumer behaviors. Specifically, the impact of formal and informal surveillance on consumer behavior is investigated in terms of customer theft rate, customer approach rate, and customer conversion rate. We are then able to accurately quantify the overall effectiveness and economic impact of different surveillance setups in an unmanned retail environment.

The deterrent qualities of our two technological interventions, CCTV surveillance systems and sensor greeting bells, fall under the following two classifications, formal surveillance and informal surveillance, as described by the CPTED framework. We expect the CPTED framework and deterrence theory to help explain the impact of the two technological interventions on customer theft rates.

As CCTV surveillance systems record video data of customers once they approach the unmanned retail shelf, this represents a potential information privacy risk. Customers' inability to control potential secondary uses (Bélanger et al. 2002) of this video data will lead to potential information privacy concerns. We expect information privacy concerns to help explain the impact of the two technological interventions on customer approach rate.

Finally, after customers approach the unmanned retail shelf, we expect CCTV surveillance systems and sensor greeting bells to induce different psychological responses, based on the different characteristics of the technological interventions. The different psychological responses induced by these characteristics can be explained by assurance and social presence theory respectively and will have an impact on customer conversion rate.

Figure 2-1 below summarizes our research model. We theorize the main effects of formal and informal surveillance on approach rate, conversion rate, and theft rate, as well as the moderating effects of informal surveillance on formal surveillance.

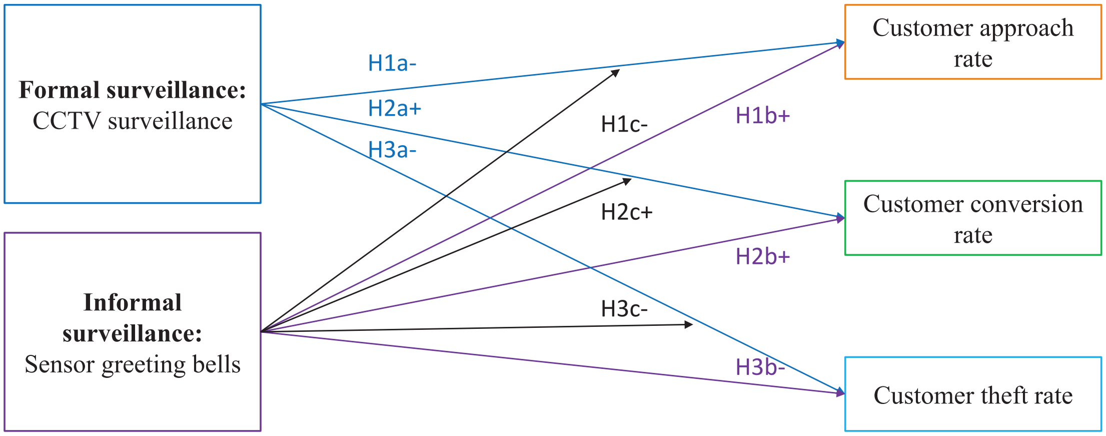


Figure 2-1: Research model

Figure 2-2 below summarizes our theorizing framework. We theorize the main effects of formal and informal surveillance on approach rate, conversion rate, and theft rate, through the theories reviewed such as privacy, assurance, deterrence, CPTED, and social presence.

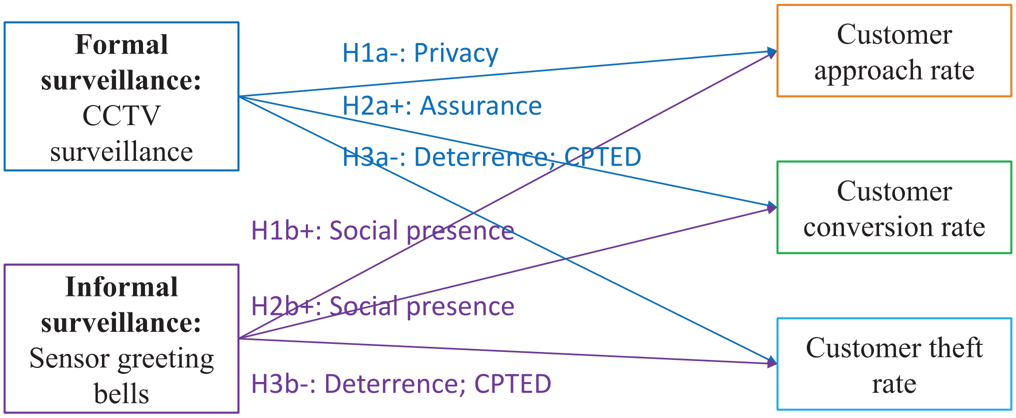


Figure 2-2: Theorizing Framework

2.3.1 Customer Approach Rate

We define the customer approach rate as the ratio of the total number of subjects that approach and display an active interest in the unmanned retail shelf to the total number of subjects that passed by the retail shelf. We categorize subjects who had stopped in front of the retail shelf for more than five seconds as approaching subjects. The customer approach rate reflects the effectiveness of the retail environment in capturing interest from potential customers to interact with the retail shelf. Customer approach rate is an important measure since approaching the retail shelf is an intermediate state for all paying customers.

In our study, CCTV surveillance technology could be a cause for information privacy concerns due to its capabilities to collect and store video data of the subject. In terms of the three IUIPC dimensions, the presence of CCTV cameras indicates to subjects that video data about them will be **collected** once they approach the unmanned retail shelf. Once the video data is collected, the subject has neither **control** over the collected information nor **awareness** of how the collected information is used.

Hence, approaching an unmanned retail shelf equipped with CCTV surveillance technology could expose users to information privacy risks. To avoid exposure to this potential information privacy risk, users might simply choose to not approach these unmanned retail shelves altogether. In doing so, these users can then avoid being recorded by the CCTV camera, thus not risk exposure to information privacy risks. Therefore, we argue that information privacy concerns caused by CCTV cameras would directly impact the customer approach rate of an unmanned retail shelf. Hence, we propose the following:

H1a: The presence of CCTV surveillance is negatively associated with customer approach rate

Compared to CCTV surveillance systems, which record and collect video data, sensor greeting bells do not collect data on a potential customer as he or she approaches it. Since no collection of personal information takes place, sensor greeting bells will not be perceived as a privacy risk by potential customers. Therefore, privacy concerns would not cause customers to avoid an unmanned retail shelf that implements only sensor greeting bells. On the contrary, the greeting message played by the sensor greeting bell when subjects walk by could act as an auditory cue that evokes a sense of social presence within subjects. This social presence could interest potential customers to stop at the retail shelf and further investigate. Hence, we propose the following:

H1b: The presence of sensor greeting bells is positively associated with customer approach rate

As discussed, the presence of sensor greeting bells may evoke a sense of positive social presence through a friendly greeting message. Besides gathering interest from potential customers and encouraging them to investigate, positive social presence may result in a decrease in negative emotions by satisfying subjects' need for association. This decrease could apply to the negative emotions within potential customers caused by the possibility of unauthorized secondary use and improper access to personal information by the retailer. Ultimately, the presence of sensor greeting bells would reduce negative emotions, causing potential customers to be less concerned about the information privacy risk they are exposing themselves to when a CCTV camera is present. This would reduce the information privacy concerns caused by the CCTV camera. Hence, we propose the following:

H1c: The negative effect the presence of CCTV surveillance has on customer approach rate is weaker when sensor greeting bells is also present

2.3.2 Customer Conversion Rate

We define the customer conversion rate as the ratio of the total number of converted customers who paid for goods to the total number of customers that approached the retail shelf. We categorize subjects who had successfully paid for bottled water through WeChat Pay as converted customers. The customer conversion rate reflects the effectiveness of the retail environment in converting potential customers into paying customers. Customer conversion rate is a function of purchase actions by customers at a retail shelf, which in turn reflects the trusting intentions of customers towards the said retail shelf.

Due to the unmanned and novel nature of the retail shelf, there could be greater uncertainty associated with the transaction and merchandise security of unmanned retail shelves. In the case of transaction security, as there are no longer any cashiers present to verify that payment had been made by the customer and received by the retailer, this increases the risk of potential payment disputes. The risk for potential disputes remains even though customers who paid through WeChat Pay would have an electronic record of the payment made. This is because the electronic record only proves that payment was made but does not prove that the customer did not take more items than what he or she paid for. Given the relatively frequent occurrences of theft at unmanned retail shelves, the lack of payment verification could lead to potential disputes and accusations for innocent, paying customers.

In the case of merchandise security, the unmanned nature of the retail shelf could provide opportunities for bad actors to tamper with the merchandise. The risk that the merchandise might have been tampered with could discourage customers from buying and consuming merchandise from the unmanned retail shelf.

To mitigate the increased uncertainty, we investigate how surveillance technology can reduce both types of perceived security risks. We argue that video surveillance can address the increase in perceived security risk through an assurance mechanism. For example, a customer concerned about transaction security risk could choose to complete all transactions in front of the CCTV camera, such that a video record of the transaction is kept. The availability of video records will provide assurance to the customer that transaction disputes can be objectively resolved should they arise, thereby mitigating perceived transaction security risks. The presence of CCTV will also deter bad actors from tampering with the merchandise, thereby mitigating perceived merchandise security risks. Ultimately, the assurance resulting from the presence of the CCTV will mitigate increased uncertainty within customers that is a result of the novel nature of the unmanned retail shelf. The mitigation of this uncertainty will reduce perceived security risks and have a positive impact on purchase intentions and therefore the conversion rate. Hence, we propose that:

H2a: The presence of CCTV surveillance is positively associated with customer conversion rate

When a customer walks by an unmanned retail shelf that has a sensor greeting bell, the motion triggers the sensor greeting bell, causing an audio greeting message to be played. This allows a customer to experience customer service staff as being psychologically present. While this psychological presence is only experienced briefly, we argue that this effect is especially pronounced since social presence is effectively nil at an unmanned retail shelf otherwise. Thus, we expect that the presence of sensor greeting bells at these unmanned retail shelves results in higher levels of social presence. As discussed in the previous section, Gefen and Straub (2003) found in their study that social presence enhances consumer trust. As subjects place greater trust in the retailer, this will help to mitigate the increased uncertainty associated with the novel nature of the unmanned retail shelf. This would then increase the conversion rate. Hence, we propose that:

H2b: The presence of sensor greeting bells is positively associated with customer conversion rate

From a conversion rate and purchase intention perspective, the goal of the retailer is to build consumer trust with respect to the consumer experience. As discussed in the previous section, this is a challenge in unmanned retail as compared to traditional retail due to the lack of interpersonal interaction.

The implementation of sensor greeting bells evokes a social presence that is expected to enhance consumer trust. CCTV surveillance systems, on the other hand, improve consumer trust through an assurance mechanism. As observed by Wood et al. (2006), one of the benefits of surveillance was that citizens could expect their rights to be respected because there were protected by accurate records. As discussed, accurate records could then reduce perceived transaction security risk.

In situations where both CCTV surveillance and sensor greeting bells are implemented, we argue that the triggered greeting message from the sensor greeting bell would help CCTV surveillance provide even stronger assurance that transaction disputes can be objectively resolved. While CCTV surveillance provides assurance that retailers have the data and thus the ability to objectively resolve transaction disputes, it does not assure customers that the retailer will utilize the video data impartially. When sensor greeting bell is also present, the triggered welcome greeting played enhances consumer trust through social presence. This enhanced consumer trust helps assure customers that video data is not only collected but will also be used objectively in the event of a dispute. We argue that this would lead to increased mitigation of perceived transaction security risk and ultimately result in an increase in conversion rate. Hence, we propose the following:

H2c: The positive effect the presence of CCTV surveillance has on customer conversion rate is stronger when sensor greeting bells is also present

2.3.3 Customer Theft Rate

We define the customer theft rate as one minus the ratio of the total number of subjects who paid for goods to the total number of subjects who removed goods from the retail shelf (including both subjects who had and had not paid). We categorize subjects who took merchandise without making payment as thieving subjects. Customer theft presents a significant problem for retailers financially, both in terms of shrinkage costs and required investment in additional retail security. Increases in shoplifting have been attributed to modern retailing practices—for example, open displays and self-service (Bannister 1979; D'Alto 1992), and a retail setting which provides opportunities for shoplifting coupled with low risks of apprehension (Ekblom 1986; Lo 1994; Nelson et al. 1996; Shapland 1995).

An unmanned retail shelf with neither formal nor informal surveillance could represent a modern retail setting with almost zero risk of apprehension. With no onsite staff nor surveillance interventions, there would be neither witnesses nor evidence that could incriminate an offender. According to deterrence theory, this low risk of apprehension would substantially increase the likelihood of theft.

By introducing CCTV surveillance systems, a form of formal surveillance, into the unmanned retail environment, potential shoplifters will find it riskier to commit shop theft since their actions will be captured and recorded by the CCTV. So long as the recorded video data is properly managed, it could be used by law enforcers at any point in the future, either as information used to identify violators or as the evidence required to incriminate suspects. This threat will increase potential violators' perceived apprehension risk, and correspondingly increase perceived certainty of punishment, from near-nil levels. According to deterrence theory, the rate of commission of a particular offense varies inversely with the certainty of punishment for that crime (Gibbs 1968), thus it follows that the implementation of the CCTV would reduce the likelihood of theft. Thus, we propose the following:

H3a: Presence of CCTV surveillance is negatively associated with theft rate

In this study, we also introduced a second technological intervention, which is a sensor greeting bell that triggers a greeting message whenever a subject walks by the unmanned retail shelf. The sensor greeting bell acts as a form of informal surveillance by fostering positive social control through the greeting message. Since the greeting message is triggered upon subjects passing by the shelf, it would cause subjects to perceive that the greeting message was triggered because the unmanned retail shelf system was aware of the subjects' presence. This then increases the subject's perceived apprehension risk and certainty of punishment. Additionally, the positive social control exerted by the greeting message would heighten subjects' awareness of potential legal repercussions for even petty offenses such as shoplifting, and therefore the expected severity of punishment associated with the crime. The increase in perceived certainty and expected severity of punishment leads to a deterrence effect on criminal intent. This in turn reduces the likelihood of theft. Thus, we propose the following:

H3b: Presence of sensor greeting bells is negatively associated with theft rate

While both CCTV cameras and sensor greeting bells increase the subject's perceived apprehension risk, the true effectiveness of CCTV cameras as a deterrent lies within the surveillance gaze described in the previous section, which induces a 'state of conscious and permanent visibility' within subjects. On the contrary, the sensor greeting bell achieves informal surveillance through positive social control, which pressures subjects into abiding by social norms, making them less likely to engage in deviant behaviors. We argue that the two mental states are mutually exclusive, meaning that the positive psychological state induced by the sensor greeting bell's friendly greeting message might interrupt the state of constant intensive surveillance that CCTV cameras might otherwise induce. Hence, combining formal and informal surveillance could in practice lead to lower effective deterrence. To better understand how interference might occur, we compare the different mechanisms through which formal and informal surveillance achieves deterrence below.

As discussed in the previous section, CCTV surveillance systems deter unlawful behavior through the ‘surveillance gaze’, which threatens the possibility of rapid intervention at any moment. This results in a psychological state of being controlled by invisible overseers within customers. This then creates a self-regulating mechanism within customers that can be described as a bad conscience. This bad conscience represents an internalization of the control exerted by the CCTV surveillance system. Once internalized, the deterrent effect of the CCTV surveillance system becomes automatically functioning and permanent, which is what makes CCTV surveillance so effective at deterring deviant behavior.

Informal surveillance, on the other hand, works through social control methods such as fostering positive social interaction between sales staff and customers, or in the case of our study, a greeting message from a sensor greeting bell. We argue that the positive emotional response resulting from the social presence generated by the sensor greeting bell directly interferes with the effectiveness of a CCTV surveillance system in achieving a psychological state of intensive surveillance. A customer that just received a friendly greeting message, would be momentarily relieved of the intense psychological pressure exerted by CCTV surveillance. Even though the relief is only temporary and psychological (since the CCTV continues to record regardless of the greeting), it disrupts the effectiveness of the CCTV by rendering less salient subjects’ perception of permanent visibility. As a result, a CCTV surveillance system would be less effective in deterring potential violators when there is a sensor greeting bell playing a greeting message.

In the context of our study, a subject that passes by an unmanned retail shelf with CCTV would experience a negative emotion since he or she would be subjected to the intense psychological pressures of being watched once he or she is aware of the presence of the CCTV, either through noticing the prominently placed CCTV itself or seeing the signboard announcing that the area is under CCTV surveillance. However, if at this time, a friendly greeting message is played by a sensor greeting bell, the positive emotion that is induced by the greeting message would counteract the negative emotion that is induced by the psychological pressures of being watched. This effectively alleviates the psychological pressures of being watched within the subject, which results in the CCTV having a weaker deterrence effect on criminal intent. Therefore, we propose that:

H3c: The negative effect the presence of CCTV surveillance has on theft rate is weaker when sensor greeting bell is present

2.4 METHODOLOGY

The hypotheses proposed in the present study were tested through a field experiment with a 2 × 2 full-factorial between-subjects design (i.e., CCTV surveillance system × sensor greeting bell). To avoid the confounding of implied surveillance caused by the presence of experimenters in a lab setting with our manipulation of formal and informal surveillance, we adopted a field experiment methodology. Additionally, since we are trying to understand the impact of implementing technological interventions, the realism of the experiment is important. Hence for our experiment, natural, field, or artifactual experiments are preferred (Gupta et al. 2018).

2.4.1 Experimental Setup

We conducted our field experiment using unmanned retail shelves that would primarily sell bottled water by partnering with a local bottled water company. Each unmanned retail shelf would have four shelf levels, housing anywhere up to 96 bottles of water. Each bottle of water would retail at 1.5 RMB, the prevailing price for a small bottle of water in the nearby supermarkets.

Each unmanned shelf would be assigned to one of the four treatment conditions, 1. Formal surveillance with CCTV only 2. Informal surveillance with sensor greeting bell only 3. Both CCTV and sensor greeting bell 4. Control.

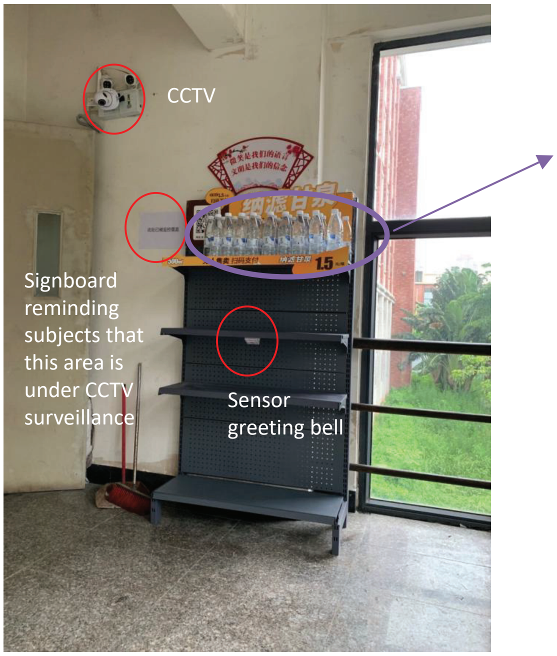

CCTV
Signboard reminding subjects that this area is under CCTV surveillance
Sensor greeting bell

Figure 2-3: An Unmanned Retail Shelf with both Sensor Greeting Bell and CCTV

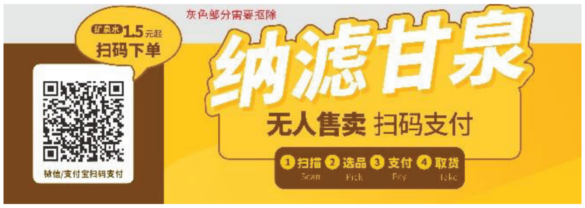


Figure 2-4: QR Code with 4-step Payment Instructions

Figure 2-3 shows an unmanned retail shelf under the third treatment condition, where both the sensor greeting bell as well as CCTV are present. In the first treatment condition, only the CCTV and the signboard stating that the area is under CCTV surveillance are present. In the second treatment condition, only the sensor greeting bell is present. In the control condition, neither the CCTV nor the sensor greeting bell is present.

For the CCTV treatment, the CCTV camera is mounted above the shelf but remains prominent due to its size and contrast with the white walls it is mounted against. In addition, the signboard explicitly stating that the area is under CCTV surveillance is placed next to the retail shelf at eye level (see Figure 2-3). The CCTV camera is active 24/7 during our experiment.

For the sensor greeting bell treatment, the sensor greeting bell is placed under one of the shelves below eye level, such that it can only be heard and not seen. The sensor greeting bell's motion sensor activates a welcome message whenever a subject walks by the vicinity of the unmanned retail shelf.

These unmanned retailed shelves are deployed in hostel buildings of a university, providing convenience to subjects who want to purchase bottled water but do not wish to walk all the way to the supermarket. A subject that wishes to purchase a bottle of water only needs to scan a QR code for payment through WeChat Pay, one of the most popular mobile payment platforms in China (Ma 2019). The QR Code to be scanned for payment will be prominently displayed on the top level of the shelf with a simple 4-step instruction – 1. Scan 2. Pick 3. Pay 4. Take (see Figure 2-4). Every scan or payment through the QR code is recorded on the payment system with a timestamp and payment amount (if any). After payment, subjects can then pick and take a bottle of water from the unmanned retail shelf by themselves.

The 4-step instructions for payment are present in all conditions, however, there are neither physical restrictions nor onsite staff that could stop subjects from freely taking bottled water from the shelves without payment should they choose to. The presence/absence of formal/informal surveillance in the form of CCTV and sensor greeting bells under different treatment conditions causes subjects to experience different levels of psychological deterrence that could discourage them from taking the bottled water without making payment. The proportion of subjects who chose to take bottled water from the shelves without making any payment is then defined as the theft rate associated with that particular unmanned retail shelf.

Besides psychological deterrence for the potential shoplifters, the presence of surveillance artifacts could also present privacy concerns or transaction security assurances, which could impact the customer approach or conversion rates respectively.

2.4.2 Experimental Location

A university town living area in China was selected to test our research model as student accommodations represent one of the most ideal deployment scenarios for unmanned retail shelves. University towns in China house the entire student undergraduate student population of a university, which amounts to tens of thousands of students. Yet, they have limited real estate for convenience stores. Supermarkets are usually located near cafeterias, which might require up to a fifteen-minute walk. Unmanned retail shelves represent an opportunity for retailers to service this previously underserved market.

We selected 24 locations within the university town, with 6 locations for each of our 4 treatment groups. Within each of the 4 treatment groups, 3 locations are only accessible to male students of that treatment group while 3 locations are only accessible to female students of that treatment group. We captured the interaction of each subject with the unmanned retail shelf using video cameras (hidden cameras are used for the control group and informal surveillance treatment group), including the number of subjects who walked past and approached the unmanned retail shelf. This information can be then used to calculate the approach rate and conversion rate.

2.5 DATA ANALYSIS AND RESULTS

2.5.1 Overview

From 23 June 2020 to 12 July 2020, we deployed 24 unmanned retail shelves across 24 different locations, or 6 locations for each of the 4 conditions from our experimental design. Over the three weeks during which our unmanned retail shelf was deployed, we collected a total of 3000 hours of video footage. In a random sampling of 50 video clips from the control group and informal surveillance treatment group, we do not encounter video clips whereby the subjects are found to have noticed the hidden cameras.

We analyzed the 3000 hours of video footage using a combination of video analytics techniques and manual labeling. Specifically, we extracted the relevant video clips along with the number of subjects (traffic count) within the video clips using an implementation combining the DeepSort and YOLO algorithms (Zhang et al. 2019). We then extracted the total approaching subjects (approach count) through manual labeling of the relevant video clips. Payment data was obtained from the payment system, while the total number of bottles of water taken were obtained from daily inventory checks for each unmanned retail shelf.

A total of 754 bottles of water were taken from the unmanned retail shelves during which, there were 59157 passersby, 2635 approaching subjects, and 594 payments made. Table 2-1 shows a summary of the transaction information across different experimental conditions.

Table 2-1: Aggregate Rate Summary

		Number of						
Condition	Gender/ Location	Passersby	Approaches	Payment Made	Bottles Taken	Approach Rate	Conversion Rate	Theft Rate
CCTV	Male	19433	259	96	105	1%	37%	9%
Bell	Male	2378	230	135	203	10%	59%	33%
CCTV+ Bell	Male	4492	543	80	89	12%	15%	10%
Control	Male	2762	250	44	78	9%	18%	44%
Total	**Male**	**29065**	**1282**	**355**	**475**	**4%**	**28%**	**25%**
CCTV	Female	7266	678	83	92	9%	12%	10%
Bell	Female	3887	130	37	41	3%	28%	10%
CCTV+ Bell	Female	15178	406	53	61	3%	13%	13%
Control	Female	3761	139	66	85	4%	47%	22%
Total	**Female**	**30092**	**1353**	**239**	**279**	**4%**	**18%**	**14%**
	Total	**59157**	**2635**	**594**	**754**	**4%**	**23%**	**21%**

To conduct the statistical analysis to test our hypothesis, we aggregated the approach rate, conversion rate, and theft rate to the daily level, hence the unit of analysis for our data is at the daily level from 23 June 2020 to 12 July 2020 for each of the 24 unmanned retailed stands.

2.5.2 Analysis Strategy

We conducted ANOVA, mediation analysis, and regression analysis in the following subsections to test our hypotheses and answer our research question – how would surveillance technology impact consumer behavior in an unmanned retail environment? We first conducted an ANOVA to test our hypotheses for the main effects and interaction effects of formal and informal surveillance on approach rate, conversion rate, and theft rate. We then conducted a mediation analysis to understand how approach rate, conversion rate, and theft rate might mediate the relationships between the surveillance technologies and economic outcomes.

Next, we conducted a series of regression analyses that also tested for the main effects and interacting effects of the surveillance technologies, as well as the mediating effects of approach rate, conversion rate, and theft rate on economic outcomes. While the ANOVA results make it easier to interpret the interaction effects, the regression analysis allows us to control for each retail shelf's daily traffic count and to quantify effect sizes.

2.5.3 ANOVA Results on Approach Rate

ANOVA test was conducted to test the effects of CCTV and sensor greeting bell on theft rate. Results are shown in Table 2-2.

Table 2-2: ANOVA Test – Main and Interaction Effects on Approach Rate

Source	df	Mean square	F	Sig.
CCTV	1	.110	14.521	.000
SensorBell	1	.106	14.012	.000
Gender	1	.145	19.150	.000
SensorBell × CCTV	1	.007	0.872	.352
CCTV × Gender	1	.053	6.926	.009
SensorBell × Gender	1	.376	49.638	.000
CCTV × SensorBell × Gender	1	.003	.453	.502

ANOVA results showed CCTV significantly influenced approach rate (F(1, 149) = 14.52, *$p < 0.01$*); that is, approach rate is lower in unmanned retail locations where CCTV are present as compared to locations where CCTV are not present. Hence, H1a was supported.

ANOVA results showed sensor greeting bells significantly influenced approach rate (F(1, 149) = 14.01, *$p < 0.01$*); that is, approach rate is higher in unmanned retail locations where sensor greeting bells are present as compared to locations where sensor greeting bells are not present. Hence, H1b was supported.

ANOVA results also showed that gender significantly influenced approach rate (F(1, 149) =19.15, *$p < 0.01$*); that is, approach rate is higher in unmanned retail locations accessible to only male subjects compared to locations accessible only to female subjects.

There was no significant interaction effect between CCTV and sensor greeting bells (F(1, 149) = 0.87, $p > 0.1$); hence, H1c was not supported.

There was a significant interaction effect between CCTV and gender (F(1, 149) = 6.93, $p < 0.01$) as well as sensor greeting bell and gender (F(1, 149) = 49.64, $p < 0.01$); that is, the main effect of CCTV and sensor greeting bells on approach rate is bigger for male subjects than female subjects. Figure 2-5 shows the interaction effects of CCTV and gender, as well as sensor greeting bell and gender on approach rate. Finally, there was no significant three-way interaction effect between CCTV, sensor greeting bells and gender (F(1, 149) = 0.45, $p > 0.1$) on approach rate.

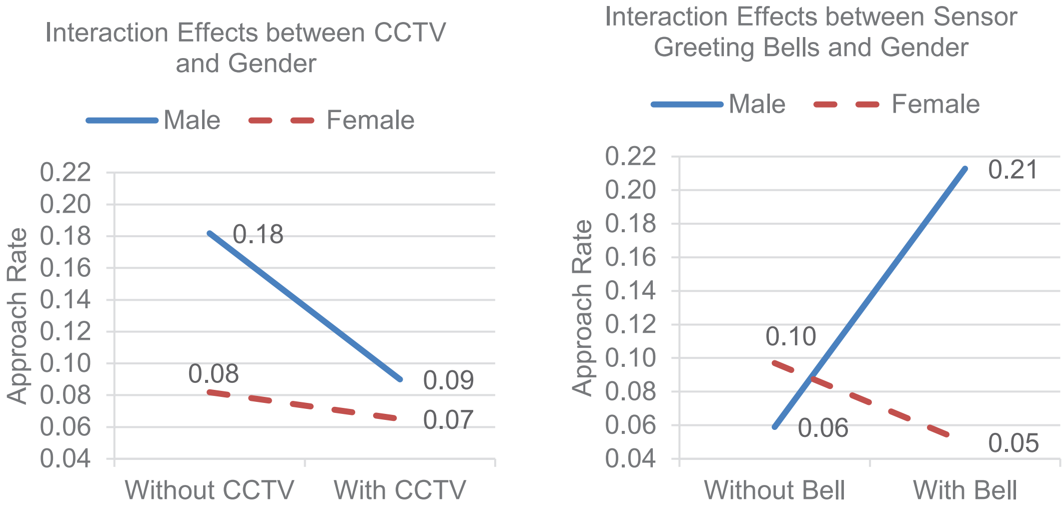


Figure 2-5: Interaction Effects between CCTV and Gender, and Sensor Greeting Bell and Gender on Approach Rate

2.5.4 ANOVA Results on Conversion Rate

ANOVA test was conducted to test the effects of CCTV and sensor greeting bell on conversion rate. Results are shown in Table 2-3.

Table 2-3: ANOVA Test – Main and Interaction Effects on Conversion Rate

Source	df	Mean square	F	Sig.
CCTV	1	.643	12.102	.001
SensorBell	1	.043	.806	.371
Gender	1	.130	2.450	.120
SensorBell × CCTV	1	.755	14.205	.000
CCTV × Gender	1	.295	5.560	.020
SensorBell × Gender	1	.675	12.693	.000
CCTV × SensorBell × Gender	1	1.296	24.389	.000

ANOVA results showed CCTV significantly influenced conversion rate (F(1, 149) = 12.10, *p < 0.01*); that is, conversion rate is lower in unmanned retail locations where CCTV are present as compared to locations where CCTV are not present. However, the main effect is significant in the opposite direction as we had hypothesized, hence, H2a was not supported.

Sensor greeting bell was found to not have a significant effect on conversion rate (F(1, 149) = 0.81, *p > 0.1*); that is, there is no significant difference in conversion rate between locations where sensor greeting bells are present and where sensor greeting bells are not present. Hence, H2b was not supported.

ANOVA results also showed that gender did not significantly influence conversion rate (F(1, 149) = 2.45, *p > 0.1*); that is, conversion rate did not show a significant difference between unmanned retail locations accessible to only male subjects compared to locations accessible only to female subjects.

There was a significant interaction effect between CCTV and sensor greeting bell (F(1, 149) = 14.21, *p < 0.01*); that is, the main effect of CCTV on conversion rate is bigger when sensor greeting bells are also present. However, as the main effect of CCTV surveillance on conversion rate is negative instead of positive, H2c is not supported. Figure 2-6 shows the interaction effects of CCTV and sensor greeting bells on conversion rate.

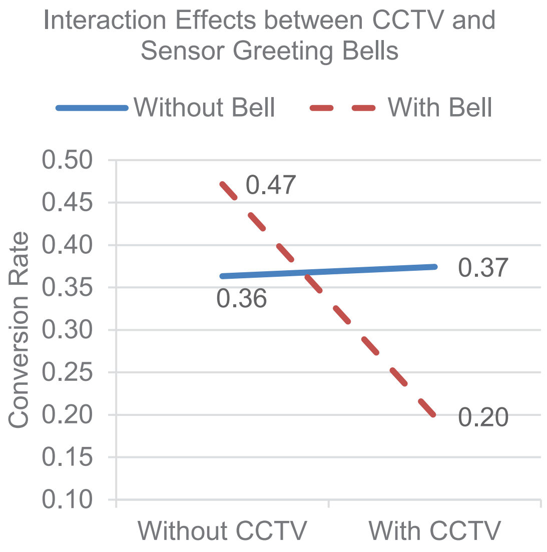


Figure 2-6: Interaction Effects between CCTV and Sensor Greeting Bell on Conversion Rate

There was a significant interaction effect between CCTV and gender (F(1, 149) = 5.56, $p < 0.05$); that is, the main effect of CCTV on conversion rate is bigger for female subjects than male subjects. There was a significant interaction effect between sensor greeting bells and gender (F(1, 149) = 12.69, $p < 0.01$) on conversion rate. Figure 2-7 shows the interaction effects between CCTV and gender, and sensor greeting bell and gender on conversion rate.

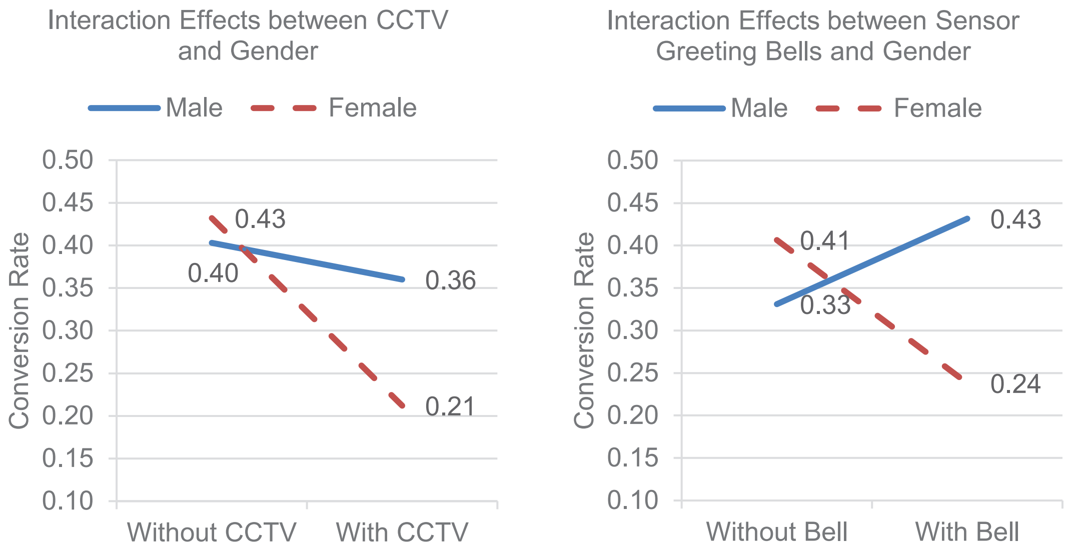


Figure 2-7: Interaction Effects between CCTV and Gender, and Sensor Greeting Bell and Gender on Conversion Rate

Finally, there was a significant three-way interaction effect between CCTV, sensor greeting bells, and gender (F(1, 149) = 24.39, $p < 0.01$) on conversion rate. Figure 2-8 shows the three-way interaction effects on conversion rate.

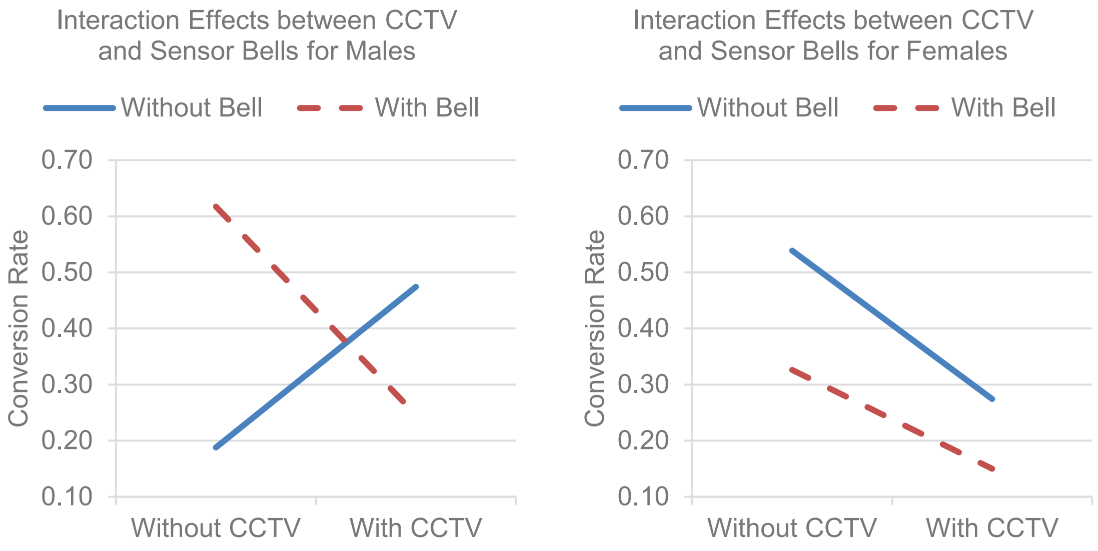


Figure 2-8: Three-way Interaction Effects between Gender, CCTV, and Sensor Greeting Bell on Conversion Rate

2.5.5 ANOVA Results on Theft Rate

ANOVA test was conducted to test the effects of CCTV and sensor greeting bell on theft rate. Results are shown in Table 2-4.

Table 2-4: ANOVA Test – Main and Interaction Effects on Theft Rate

Source	df	Mean square	F	Sig.
CCTV	1	.646	14.569	.000
SensorBell	1	.048	1.089	.298
Gender	1	.308	6.946	.009
SensorBell × CCTV	1	.115	2.590	.110
CCTV × Gender	1	.397	8.961	.003
SensorBell × Gender	1	.017	.389	.534
CCTV × SensorBell × Gender	1	.061	1.376	.243

ANOVA results showed CCTV significantly influenced theft rate (F(1, 149) = 14.57, $p < 0.01$); that is, theft rate is lower in unmanned retail locations where CCTV are present as compared to locations where CCTV are not present. Hence, H3a was supported.

Sensor greeting bell was found to not have a significant effect on theft rate (F(1, 149) = 1.09, *p > 0.1*); that is, there is no significant difference in theft rate between locations where sensor greeting bells are present and where sensor greeting bells are not present. Hence, H3b was not supported.

ANOVA results also showed that gender significantly influenced theft rate (F(1, 149) = 6.95, *p < 0.01*); that is, theft rate is higher in unmanned retail locations accessible to only male subjects compared to locations accessible only to female subjects.

There was no significant interaction effect between CCTV and sensor greeting bells (F(1, 149) = 2.59, *p > 0.1*), hence, H3c was not supported.

There was a significant interaction effect between CCTV and gender (F(1, 149) = 8.96, *p < 0.01*); that is, the main effect of CCTV on theft rate is bigger for male subjects than female subjects. Figure 2-9 shows the interaction effects of CCTV and gender on theft rate, as well as the interaction effects of sensor greeting bells and gender on theft rate.

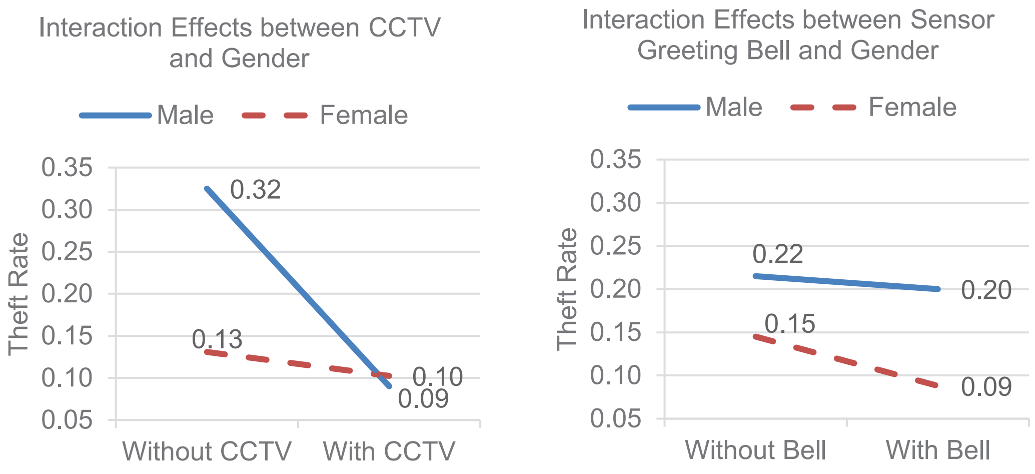


Figure 2-9: Interaction Effects between CCTV and Gender, and Sensor Greeting Bell and Gender on Theft Rate

There were no significant interaction effects between sensor greeting bell and gender (F(1, 149) = 0.39, $p > 0.1$) or three-way interaction effects between CCTV, sensor greeting bell and gender (F(1, 149) = 1.38, $p > 0.1$) on theft rate.

2.5.6 Mediation Test Results

A mediation analysis was conducted following Baron and Kenny (1986)'s method with approach, conversion, and theft rate as the mediating variables, CCTV and sensor greeting bell as the independent variables, and revenue and gross profit as the dependent variables as shown in Figure 2-10 below.

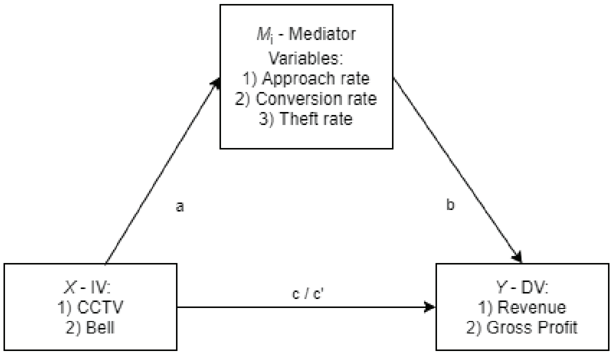


Figure 2-10: Mediation Analysis Model

Results in Table 2-5 show the results for the direct effects of Paths *a, b, c,* and *c'* in Figure 2-10 for CCTV as the IV. Path *a* is significant for the mediators approach rate, conversion rate, and theft rate on both revenue and gross profit. Path *b* is significant for the mediators approach rate, conversion rate, and theft rate on revenue when controlled for the IV. Path *b* is significant for the mediator's conversion rate and theft rate but not approach rate for gross profit when controlled for the IV. Hence approach rate does not mediate the impact of CCTV on gross profit.

Table 2-5: Mediation Test Results for CCTV – Direct and Total Effects

		IV = CCTV, DV = Revenue				IV = CCTV, DV = Gross Profit			
	Path	b	df2	t	p	b	df2	t	p
Effect of IV on mediator									
Approach rate	a	-0.05	154	-3.20	0.0017	-0.05	154	-3.20	0.0017
Conversion rate	a	-0.14	154	-3.15	0.0019	-0.14	154	-3.15	0.0019
Theft rate	a	-0.15	154	-4.27	0.0000	-0.15	154	-4.27	0.0000
Effect of IV and mediator on DV									
IV	c'	0.75	151	1.14	0.2573	0.39	151	0.87	0.3845
Approach rate	b	5.87	151	2.08	0.0390	2.68	151	1.40	0.1638
Conversion rate	b	7.32	151	6.66	0.0000	4.32	151	5.79	0.0000
Theft rate	b	-3.53	151	-2.55	0.0117	-5.41	151	-5.77	0.0000
Total effects									
IV	c	-0.04	154	-0.06	0.949	0.46	154	0.94	0.3467

For both revenue and gross profit, while Path *c'* is not significant, Path *c* is not significant as well, thus revealing an insignificant total effect. Although the total effect was insignificant, according to Hayes (2009) it is still possible for total effects that do not exist to be mediated if two or more indirect effects with opposite signs cancel each other producing an insignificant total effect. Table 2-6 shows the results for the indirect effects, Path *a* × *b*. Zero falls within the confidence intervals of only CCTV's indirect effect on gross profit through approach rate, revealing that approach rate, conversion rate, and theft rate mediates the relationship between CCTV and revenue, while conversion rate and theft rate mediates the relationship between CCTV and gross profit.

Table 2-6: Mediation Test Results for CCTV – Indirect Effects

	IV = CCTV, DV = Revenue				IV = CCTV, DV = Gross Profit			
	Effect	SE	Lower CI	Upper CI	Effect	SE	Lower CI	Upper CI
Total	-0.80	0.53	-1.97	0.13	0.06	0.36	-0.67	0.72
Approach rate	-0.32	0.24	-0.92	-0.01	-0.14	0.13	-0.49	0.04
Conversion rate	-1.00	0.37	-1.80	-0.36	-0.59	0.22	-1.05	-0.20
Theft rate	0.52	0.22	0.14	1.00	0.80	0.23	0.38	1.28

Results in Table 2-7 show the results for the direct effects of Paths *a, b, c,* and *c'* in Figure 2-10 for sensor greeting bell as the IV. Path *a* is significant for only the mediator approach rate on both revenue and gross profit. However, Path *b* is not significant for the mediator approach rate, on both revenue and gross profit when controlled for the IV. Hence approach rate does not mediate the impact of sensor greeting bell on the DVs.

Table 2-7: Mediation Test Results for Sensor Greeting Bell – Direct and Total Effects

		IV = Bell, DV = Revenue				**IV = Bell, DV = Gross Profit**			
	Path	b	df2	t	p	b	df2	t	p
Effect of IV on mediator									
Approach rate	a	0.05	154	3.09	0.0024	0.05	154	3.09	0.0024
Conversion rate	a	-0.04	154	-0.82	0.4137	-0.04	154	-0.82	0.4137
Theft rate	a	-0.03	154	-0.83	0.4095	-0.03	154	-0.83	0.4095
Effect of IV and mediator on DV									
IV	c'	1.51	151	2.48	0.0141	0.54	151	1.30	0.1970
Approach rate	b	3.37	151	1.21	0.2283	1.66	151	0.87	0.3880
Conversion rate	b	7.24	151	6.86	0.0000	4.25	151	5.85	0.0000
Theft rate	b	-3.77	151	-2.92	0.0041	-5.58	151	-6.27	0.0000
Total effects									
IV	c	1.53	154	2.26	0.0253	0.64	154	1.33	0.1864

Table 2-8 shows the results for the indirect effects, Path *a* × *b*. Zero falls within the confidence intervals of all the indirect effects, further confirming that there is no mediation effect for any of the mediators for the relationship between sensor greeting bell and the DVs.

Table 2-8: Mediation Test Results for Sensor Greeting Bell – Indirect Effects

	IV = Bell, DV = Revenue				**IV = Bell, DV = Gross Profit**			
	Effect	SE	Lower CI	Upper CI	Effect	SE	Lower CI	Upper CI
Total	0.03	0.38	-0.65	0.86	0.10	0.30	-0.43	0.73
Approach rate	0.18	0.19	-0.10	0.62	0.09	0.12	-0.10	0.36
Conversion rate	-0.27	0.31	-0.84	0.39	-0.16	0.18	-0.49	0.22
Theft rate	0.11	0.15	-0.16	0.43	0.17	0.20	-0.23	0.57

2.5.7 Regression Test Results on Revenue and Gross Profit

Besides approach rate, conversion rate, and theft rate, revenue, and gross profits are dependent variables with strong practical implications for our field experiment. Outcomes such as revenue and gross profit are relevant to companies deploying unmanned retail shelves as it informs them of the ultimate economic benefits that are associated with implementing surveillance technology together with the unmanned retail shelves. We first test the relationship between the independent variables and revenue as well as gross profit with the following regression models:

$$\begin{aligned} Revenue_{it} = {} & \alpha_0 + \alpha_1 ApproachRate_{it} + \alpha_2 ConversionRate_{it} \\ & + \alpha_3 TheftRate_{it} + \alpha_4 TrafficCount_{it} + \alpha_5 Gender_i \\ & + \alpha_6 CCTV_i + \alpha_7 Sensorbell_i + \alpha_8 CCTV_i \times Sensorbell_i \\ & + \alpha_9 Gender_i \times CCTV_i + \alpha_{10} Gender_i \times Sensorbell_i \\ & + \alpha_{11} TrafficCount_i \times CCTV_i \\ & + \alpha_{12} TrafficCount_i \times Sensorbell_i + \varepsilon_{it} \end{aligned} \tag{1}$$

$$\begin{aligned} & GrossProfit_{it} \\ & = \beta_0 + \beta_1 ApproachRate_{it} + \beta_2 ConversionRate_{it} \\ & + \beta_3 TheftRate_{it} + \beta_4 TrafficCount_{it} + \beta_5 Gender_i \\ & + \beta_6 CCTV_i + \beta_7 Sensorbell_i + \beta_8 CCTV_i \times Sensorbell_i \\ & + \beta_9 Gender_i \times CCTV_i + \beta_{10} Gender_i \times Sensorbell_i \\ & + \beta_{11} TrafficCount_i \times CCTV_i \\ & + \beta_{12} TrafficCount_i \times Sensorbell_i + \varepsilon_{it} \end{aligned} \tag{2}$$

The first column of Table 2-9 shows the regression results of Equation (1) while the second column shows the regression results of Equation (2). From the regression results for both revenue and gross profit, we find that the coefficients for conversion rate and sensor greeting bell to be positive and significant. We find that the coefficients for theft rate to be negative and significant. We find that the coefficients for the interaction effects between sensor greeting bell and CCTV, and sensor greeting bell and gender to be negative and significant. The coefficients for approach rate, traffic count, gender, and CCTV were not significant.

Table 2-9: Revenue and Gross Profit Estimation Results

	(1)	(2)
VARIABLES	Revenue	Gross profit
Approach rate	2.089	1.446
	(3.771)	(2.617)
Conversion rate	6.725***	3.727***
	(1.170)	(0.812)
Theft rate	-3.018**	-4.895***
	(1.389)	(0.964)
Traffic count	-0.001	-0.001
	(0.003)	(0.002)
Gender	-1.233	-0.447
	(1.050)	(0.729)
Sensor greeting bell	4.136***	1.986**
	(1.270)	(0.882)
CCTV	-0.310	0.484
	(1.459)	(1.012)
Sensor greeting bell × CCTV	-2.868*	-2.095**
	(1.527)	(1.060)
Sensor greeting bell × Gender	-3.199**	-2.248**
	(1.493)	(1.036)
CCTV × Gender	1.381	-0.042
	(1.411)	(0.979)
Sensor greeting bell × Traffic count	0.002	0.002
	(0.002)	(0.002)
CCTV × Traffic count	0.003	0.001
	(0.003)	(0.002)
Constant	2.716**	2.074**
	(1.171)	(0.812)
Observations	157	157
R-squared	0.406	0.406

Standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

2.5.8 2-stage Regression Results on Approach Rate, Conversion Rate, and Theft Rate

To better understand the impact of the treatments, we also conducted a 2-stage regression analysis. We first obtain predicted values of approach rate, conversion rate, and theft rate through the following regression models:

$$
\begin{aligned}
&Appro\widehat{ach}Rate_{\imath t} \\
&\qquad = \lambda_0 + \lambda_1 \times CCTV_i + \lambda_2 \times Sensorbell_i + \lambda_3 \times Gender_i \\
&\qquad + \lambda_4 \times TrafficCount_{it} + \lambda_5 \times (CCTV_i \times Sensorbell_i) \\
&\qquad + \lambda_6 \times (Gender_i \times CCTV_i) + \lambda_7 \times (Gender_i \times Sensorbell_i) \\
&\qquad + \lambda_8 \times (TrafficCount_{it} \times CCTV_i) \\
&\qquad + \lambda_9 \times (TrafficCount_{it} \times Sensorbell_i) + \varepsilon_{it}
\end{aligned}
\tag{3}
$$

$$
\begin{aligned}
&Conver\widehat{s\imath on}Rate_{\imath t} \\
&\qquad = \gamma_0 + \gamma_1 \times CCTV_i + \gamma_2 \times Sensorbell_i + \gamma_3 \times Gender_i \\
&\qquad + \gamma_4 \times TrafficCount_{it} + \gamma_5 \times (CCTV_i \times Sensorbell_i) \\
&\qquad + \gamma_6 \times (Gender_i \times CCTV_i) + \gamma_7 \times (Gender_i \times Sensorbell_i) \\
&\qquad + \gamma_8 \times (TrafficCount_{it} \times CCTV_i) \\
&\qquad + \gamma_9 \times (TrafficCount_{it} \times Sensorbell_i) + \varepsilon_{it}
\end{aligned}
\tag{4}
$$

$$
\begin{aligned}
The\widehat{ftR}ate_{\imath t} &= \omega_0 + \omega_1 \times CCTV_i + \omega_2 \times Sensorbell_i + \omega_3 \times Gender_i \\
&+ \omega_4 \times TrafficCount_{it} + \omega_5 \times (CCTV_i \times Sensorbell_i) \\
&+ \omega_6 \times (Gender_i \times CCTV_i) + \omega_7 \times (Gender_i \times Sensorbell_i) \\
&+ \omega_8 \times (TrafficCount_{it} \times CCTV_i) \\
&+ \omega_9 \times (TrafficCount_{it} \times Sensorbell_i) + \varepsilon_{it}
\end{aligned}
\tag{5}
$$

The three columns of Table 2-10 show the regression results of Equations (3), (4), and (5) respectively. The results were also used to test our hypotheses proposed. From the first column of the regression results for approach rate, we find that the coefficient for CCTV to be negative and significant, while the coefficient for sensor greeting bell to be positive and significant. Thus, both H1a and H1b were supported. The coefficient for the interaction effect between CCTV and sensor greeting bells was marginally significant but negative, thus H1c was not supported.

From the second column of the regression results for conversion rate, we find that the coefficient for CCTV to be positive and marginally significant, while the coefficient for sensor greeting bell to be positive and significant. Thus, both H2a and H2b were supported. The coefficient for the interaction effect between CCTV and sensor greeting bells was significant but negative, thus H2c was not supported.

From the third column of the regression results for theft rate, we find that the coefficient for CCTV to be negative and significant, while the coefficient for sensor greeting bell to be positive and not significant. Thus, H3a was supported but H3b was not supported. The coefficient for the interaction effect between CCTV and sensor greeting bells was not significant, thus H3c was not supported.

Table 2-10: 2-stage Regression - Approach, Conversion, and Theft Rate Results

Equation	(3)	(4)	(5)
variables	Approach rate	Conversion rate	Theft rate
CCTV	-0.074**	0.179*	-0.271***
	(0.030)	(0.096)	(0.081)
Sensor greeting bell	0.165***	0.227***	-0.070
	(0.024)	(0.075)	(0.064)
Gender	0.010	0.175**	-0.181***
	(0.022)	(0.071)	(0.060)
Traffic count	-0.000***	0.000	-0.000
	(0.000)	(0.000)	(0.000)
Sensor greeting bell × CCTV	-0.054*	-0.344***	0.124
	(0.032)	(0.102)	(0.087)
Sensor greeting bell × Gender	-0.146***	-0.234**	0.035
	(0.030)	(0.096)	(0.081)
CCTV × Gender	0.037	-0.256***	0.197**
	(0.030)	(0.095)	(0.080)
Sensor greeting bell × Traffic count	-0.000	0.000	-0.000
	(0.000)	(0.000)	(0.000)
CCTV × Traffic count	0.000***	-0.000	0.000
	(0.000)	(0.000)	(0.000)
Constant	0.136***	0.272***	0.371***
	(0.018)	(0.058)	(0.049)
Observations	157	157	157
R-squared	0.544	0.245	0.209

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

2.5.9 2-stage Regression Results on Revenue and Gross Profit

For the second stage, we regress the predicted values of approach rate, conversion rate, and theft rate on revenue and gross profit.

$$Revenue_{it} = \sigma_0 + \sigma_1 \times \widehat{ApproachRate}_{it} + \sigma_2 \times \widehat{ConversionRate}_{it} + \sigma_3 \times \widehat{TheftRate}_{it} + \sigma_4 \times TrafficCount_{it} + \sigma_5 \times Gender_i + \varepsilon_{it} \tag{6}$$

$$GrossProfit_{it} = \tau_0 + \tau_1 \times Appr\widehat{oach}Rate_{\imath t} + \tau_2 \times Conver\widehat{s\imath on}Rate_{\imath t} \\ + \tau_3 \times The\widehat{ftR}ate_{\imath t} + \tau_4 \times TrafficCount_{it} + \tau_5 \times Gender_i \\ + \ \varepsilon_{it} \qquad (7)$$

The first two columns of Table 2-11 show the regression results of Equations (6) and (7) respectively. We also regressed the values of observed values of approach rate, conversion rate, and theft rate on revenue and gross profit in columns 3 and 4.

From the first column of the regression results for revenue on predicted values, we find that the coefficients for predicted approach rate, predicted conversion rate, and traffic count to be positive and significant, while the coefficients for predicted theft rate and gender to be not significant.

From the second column of the regression results for gross profit on predicted values, we find that the coefficients for predicted approach rate, predicted conversion rate, and traffic count to be positive and significant, while the coefficient for predicted theft rate to be negative and marginally significant. Finally, the coefficient for gender was not significant.

From the third column of the regression results for revenue on observed values, we find that the coefficients for observed approach rate, observed conversion rate, and traffic count to be positive and significant, while the coefficients for observed theft rate and gender to be negative and significant.

From the fourth column of the regression results for gross profit on observed values, we find that the coefficient for observed approach rate, observed conversion rate, and traffic count to be positive and significant, while the coefficient for observed theft rate and gender to be negative and significant.

Table 2-11: 2-stage Regression Results on Revenue and Gross Profit

Equation	(6)	(7)	(8)	(9)
variables	Revenue	Gross profit	Revenue	Gross profit
Approach Rate Hat	23.674***	10.932**		
	(6.029)	(4.267)		
Conversion Rate Hat	7.506***	5.633***		
	(2.530)	(1.791)		
Theft Rate Hat	-4.257	-6.324*		
	(4.599)	(3.255)		
Gender	-0.822	-0.724	-1.507**	-1.012**
	(0.818)	(0.579)	(0.620)	(0.422)
Traffic count	0.004***	0.002**	0.002**	0.001**
	(0.001)	(0.001)	(0.001)	(0.001)
Approach rate			9.394***	4.915**
			(3.164)	(2.155)
Conversion rate			7.357***	4.375***
			(1.058)	(0.721)
Theft rate			-2.967**	-5.023***
			(1.351)	(0.920)
Constant	0.129	0.674	2.483**	1.958***
	(2.084)	(1.475)	(0.977)	(0.665)
Observations	157	157	157	157
R-squared	0.235	0.204	0.339	0.364

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

2.5.10 Summary of Results

Table 2-12 below summarizes the ANOVA and regression test results for our hypotheses. H1a posits that the presence of CCTV cameras will reduce the approach rate due to information privacy concerns and is supported by both the ANOVA and regression analysis results. H1b posits that the presence of sensor greeting bells will increase approach rate due to positive social presence induced by the sensor greeting bell and is supported by both the ANOVA and regression analysis results. H1c posits that the negative effect of CCTV on approach rate will be weaker when sensor greeting bell is also present due to positive social presence desensitizing customers from information privacy risk and is supported by neither the ANOVA analysis nor the regression analysis.

Table 2-12: Summary of Results on Hypotheses Testing

#	Hypothesis	ANOVA Analysis	2-stage Regression Analysis
H1a	CCTV → approach rate (-)	Significant, supported	Significant, supported
H1b	Bell → approach rate (+)	Significant, supported	Significant, supported
H1c	CCTV x Bell → approach rate (-)	Not significant	Marginally significant, not supported
H2a	CCTV → conversion rate (+)	Significant, not supported	Marginally significant, supported
H2b	Bell → conversion rate (+)	Not significant	Significant, supported
H2c	CCTV x Bell → conversion rate (+)	Significant, not supported	Significant, not supported
H3a	CCTV → theft rate (-)	Significant, supported	Significant, supported
H3b	Bell → theft rate (-)	Not significant	Not significant
H3c	CCTV x Bell → theft rate (-)	Not significant	Not significant

H2a posits that the presence of CCTV cameras will increase the conversion rate due to an assurance mechanism reducing the perceived transaction and merchandise security risk. This is supported by the regression analysis but not the ANOVA analysis. H2b posits that the presence of sensor greeting bells will increase conversion rate due to positive social presence induced by the sensor greeting bell. This is supported by the regression analysis results but not the ANOVA analysis results. H2c posits that the positive effect of CCTV on conversion rate will be stronger when sensor greeting bell is also present due to positive social presence strengthening the assurance mechanism of the CCTV. This is supported by neither the ANOVA analysis nor the regression analysis.

H3a posits that the presence of CCTV cameras will reduce the theft rate by acting as formal surveillance which increases apprehension risk perceived by potential shoplifters. This is supported by both the regression analysis and the ANOVA analysis results. H3b posits that the presence of sensor greeting bells will reduce theft rate by acting as informal surveillance which increases apprehension risk perceived by potential shoplifters and fosters social control upon them. This is supported by neither the regression analysis results, nor the ANOVA analysis results. H3c posits that the negative effect of CCTV on theft rate will be weaker when sensor bell is also present due to the conflicting mechanisms through which formal and informal surveillance impact theft rate. This is supported by neither the ANOVA analysis nor the regression analysis.

Our model specification for the 2-stage regression analysis was able to control for the daily traffic count for each unmanned retail shelf, a variable omitted in the ANOVA analysis. This led to a discrepancy in the hypothesis testing for H2a and H2b, which was supported by the regression results but not the ANOVA results. We argue that the regression analysis provides us with more accurate hypothesis testing results. The ANOVA results, however, remain informative in interpreting the interaction effects between gender and the two treatments.

2.6 DISCUSSION

Our objective for this study has been to investigate the effectiveness of IT artifacts in replacing onsite employees in deterring theft without reducing customer approaches and sales conversion. Our study provides an empirical look into the treatment effects of formal and informal surveillance methods to deter potential shoplifters as suggested by the CPTED framework (Moffatt 1983; Newman 1972). We conducted a controlled experiment, which represents the most convincing method to create the counterfactual to evaluate treatment effects (Harrison and List 2004). Although both laboratory and field experiments are controlled experiments, it would be difficult for a lab experiment to fully exogenize the impact of surveillance since the subjects will be perpetually aware of the presence of the experimenter, which could amount to a form of surveillance for some subjects. Indeed, our field experiment setup and the unmanned nature of our retail shelves provided us a unique opportunity to observe and measure theft behavior through the analysis of video and mobile payment data.

Our hypothesis testing results revealed that the presence of formal surveillance, in the form of CCTV, reduces theft rate. Through the theoretical lens of deterrence theory, we suggest that this finding may be explained by the increase in certainty of punishment for a crime committed in the presence of a CCTV. Compared to the counterfactual control group, where surveillance is completely absent since the retail shelf itself is unmanned, subjects considering shoplifting at a retail shelf with CCTV present perceive a much higher apprehension risk, and thus a much higher certainty of punishment.

However, contrary to our expectations, the presence of informal surveillance, in the form of sensor greeting bells, did not have a significant effect on the reduction of the theft rate at unmanned retail shelves. In earlier sections, we had hypothesized that the presence of informal surveillance has the effect of increasing people's perception that they can be seen, thus increasing the apprehension risk associated with taking bottled water from the retail shelf without paying. Although we believe this mechanism to be valid, it could be that the perception of being watched induced by informal surveillance is too weak to result in a meaningful impact on perceived apprehension risk by subjects. Similarly, the social control fostered by informal surveillance could also have been too weak to result in a meaningful impact on expected severity of punishment by subjects.

Besides the main effects, we had hypothesized that the presence of sensor greeting bells weakens the impact CCTV has on theft rate. We believed the presence of both formal and informal surveillance at a single unmanned retail shelf resulted in competing psychological states within the subject. This would have reduced the effectiveness of the CCTV in reducing the theft rate at an unmanned retail shelf. However, this interaction effect was not statistically significant. It is likely that the deterrence effect induced by the CCTV on potential violators is so strong as compared to the social presence of the sensor greeting bells, that the sensor greeting bells did little to weaken the CCTV's main effects.

The results of the hypothesis testing for theft rate would seem to suggest that retailers should implement only CCTV cameras and not sensor greeting bells to improve economic outcomes for unmanned retail shelves. However, the scope of our research question extends beyond just theft rate to consumer behavior in general. While the impact on theft rate may be one of the key factors how surveillance technology might impact economic outcomes for an unmanned retail shelf, it is certainly not the only factor. Hence, we had also been interested in the impact of surveillance technology on customer approach rate and sales conversion rate as well.

For formal surveillance, our hypotheses testing found that CCTV cameras reduce approach rate. In our hypothesis, we explained that information privacy concerns caused by CCTV cameras could result in this reduction in approach rate. On the other hand, for informal surveillance, our hypothesis testing found that sensor greeting bells increase approach rate.

Our conversion rate hypothesis testing yielded different conclusions for our ANOVA and regression analysis of formal surveillance. We had proposed that the presence of CCTV cameras would lead to a higher conversion rate by reducing perceived transaction security risk through an assurance mechanism. Although this was significant in the ANOVA analysis, the CCTV main effect was found to have a negative impact on conversion rate. However, in our regression analysis, we found CCTV cameras to be marginally significant and positive on conversion rate, thus supporting our hypothesis. To reconcile the differing conclusions, we could perform the ANOVA computations using linear regression computations, with each row of the ANOVA table corresponding to the variance of a corresponding set of regression coefficients (Gelman 2005). Thus, the ANOVA main effect for CCTV would be a simple linear regression with only a constant and the CCTV treatment variable. This leads to a discrepancy with our two-stage regression analysis because the regression included the main and interaction terms for other explanatory variables such as sensor greeting bells, gender, and traffic count, in addition to CCTV cameras.

There was also a discrepancy between the ANOVA and regression analysis for the main effect of sensor greeting bells on conversion rate. We had hypothesized that social presence induced by sensor greeting bells would lead to higher sales conversion rate for the unmanned retail shelf. While this was not significant in our ANOVA analysis, it was supported by our regression analysis.

In addition to the main effects, we had also considered the interaction effects between the two treatments CCTV cameras and sensor greeting bells in our hypothesis. We had expected that the positive social presence of sensor greeting bells would reduce information privacy concerns associated with CCTV cameras, thus reducing the negative impact of CCTV on approach rate. This interaction effect was found to be not significant for the ANOVA analysis but significant for the regression analysis. However, the negative coefficient for the interaction term suggests that the impact of sensor greeting bells on CCTV cameras was opposite to what was hypothesized.

The interaction effect of sensor greeting bells and CCTV cameras on sales conversion rate was also found to be opposite of the hypothesized interaction effect. We had expected the positive social presence to further strengthen the assurance mechanism through which CCTV improves conversion rate. Instead, it was revealed that the interaction term of sensor greeting bells and CCTV cameras had a negative coefficient through the regression analysis.

In summary, while CCTV cameras had a positive economic impact in reducing theft rate and increasing sales conversion rate, they also had a negative economic impact through the reduction of customer approach rate. On the other hand, while sensor greeting bell improves both approach rate and conversion rate, it had no significant impact in reducing theft rate, which was the main purpose of implementing informal surveillance in the first place. Further complicating the decision-making for retailers is the presence of interaction effects between sensor greeting bells and CCTV cameras that could reduce the overall approach rate and conversion rate.

Hence, to better understand the overall economic impact, we estimated the impact of the treatment variables sensor greeting bell and CCTV, as well as gender, traffic count, approach rate, conversion rate, and theft rate on revenue and gross profit.

As shown in Table 2-9 we find sensor greeting bell to have a positive and significant coefficient when regressed on both revenue and gross profit, whereas CCTV did not have a significant coefficient. The coefficient interaction term between sensor greeting bell and CCTV was marginally significant but negative on both revenue and gross profit. Hence, the estimation results from Equations (1) and (2) would suggest that a retailer implement only sensor greeting bells but not CCTV cameras to maximize the economic impact in terms of revenue and gross profit.

2.6.1 Implications for Research

This study makes three theoretical contributions. First, while there have been numerous studies that have explored the impact of electronic surveillance on employees at the workplace (Ball 2010; D'Urso 2006; Friedman and Reed 2007; Watkins Allen et al. 2007), to our knowledge, there have been no empirical studies focusing on the impact of surveillance on consumer behavior in retail environments. Concerning this, although there have been related studies that investigated the relationship between privacy concerns and purchase intentions (Malhotra et al. 2004; Smith et al. 1996; Van Slyke et al. 2006) these studies have all been based on a scenario where retailers actively request for a discrete amount of personal information from the subject. The privacy risk in our study is different in terms of magnitude and specificity. While personal information as requested by retailers might be highly specific, the amount of data they request are limited to a few key attributes such as home address, credit card information, email address, etc. Instead of actively requesting specific data from the customer, a CCTV surveillance system collects information passively and continuously. Most of the video data collected might neither be useful to the retailer nor by itself comprise a substantial privacy threat to the customer. However, in an environment of dataveillance where information from multiple data sources can be accessed and cross-referenced (Lyon 2001), CCTV surveillance data can and will substantially contribute to the 'dossier' of the individual through its sheer volume. We argue that in today's world, with its ability to collect ever-increasing amounts of data and retain them indefinitely (Bellia 2008), CCTV surveillance has evolved into a highly relevant privacy threat that warrants further investigation. Our study reveals a significant and negative main effect for CCTV (formal surveillance) on approach rate, compared to a significant and positive main effect for sensor greeting bell (informal surveillance). This study expands current surveillance literature by providing empirical evidence that surveillance technology collecting identifying information on subjects causes privacy concerns among subjects.

Second, this study contributes to the body of literature that explores the effectiveness of technology in replacing human actors from a social presence perspective. There have been multiple studies that are devoted to the study of technology-enabled social presence in the context of a virtual environment (Guadagno et al. 2007; Nowak and Phelps 1995; Von der Puetten et al. 2010), an online e-commerce environment (Kumar and Benbasat 2006; Zhu et al. 2010), or an online teaching environment (Anderson and Agarwal 2011; Garrison et al. 2001). In these studies, the entire environment through which subjects interact is technology-enabled and artificially manufactured. Compared to previous studies on technology-enabled social presence, interactions between subjects and the sources of social presence are set in the physical world in this study.

Instead of acting as the interaction medium, technology acts as the source of social presence in this study. As we seek to progress technological artifacts beyond conducting simple, well-defined tasks in the physical world, human-like qualities such as social presence will play an important role in determining its effectiveness in replacing the human actor. Our study reveals a significant and positive main effect for sensor greeting bell (informal surveillance) on both approach rate and conversion rate. This study expands contributes to existing social presence literature by providing empirical evidence social presence can be generated by technological artifacts not just in virtual or online settings, but in physical retail settings as well.

Third, this study empirically tests the effectiveness of surveillance methods in the deterrence of deviant behavior through a controlled experiment that applies and tests for treatment effects of surveillance technology. This contributes to the surveillance research stream that had previously been limited to understanding the impact of surveillance technology on deviant behavior through interviews (Gates 2010; Gill 2007) and surveys (Kajalo and Lindblom 2011; Lindblom and Kajalo 2011). This is hardly surprising, given the difficulty in generating credible counterfactuals to study deviant behavior such as theft. Indeed, the very presence of the experimenter in a lab experiment could influence the behavior of subjects engaged in an experimental task (Guerin 1986; Klein et al. 2012). Our field experiment setup overcomes the limitations of the presence of experimenters in lab experiments by studying while retaining the advantages of controlled experiments, which represent the most convincing method of constructing the counterfactual (Harrison and List 2004).

2.6.2 Implications for Practice

Over the past 15 years, video surveillance systems have gone from simple video acquisition displays to capable of performing complex procedures that can incorporate knowledge extraction algorithms such as face detection, face recognition, ID re-identification, and object detection and tracking (Tsakanikas and Dagiuklas 2018). In addition, the digitization of information and the rise of data mining have resulted in real advances in commercial consumer surveillance that led to the generation of electronic consumer profiles that allowed for previously unknown and unknowable consumption patterns and behavioral relationships the emerge (Pridmore and Zwick 2011). These trends led to the rise of information privacy concerns with not just the government (Dinev et al. 2006a; Dinev et al. 2008; Reddick et al. 2015), but also with businesses (Bélanger et al. 2002; Dinev and Hart 2006; Zuboff 2019).

Our study provides a useful reference for decision-making by retailers for the specific case of implementing surveillance technology to improve economic outcomes for unmanned retail shelves. While formal surveillance methods such as CCTV cameras are much more effective at reducing theft rate as compared to informal surveillance methods such as sensor greeting bells, it does not necessarily lead to the most favorable economic outcome for the retailer. Despite the ubiquity of CCTV surveillance, rising information privacy concerns could cause potential customers to avoid the retail shelf altogether, thus leading to lower revenue and gross profit for retail shelves that implemented CCTV cameras, despite the reduction in theft rate.

2.6.3 Limitations

One limitation of our study is that the unit of analysis for our data is aggregated to the daily level. Although we have user payment data at the subject level, we are only able to obtain theft rate data aggregated to the daily level. As we are only able to obtain theft rate data through the daily inventory checking of each retail shelf, we are unable to obtain subject-level theft rate data.

The second limitation for our study is that the merchandise we had on our unmanned retail shelf was bottled water, which is a relatively inexpensive product. We would expect the value of the merchandise to influence deviant behavior such as theft. For example, subjects might be more tempted to steal if the merchandise on the unmanned retail shelf was of a higher value since the risk to reward ratio will be more favorable. However, due to budgetary limitations, we were not able to conduct the field experiment with more expensive merchandise.

The third limitation of our study was that due to our unmanned field experimental setup, we were unable to conduct post-hoc manipulation checks for each treatment following subjects' interaction with the retail shelf. Instead, to ensure the effectiveness of the CCTV treatment, we had a signboard that explicitly reminded subjects that the area is under CCTV surveillance. From the regression results in Table 2-12, we see that all main effects are statistically significant except for sensor greeting bell's main effect on theft rate. Hence, we could infer that the experimental manipulations were effective.

The final limitation of our study is that the proposed field experiment takes place in China, which has some unique characteristics regarding retailing and privacy. As described in Liang et al. (2018), the Social Credit Score system of the PRC is currently unique and likely to have a significant influence on the research subjects. A minor shoplifting conviction in another setting could be much more significant for a research subject in the PRC, given the differing impacts based on the Social Credit Score system. Also, since privacy is a result of the impacts of cultural, social, and physical settings (Hong and Thong 2013), the differences in cultural characteristics between China and the Western world would mean that the subjects in our study might behave differently from subjects in a study conducted in western cultures, presenting a challenge to the external validity of our study.

CHAPTER 3 STUDY II: UNDERSTANDING PRIVACY-PRESERVING FEATURES IN DIGITAL CONTACT TRACING: AN EXTENDED PRIVACY CALCULUS PERSPECTIVE

3.1 INTRODUCTION

The recent COVID-19 pandemic as a global public health crisis has urged governments and health authorities to take proactive actions to prevent its outbreak, including work-from-home policies, social distancing, and even mandatory lockdowns. Contact tracing, a process to identify and isolate individuals who had close contact with known infected cases (Ahmed et al. 2020), is one of the most effective tools in curtailing the spread of the COVID-19 pandemic, said Emanuele Capobianco, the director of Health and Care at the International Federation of Red Cross and Red Crescent Societies (Walsh 2020). However, considering the large demand for labor, scientists believe the traditional approach of contact tracing using manual interviews may not be ideal or even feasible when there is a surge in the number of newly confirmed cases (Ahmed et al. 2020). Instead, digital contact tracing (DCT), which leverages digital technologies such as mobile apps to facilitate the contact tracing process, has emerged as a promising alternative to the traditional approach.

Technically, digital contact tracing (DCT) technologies can largely improve the effectiveness and efficiency of contact tracing by accessing the granular data of users' location, timing, and nearby contacts, as well as providing notification instantaneously upon case confirmation. Therefore, the health authorities in many countries put considerable effort into developing and deploying digital contact tracing (Asher 2020; Gerdo 2020). Singapore was one of the first countries that had implemented digital contact tracing (DCT) to control the spread of

COVID-19. In March 2020, the Singapore government developed its national DCT technology, which uses Bluetooth to track users' proximity to other users and alert those who encounter an infected person or someone at high risk of carrying the coronavirus. DCT helped Singapore accomplish what few countries could in March 2020, i.e., successfully controlling the spread of COVID-19 within its borders (Holmes 2020).

Despite the potential of DCT to help control the spread of COVID-19, recent reports show that the adoption and usage rate of DCT in many countries is low, to a large extent, due to users' privacy concerns (Garza 2020). This is far from satisfactory because DCT is only effective if the rate of adoption is sufficiently high beyond a critical mass (Riemer et al. 2020). In the United States, for example, no state has achieved a satisfactory adoption rate till November 10, 2020, where the highest, i.e., Virginia, has achieved an adoption rate of only 10.6% (Garza 2020). A widely acknowledged reason for the low adoption rate is privacy concerns (Asher 2020; Gerdo 2020; Redmiles 2020).

As such, a natural solution to increasing the adoption rate of DCT appears to be to alleviate privacy concerns by designing DCT technologies with privacy-preserving features, meaning that no Personally Identifiable Information (PII) will be revealed without users' explicit permission (Ahmed et al. 2020). We identify two particularly relevant privacy-preserving features in the DCT context, namely the collection of location data and data storage architecture. *Location data collection* can be designed to collect geolocation data, which is usually derived from GPS data, cell phone towers, Wi-Fi routers, etc., and can accurately reveal the exact location of a user, as well as relative location data which captures only relative proximity with other users through means of pairing like Bluetooth connections (Clarke 2001; Xu et al. 2009). In privacy-preserving design, only relative location data is collected. Geolocation data, which is regarded as more sensitive information that may cause considerable risk (Jones et al. 2019) is not collected. Therefore, DCT technologies that collect relative location data only would be regarded as a privacy-preserving design. The other privacy-preserving feature pertains to the *data storage location*. In the baseline design of centralized data storage location, contact tracing data is periodically and automatically uploaded to a centralized server for authorities to have up-to-date information, meaning users have no control over data provision. In the privacy-preserving design of decentralized data storage location, contact tracing data is first stored locally on users' personal devices and can later be uploaded to relevant authorities upon users' explicit permission. This affords control over data provision to the user.

Prior research has shown that privacy-preserving features can alleviate the risk of privacy invasion (Sutanto et al. 2013) or address users' privacy concerns (Karwatzki et al. 2017). However, they could also be counterproductive, such that they may inevitably hurt the system functionality because less data is available due to restrictions in data collection, and because the efficiency of utilizing the collected data is compromised (Cheng et al. 2018). In this study, we aim to examine the tension of the above two privacy-preserving features between preserving privacy and maintaining the effectiveness of contact tracing in the DCT context. In addition, we consider a contextual factor that could be leveraged as a potential solution for this tension, i.e., the size of existing user base. It is particularly important because the intended health, economic and societal benefits of the contact tracing technology can only be achieved if a significant user base adopts and uses it (Riemer et al. 2020). Thus, the size of the existing user base could in turn have an impact on how users perceive the effectiveness of DCT in terms of its functionality, and the effectiveness of the privacy-preserving features that has already been implemented. These would in turn drive adoption intentions. Specifically, we raise our research question as following:

RQ: What are the positive and negative impacts of privacy-preserving features in DCT, respectively? And what is the role of the existing user base?

To investigate this research question, we refer to the theoretical perspective of privacy calculus, which proposes a risk-benefit analysis for privacy-related intention and behavioral outcome. And we investigate how privacy-preserving features and existing user base influence two core constructs of the privacy calculus, i.e., privacy risk and perceived contact traceability. While privacy risk is often used in prior research, perceived contact traceability, which is defined as the effectiveness of a DCT technology in helping a community to improve the efficiency and accuracy of contact tracing, measures users' perception of the ability of DCT technologies to accurately trace the contacts of each user. Effective contact traceability does not only benefit the individual DCT users, but more importantly, the community or society for which the technology is intended to support.

Our results from an online experiment show that both privacy-preserving features, collection of relative location only (vs. geolocation and relative location) data, and a decentralized (vs. centralized) data storage location, can significantly reduce privacy risks for DCT users, but contrary to our expectation, such effects don't come at the price of compromising the contact traceability of DCT. In addition, our results support the dual role of existing user base, where one is to strengthen the effect of privacy-preserving features on reducing privacy risk, the other is to directly increase the perceived contact traceability of DCT. We also confirmed that privacy risk negatively influences while perceived contact traceability positively influences users' intention of using DCT technology.

Our study informs several important theoretical and practical implications. Firstly, we contribute to the privacy calculus literature by examining the less studied design features, specifically, the privacy-preserving features, as antecedents of privacy calculus. Their effects on both privacy risk and the benefit of contact tracing are examined. Secondly, we contribute to the literature on privacy-preserving design. Our findings show that the two privacy-preserving features indeed significantly reduce privacy risk, but surprisingly, do not lead users to perceive a decrease in the contact traceability of DCT. It challenges long-lasting views about the inevitable trade-offs between preserving privacy and maintaining functionality. Lastly, we contextualize the privacy calculus perspective beyond the well-studied settings of individual technology use, to a broader setting related to public health surveillance that aims at serving a whole society or community, i.e., DCT technologies. And we show that in the DCT context, contact traceability is an important driver for users' intention to use DCT technology. Practically, our findings suggest DCT developers implement designs with privacy-preserving features since they can effectively reduce users' privacy risk without causing a significant decrease in functionality and effectiveness. We also provide implications for health authorities and governments by demonstrating that expanding the user base when deploying DCT is crucial and rewarding.

3.2 LITERATURE REVIEW

3.2.1 Privacy Calculus

Privacy calculus has been the widely adopted theoretical perspective in the privacy literature to understand users' privacy behavior. Privacy calculus proposes that individuals make data disclosure decisions based on a risk-benefit analysis of all factors related to a privacy decision context (Dinev and Hart 2006; Hui et al. 2007; Jiang et al. 2013). More specifically, privacy calculus posits that individuals' subsequent intention and behavioral outcomes are determined positively by the expected utility, and negatively by the risk of a potential privacy violation (Culnan and Armstrong 1999). Table 3-1 summarizes the literature on privacy calculus.

While the risks examined in privacy calculus literature are mostly conceptualized as either privacy risks or privacy concerns, the conceptualization of benefit is more diverse depending on the context. Prior research has examined various benefits, including both tangible compensations, e.g., monetary incentives (Xu et al. 2009) as well as intangible benefits (Cheung et al. 2015; Jiang et al. 2013; Krasnova et al. 2010; Krasnova et al. 2012). In the context of social media, widely studied intangible benefits include social reward (Choi et al. 2018; Jiang et al. 2013; Morosan 2019; Wang et al. 2017), relationship building (Cheung et al. 2015; Krasnova et al. 2010), self-expression (James et al. 2015), and enjoyment (Cheung et al. 2015; Krasnova et al. 2010). Prior research has also investigated how these benefits are weighed against privacy concerns or privacy risk in determining individuals' intentions or behavioral outcomes. Xu et al. (2009), for example, found that in the context of location-based services, the personalization benefits users could derive from locatability can increase users' intention to disclose personal information, while privacy risk decreases such intention. Although these studies enrich our understanding of privacy calculus by investigating various contextualized benefits, we find that the existing literature focuses exclusively on the personal benefit for the focal user, while little research takes into consideration the benefit in a societal sense, for instance, the community. However, as some emerging technologies are being designed for societal good, e.g., public health surveillance systems, both technology designers and marketing campaigns emphasize the benefit for "everyone around you". It is therefore important to understand whether the privacy calculus is still valid in such contexts.

Existing privacy calculus research has extensively explored the antecedents of the core privacy calculus constructs, i.e., risk and benefit. The following categories of antecedents, namely individual characteristics, cognitive or affective factors, and contextual factors, have thus far been explored. Individual characteristics that influence privacy calculus constructs include extroversion (Kummer et al. 2018), privacy self-efficacy (Schade et al. 2018), general institutional trust (Kehr et al. 2015), general privacy concerns (Kehr et al. 2015; Li et al. 2014), prior experience with privacy invasion (Li et al. 2014), self-esteem (Wang et al. 2017), and demographic factors related to particular research contexts, e.g., age and health status in the context of virtual health community (Kordzadeh et al. 2016). For cognitive and/or affective factors, many studies consider trust (Cheung et al. 2015; Dinev et al. 2016; Schade et al. 2018) and perceived control (Dinev et al. 2016; Li et al. 2014; Wang et al. 2016; Zhao et al. 2012) as important antecedents of privacy risk or privacy concern. There are also studies investigating specific contextual factors, for example, industry self-regulation (Xu et al. 2009), government regulation (Xu et al. 2009), and provision of incentives (Xu et al. 2009; Zhao et al. 2012) in the context of location-based services, and network mutuality and profile diagnosticity in social media (Choi et al. 2018). Surprisingly, however, the study of design features as antecedents of privacy calculus was lacking. As is well-acknowledged that the IT artifact should play a central role in IS research (Benbasat and Zmud 2003), we believe it is important to shift the focus more to the design features, which should be directly related to users' assessment of privacy calculus. Privacy-preserving features are naturally one type of such design feature.

In sum, our review of the literature on privacy calculus reveals that, although privacy calculus is one of the most well-studied theoretical lenses in the privacy literature that has attracted tremendous empirical studies in a variety of contexts, there exist two important research gaps worthy of further exploration. One is that the benefits examined in the existing literature focus exclusively on personal benefits for the focal user. However, digital contact tracing (DCT) technologies during the COVID-19 pandemic are expected to benefit the entire community rather than just the individuals adopting the technology. In such circumstances, it would be more pertinent to contextualize the community concept within a privacy calculus perspective and examine its applicability. The other research gap lies in the antecedents of privacy calculus, where most existing research has considered factors relevant to the context or the user, but surprisingly little research has investigated technology design features that may directly influence privacy risks. The current study aims at filling these two research gaps by first contextualizing the benefit concept as contact traceability, which pertains to the society at large or the whole community rather than to individual users. And we investigate two privacy-preserving features as antecedents of privacy calculus. Next, we will present a detailed review of privacy-preserving features.

Table 3-1: Summary of Literature on Privacy Calculus

Study	Context	Antecedents of Privacy Calculus	Benefit Studied in Privacy Calculus
Kummer et al. (2018)	check-in service	contextual factor(s): place relevance; visit frequency; audience scope individual characteristic: extroversion	personal: conditional value
Dinev et al. (2016)	electronic health records (HER)	cognitive/affective factor(s): perceived control; trust; perceived effectiveness of technological mechanisms; perceived effectiveness of regulation mechanisms	personal: perceived benefit, convenience
Morosan (2019)	facial recognition system in hotels	/	personal: benefit of disclosure; social rewards
Gao et al. (2015)	healthcare wearable devices	/	personal: performance expectancy; hedonic benefit
Xu et al. (2011)	location-aware marketing	contextual factors: personalization	personal: perceived benefit of information disclosure
Schade et al. (2018)	location-based advertising	individual characteristic: privacy self-efficacy cognitive/ affective factor(s): brand trust	personal: advertising value

Xu et al. (2009)	location-based service	contextual factor(s): compensation; industry self-regulation; government regulation	personal: privacy benefit of disclosure (locatability and personalization)
Zhao et al. (2012)	location-based service	contextual factor(s): incentive provision; interaction promotion; privacy policy cognitive/ affective factors: perceived control	personal: extrinsic benefit (personalization); intrinsic benefit (connectedness)
Kehr et al. (2015)	mobile application that assists driving	contextual factor(s): information sensitivity individual characteristics: general institutional trust; general privacy concerns	personal: perceived benefit

Wang et al. (2016)	mobile applications	cognitive/ affective factor(s):
		personalized service;
		perceived severity of personal information disclosure; perceived control
			personal:
			perceived benefit

Shaw and Sergueeva (2019)	mobile commerce	cognitive/ affective factor(s): perceived privacy risk; perceived transaction risk; perceived privacy protection	personal: perceived value
Fox (2020)	mobile health	/	personal: perceived benefit

Li et al. (2014)	persona health record system	cognitive/ affective factor(s):
		perceived control;
		
		individual characteristics: previous privacy invasion; general privacy concern
			personal:
			perceived benefit

Teubner and Flath (2019)	sharing economy	cognitive/ affective factor(s): perceived audience size; personal connection	personal: economic benefit
Lankton et al. (2019)	social media	/	personal: trusting beliefs; personal interest
Choi et al. (2018)	social media	contextual factor(s): network mutuality; profile diagnosticity	personal: expected social capital gains
Wang et al. (2017)	social media	contextual factor(s)**:** application compatibility; application reputation; individual characteristics: self-esteem; flow experience	personal: monetary rewards; social rewards
James et al. (2015)	social media	/	personal: information seeking; socialization; self-expression; pleasing others
Cheung et al. (2015)	social media	cognitive/ affective factor(s):	personal:

		trust in SNS members; perceived control; trust in SNS service provider	convenience of maintaining existing relationships; new relationship building; self-representation; enjoyment
Krasnova et al. (2012)	social media	/	personal: enjoyment
Krasnova et al. (2010)	social media	cognitive/ affective factor(s): trust in SNS members; perceived control; trust in SNS service provider	personal: convenience; relationship building; self-representation; enjoyment
Jiang et al. (2013)	synchronous online social interactions	cognitive/ affective factor(s): perceived anonymity of self; perceived anonymity of others; perceived media richness; perceived intrusiveness	personal: social rewards

3.2.2 Privacy-preserving Features

Privacy-preserving features protect privacy by providing users with privacy-friendly options and features. These are typically choice, consent, and control options for users to decide, declare and control the kind of private information that can be shared with third parties; as well as the kind of third parties that may access this private information (Chen and Williams 2010; Chen and Williams 2013).

Oetzel and Spiekermann (2014) propose a privacy impact assessment methodology for privacy-preserving features. Two important steps in the methodology are the identification of privacy threats, followed by setting controls to counter each privacy threat. These controls could be technical controls directly incorporated into a system, or non-technical controls which include management and administrative controls, and accountability measures. Privacy-preserving features can thus be understood as the specific implementations of these controls within the IT artifact. Specifically, privacy-preserving features that have been previously studied in various contexts include location data collection (Barkhuus et al. 2008; Paefgen et al. 2012; Tsai et al. 2010; Xu et al. 2012), data storage and processing location (Sutanto et al. 2013), data sharing mechanisms (Heimbach and Hinz 2018; Hoadley et al. 2010), user anonymization (Cranor 1999), and information use transparency (Karwatzki et al. 2017).

In the context of public health surveillance, e.g., digital contact tracing, privacy-preserving features have been proposed based on principles such as *privacy-preserving data storage* and *data minimization.* Decentralized data storage proposed by some DCTs is one method to achieve *privacy-preserving data storage*. *Data minimization* refers to the practice that data collection, retention, and processing shall be limited to the minimum necessary amount of data that is needed to achieve the public health objective. Data collected, retained, and aggregated must be limited in scope (WHO 2020). Thus, data collection does not necessitate the identity or absolute location data of a user. Instead, relative location data can be used as it is sufficient for the purpose of deducing exposure to confirmed cases of COVID-19 without collecting absolute geographical information of a user, which could be a privacy risk.

Notably, despite the advocation of privacy-preserving features for their effects on reducing users' privacy risk (Ahmed et al. 2020; Akinbi et al. 2021; Li et al. 2020), an inherent tension between preserving privacy and maintaining functionality has been identified as a primary challenge (Bélanger and Crossler 2011). For example, Heimbach and Hinz (2018) proposed a privacy-preserving feature, a two-click sharing button that restricts the automatic transfer of information without users' explicit consent, and evaluated its effectiveness in the context of sharing content over online social networks. By requiring two separate clicks to activate the share button to share content, the privacy-preserving feature offers a higher level of *control* to users, thereby reducing information privacy risks associated with the control dimension. However, they found that the two-click design inevitably brings inconvenience for users by requiring one additional click. That is, the two-click design reduces privacy risk, but also reduces the efficiency of users' content sharing. Similarly, the literature highlights the privacy-personalization paradox, whereby using privacy-preserving features, such as improving information transparency (Awad and Krishnan 2006) and storing user information locally on their devices (Sutanto et al. 2013), will on one hand reduce privacy risk, but on the other hand, decrease the effectiveness of personalization.

Hence, these prior studies show that even though privacy-preserving features are expected to address privacy risks, there remains a potential trade-off between preserving users' privacy and maintaining or enhancing the functionality of the technology, hence it is recommended that the rigor of the controls exerted by the privacy-safe features matches the degree of privacy protection demanded by the context (Oetzel and Spiekermann 2014). In this study, we will investigate the above tension in the DCT context.

3.3 THEORETICAL DEVELOPMENT

3.3.1 Research Model

Our research model is summarized in Figure 3-1. We theorize the effects of two privacy-preserving features, i.e., location data collection (relative location only vs. geolocation and relative location data) and data storage location (decentralized vs. centralized), and a contextual factor, i.e., existing user base, on users' privacy calculus of using DCT technology.

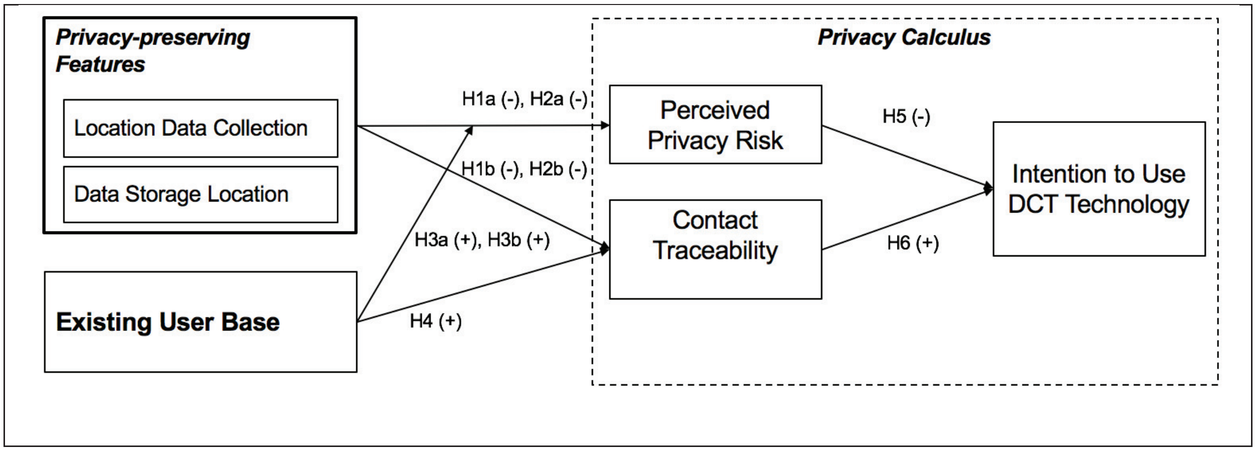


Figure 3-1: Research Model

3.3.2 Location Data Collection: Geolocation and Relative Location Data vs. Relative Location Data Only

Privacy-preserving features are designed to alleviate several different dimensions of privacy concerns. While considerable research has been conducted to conceptualize privacy concerns with different dimensions (Buchanan et al. 2007; Chen and Rea Jr 2004; Culnan 1993; Eastlick et al. 2006; Hong and Thong 2013; Liu et al. 2005; Malhotra et al. 2004), we focus on two widely-acknowledged dimensions that are particularly relevant to the context of DCT, namely, collection of personal information and control over the collected information, to identify the corresponding privacy-preserving features and examine their effects.

The collection dimension of privacy concern is defined as the degree to which a person is concerned about the type and amount of individual-specific data collected by the IT artifact (Malhotra et al. 2004). Regarding this dimension, we focus on the collection of location data. In the context of DCT, location data is collected to evaluate the risk of exposure and infection for a focal user by assessing whether he/she had been in proximate contact with other users who are infected or asymptomatic carriers. One way to collect location data could be to collect the absolute location data, aka geolocation data, which is derived from GPS data, cell phone towers, Wi-Fi routers, historical location data from third-party service providers, and reveals users' exact location with latitude and longitude information (Shukla et al. 2020). Alternatively, DCT technologies can be designed to collect the relative location data, which is generally derived from exchanging short-range handshakes with devices of other individuals in close proximity through channels such as Bluetooth (Shukla et al. 2020). When someone is found to be COVID positive, those who were close to him/her will be identified and alerted about potential infection. Prior privacy research has regarded geolocation data as fundamentally sensitive personal information (Jones et al. 2019) as it could reveal users' movement traces and result in the discovery of user identity and dynamics, especially when the geographic data are integrated with other behavioral data (Clarke 2001; Xu et al. 2009). In comparison, relative location data is believed to be less sensitive, because it is derived from the exchange of short-range data. It can only inform the relative proximity of two users (i.e., who is near you), rather than the exact location of the focal individual (i.e., where you are). Such limited information can hardly be used to infer the identity of the user and therefore would be regarded as less sensitive. Based on prior findings that collecting information of lower sensitivity induces lower privacy concern or privacy risk (Bansal and Gefen 2010; Malhotra et al. 2004), we propose that DCT technologies that collect relative location data only (vs. geolocation and relative location data) would decrease users' privacy risk:

H1a: Users will perceive DCT technologies that collect relative location data only to be associated with lower privacy risks compared to DCT technologies that collect both geolocation and relative location data.

As introduced before, there is often an inherent tension between protecting privacy and enhancing functionality (Abowd and Schmutte 2019; Dinur and Nissim 2003). In the DCT context, the tension between preserving users' privacy and enhancing the functionality of contact tracing is also a primary challenge. One reason that a privacy-preserving feature of DCT technology may diminish its functionality is the decreased information accuracy due to lesser information or less relevant and critical information collected. Abowd and Schmutte (2019)'s study shows that when national statistical agencies collect information about the population or the economy, they often face the difficulty of decreased data accuracy arising from increased privacy protection. In this study, we contextualize the benefit of DCT technologies to the society as contact traceability, defined as the effectiveness of a DCT technology in helping a community to improve the efficiency and accuracy of contact tracing. We argue that although the collection of relative location data only, as compared to geolocation and relative location data, is expected to reduce privacy risks for users, it would be accompanied with a compromise in contact traceability because relative location data is less informative than geolocation data. Indeed, collecting geolocation data can enhance the effectiveness of contact tracing that cannot be accomplished by collecting only relative location data. For example, if an infected person went to a shop, a DCT technology that collects relative location data can only inform individuals who have been concurrently in close contact with that infected person, whereas a DCT technology that also collects geolocation data can additionally remind people who have visited the shop but may not at the exact same time with the infected person of potential risks and alert the general public that may include those who have visited that shop but have not adopted the DCT technology. Thus, we hypothesize that:

H1b: DCT that collects relative location only (vs. geolocation and relative location) data will lead to lower perceived contract traceability.

3.3.3 Control: Centralized vs. Decentralized Data Storage Location

Prior research show individuals are often concerned about whether or not he/she might have adequate control over his/her personal information held in the IT artifact (Malhotra et al. 2004). In particular, the data storage location is one design feature that affords users different levels of control over their personal information (Li et al. 2020). Two alternatives are identified in the context of DCT, i.e., centralized vs. decentralized data storage locations. In a decentralized architecture, encounter logs are securely and locally stored, e.g., on the focal user's mobile phone. The encounter logs will only be provided to the authorities upon users' explicit permission when necessary, e.g., the user is diagnosed as infected. In a centralized architecture, however, users routinely upload the encounter log from the DCT technologies to a centralized server, such that the data is readily available to the authorities. Permission to access the data by the authorities is implied as long as users use the app. So, users would arguably lose some control of their data upon adoption of the DCT technology. Once users' personal data is stored in a centralized server, users have little control over potential privacy risks due to, for example, unauthorized access and undesired secondary use. Lower control over one's information usually introduces greater uncertainty about who has access to the information and how it is used (Dinev et al. 2006a). Research in the context of social media confirmed that users who have less control over their personal information report more privacy risks (Cheung et al. 2015; Zlatolas et al. 2015). Therefore, decentralized data storage location in DCT technologies, which affords users more control over whether and when to upload their encounter log, is supposed to alleviate privacy risk as compared with centralized data storage location. Accordingly, we propose that:

H2a: Users will perceive DCT technologies with a decentralized data storage location to be associated with lower privacy risk compared to DCT with a centralized data storage location.

However, similar to the privacy-preserving features of the collection of relative vs absolute and relative location data collection, decentralized data storage location may also imply a tension between privacy protection and functionality in DCT. A decentralized data storage location might diminish the efficiency of the contact tracing process. Specifically, in a centralized architecture for data storage location, as permission to access the encounter log to the centralized server is implied upon installation of the DCT technology, the data are readily available to the authorities. This allows health authorities' quick and efficient access to the data for contact tracing. So, if there is a need for contact tracing, such as when a user has been diagnosed as an infected case, contact tracing can be conducted immediately. However, for a decentralized architecture where each user exerts control over whether and when to share their encounter log to health authorities, contact tracing can only be conducted after each user gives explicit permission to access their data. Thus, the delay due to obtaining users' permission would make the process less timely and less efficient. In other words, in a decentralized architecture for data storage location, the efficiency of contact tracing and therefore the contact traceability will be compromised. This leads us to propose:

H2b: DCT with decentralized (vs. centralized) data storage location will lead to lower perceived contract traceability.

3.3.4 The Dual Role of Existing User Base

Although there is likely a tension between the effects of DCT on privacy preservation and utility enhancement, we suggest a contextual factor in DCT that could resolve this tension, i.e., existing user base, thereby maintaining utility while preserving privacy. Specifically, we propose a dual role of existing user base whereby a larger user base may 1) strengthen the effects of the two privacy-preserving features in reducing the privacy risks, and 2) directly improve the perceived contact traceability of DCT technologies. We elaborate on these two roles below.

Firstly, we refer to the theory of deindividuation (Diener et al. 1980) to hypothesize the moderating effects of existing user base for the effects of privacy-preserving features on privacy risk. Deindividuation is described as a state of diminished focus on self and reduced concern for social evaluation (Postmes and Spears 1998). Prior research on deindividuation shows when people are immersed in a large crowd, they view themselves as less traceable and identifiable. This means that a larger existing user base leads to greater sense of anonymity for each individual user (Jiang et al. 2013), which would subsequently lead them feel more protected and less concerned about their privacy. In the DCT context, we argue that the larger the existing user base is, the harder individual users' identity can be revealed. Therefore, users would perceive a higher level of anonymity, which leads to the state of deindividuation. Under the state of deindividuation, users would feel protected more easily, and therefore the effects of the privacy-preserving features, i.e., the collection of relative location only and the decentralized data storage location, would be stronger.

In contrast, when existing user base is small, we contemplate that even DCT is designed with privacy-preserving features, the privacy risk may still not be notably reduced. For example, in a small user network, even if geolocation data is not collected, or data is stored in a decentralized way, users may still be concerned that their identity might be revealed through other ways, like unintended inference and background knowledge attack. Therefore, although technically users' identities and personal information can be protected by the privacy-preserving designs, their perceived low anonymity in a small network may still lead them to perceive a high privacy risk. Hence, we hypothesize that:

H3a: The effect of collecting relative location only (vs. geolocation and relative location) data on privacy risk is stronger when there is a larger existing user base than when there is a smaller existing user base.

H3b: The effect of decentralized (vs. centralized) data storage location on privacy risk is stronger when there is a larger existing user base than when there is a smaller existing user base.

Drawing on network effects theory (Katz and Shapiro 1986), we propose another role of existing user base, which is to directly enhance contact traceability. Network effect posits that the value or utility users derive from a good or service are positively associated with the size of the network (Katz and Shapiro 1986). Information and communication technology (ICT) is a typical example that demonstrates network effect. For example, when the number of users of a mobile SNS platform increases, individual users would perceive the platform as more useful or enjoyable because they can connect with more users, therefore, they gain more benefit from using the platform (Lin and Lu 2011).

DCT technologies, as a public health surveillance system, are also expected to experience strong network effects, since its goal is to benefit the whole community by recording encounters between as many people as possible, tracking the infected case in an effective and timely manner. Health authorities claimed that the potential contribution of DCT technologies depends on the wide-scale adoption of the same tool (WHO 2020). To illustrate, imagine person A is diagnosed as infected with COVID-19 and was in close contact with person B, who was subsequently in contact with person C. In this case, C will not be notified of being at risk if B does not use the DCT. That is, the contact traceability will be decreased if there are not enough users in the network. Hence, having a large portion of the whole population using DCT technologies can result in an enhancement of contact traceability of the contact tracing. Thus, we hypothesize that:

H4: Existing user base will be positively associated with contact traceability.

3.3.5 Privacy Calculus Revisited

As introduced earlier, the novel context of DCT allows us to contextualize the benefit concept in privacy calculus to a broader sense. Because DCT as a public health surveillance system is designed to benefit not only the focal user but the whole community.

Based on privacy calculus, we propose that community benefit, which is contextualized as contact traceability in this research, would be evaluated against privacy risk to determine the user's intention to use the DCT technology. Previous studies suggest that privacy risk is negatively associated with the intention to adopt certain technology (Shaw and Sergueeva 2019), while perceived benefit is positively related to the intention to adopt (Shaw and Sergueeva 2019). Following such well-established theorization of privacy calculus, we argue that users would be less likely to adopt a DCT technology if the privacy risk is high. And we argue that the positive effect of benefit on behavioral intention applies to our conceptualization of community benefit, i.e., contact traceability. Specifically, users would be more likely to use a DCT technology if they perceive the technology is effective in contact tracing and protecting the community they are living in. Hence, we propose:

H5: Privacy risk is negatively related to users' intention to use a DCT technology.

H6: Contact traceability is positively related to users' intention to use a DCT technology.

3.4 METHODOLOGY

3.4.1 Experimental Design and Procedure

We conducted an online experiment using a 2 (location data collection: relative location only vs. geolocation and relative location) x 2 (data storage location: decentralized vs. centralized) x 2 (existing user base: low vs. high adoption rate) full-factorial between-subjects design. A mock-up contact tracing app, COVIDTRAIL, was developed for the experiment, where information about the data storage location, location data collection, and existing user base was manipulated as follows.

Manipulation of data storage location provided participants with information pertaining to where the collected data would be stored, as well as the procedures required for health authorities to access these data. Specifically, for conditions of decentralized data storage location, participants were informed that all encounter logs are securely and locally stored on their personal mobile phones and will not be accessible without their explicit permission. For conditions of centralized data storage location, participants were informed that all encounter logs are routinely uploaded and stored in a central server. Manipulation of location data collection informed participants whether their relative location data or geolocation data would be collected. In the conditions of collection of relative location data only, participants were informed that contact tracing would be done by collecting their exchange of Bluetooth signals and no geolocation data would be collected, thus the information collected would not reveal where they had been. In the conditions of collection of geolocation and relative location data, participants were explicitly told that geolocation data would be collected in addition to the exchange of Bluetooth signals. Existing user base was manipulated by telling participants the proportion of people in the subject's local community that have already installed the contact tracing app, i.e., 5% vs. 50%. Table 3-2 below shows the details of the manipulation.

Table 3-2: Details on Experimental Manipulation

Independent Variable	Manipulation	Description
Data Storage Location	Centralized Data Storage	All encounter logs are uploaded and stored in a central server to allow quick and efficient access by relevant personnel for the purpose of contact tracing. Each user's encounter log is routinely uploaded to a central server.
	Decentralized Data Storage	All encounter logs are securely and locally stored on your own phone and nobody can access your data without your permission. Each user's encounter log is securely stored on his or her own phone.
Location Data Collection	Collection of Geolocation and Relative Location Data	Geolocation data from a user's phone is collected by the app.
	Collection of Relative Location Data Only	No geolocation data are collected by the app.
Existing User Base	5% Adoption Rate	Around 5% of the people in your local community have already installed COVIDTRAIL.
	50% Adoption Rate	Around 50% of the people in your local community have already installed COVIDTRAIL.

Participants were randomly assigned to one of the eight conditions. To begin with, they were shown a webpage introducing the app COVIDTRAVIL with an infographic as well as statements of privacy policies to help explain to participants how COVIDTRAIL collects and utilizes data to conduct contact tracing. Depending on the condition to which the participant was assigned, the infographic and privacy policies stated whether geolocation and relative location data or relative location data only will be collected and whether data storage location will be centralized or decentralized (see Appendix B for a sample illustration). Participants were then asked to complete a survey, where the manipulation for existing user base was presented. They were asked to evaluate the app by answering survey questions about the app itself (i.e., as a manipulation check of the treatments), perceived privacy risks, contact traceability, intention to use, experience of using a smartphone, control variables (dispositional privacy concerns and perceived pandemic threat level), and demographics. Appendix C lists all the measurement items. All survey items were measured on a five-point Likert Scale. Appendix C also includes the questions for the manipulation checks.

3.4.2 Participants

Participants were recruited from Amazon Mechanical Turk. We restricted the task to Mechanical Turk Workers with an approval rate of at least 95% for their previous tasks. It has been shown that MTurkers with a Human Intelligence Task (HIT) approval rate, which represents the proportion of completed tasks that are approved by Requesters, of at least 95% score better on measures of attentiveness compared to MTurkers with a HIT approval ratio lower than 95% (Peer et al. 2014). By imposing the restriction, we hoped to overcome the issue of unreliable workers (Hunt and Scheetz 2019). Each participant was paid $0.40 for completing the survey, which is a reasonable payment for a survey that takes around 15 minutes to complete, given that the median hourly wage of the typical Mturk worker is $1.38 per hour (Horton and Chilton 2010). We got a total of 1447 responses, of which 552 failed an attention check which required subjects to input a uniquely generated 13-digit key displayed at the bottom of the mock-up app. Of the remaining 895 responses, 197 responses that took less than five minutes to complete were deemed to be not serious in their responses, as five minutes was the minimum amount of time needed to complete the survey when the experimenters attempted the survey. Hence, we got a total of 698 responses that passed the attention check and time check, amongst which 246 failed the manipulation check and were excluded from subsequent analysis, resulting in 452 responses for analysis. The average age of the subjects was 40. 48.2% of the participants were female. The participants were on average, very active smartphone users (mean = 4.66, five-point scale), which suggested that a digital mobile app would have been relevant to them. 400 out of 452 participants were from the US. Participants from other countries include Brazil (16), Italy (10), Canada (9), the UK (5), Spain (4), and the rest of the world (8).

3.5 DATA ANALYSIS AND RESULTS

In this section, we present the results of the proposed research model. Table 3-5 shows the privacy risk and contact traceability ANOVA test results.

3.5.1 Randomization Check

We collected data for control variables associated with the DCT context including dispositional privacy concerns and perceived pandemic threat level. Multivariate ANOVA results showed no significant difference across the conditions in terms of dispositional privacy concerns ($p > 0.05$) and perceived pandemic threat level ($p > 0.05$). Also, we find no significant differences across the conditions in terms of demographic variables, age ($p > 0.05$), gender ($p > 0.05$), and experience of using a smartphone ($p > 0.05$). which implies that randomization was successful and confounds with dispositional privacy concerns or perceived pandemic threat level would be unlikely.

3.5.2 Measurement Model

The measurement model of the constructs was assessed through convergent validity, discriminant validity, and construct reliability.

Convergent validity was assessed by determining whether items within the same construct correlate highly among themselves. The loadings of all the items in their respective latent constructs are higher than 0.7 (except for CT3), indicating good convergent validity (Comrey 1973).

Discriminant validity was assessed by checking whether all the item loadings on the intended construct are higher than loadings on other constructs (Cook and Campbell 1979). As shown in Table 3-3, the loadings of indicators on their respective latent variables were higher than the loadings of other indicators on these latent variables and the loadings of these indicators on other latent variables, indicating good discriminant validity. Table 3-4 also shows that the square root of the average variance extracted (AVE) of each latent variable was greater than the correlations between that latent variable and all other latent variables, which further supported adequate discriminant validity (Barclay et al. 1995).

Table 3-3: Loadings and Cross Loadings

Constructs	Items	PR	AdopINT	CT
Perceived Privacy Risk	PR1	**0.816**	-0.138	-0.083
	PR2	**0.863**	-0.202	-0.055
	PR3	**0.886**	-0.16	-0.135
	PR4	**0.879**	-0.079	-0.065
	PR5	**0.827**	-0.248	-0.065
Intention to Use	AdopINT1	-0.234	**0.913**	0.206
	AdopINT2	-0.243	**0.909**	0.206
	AdopINT3	-0.212	**0.932**	0.188
Contact traceability	CT1	-0.146	0.301	**0.747**
	CT2	-0.176	0.106	**0.804**
	CT3	0.021	0.317	**0.672**
	CT4	-0.024	-0.017	**0.833**

Adequate reliability was demonstrated as the measurement items generally loaded heavily on their respective constructs, with loadings above 0.70 (except CT3 at 0.67) (Table 3-3). The high composite reliability and Cronbach alpha scores shown in Table 3-4 also lent support (i.e., above 0.70) to satisfactory internal consistency.

Table 3-4: Internal Consistency and Discriminant Validity of Constructs

	Composite Reliability	Cronbach's Alpha	Perceived Privacy Risk	Contact Traceability	Adoption Intentions
Perceived Privacy Risk	0.924	.922	**0.842**		
Contact Traceability	0.867	.813	-0.238	**0.792**	
Adoption Intentions	0.97	.969	-0.448	0.434	**0.956**

Notes. Bold numbers show the square roots of the AVE values, while the off-diagonal elements are the correlations between the variables.

3.5.3 Results on Perceived Privacy Risk and Contact Traceability

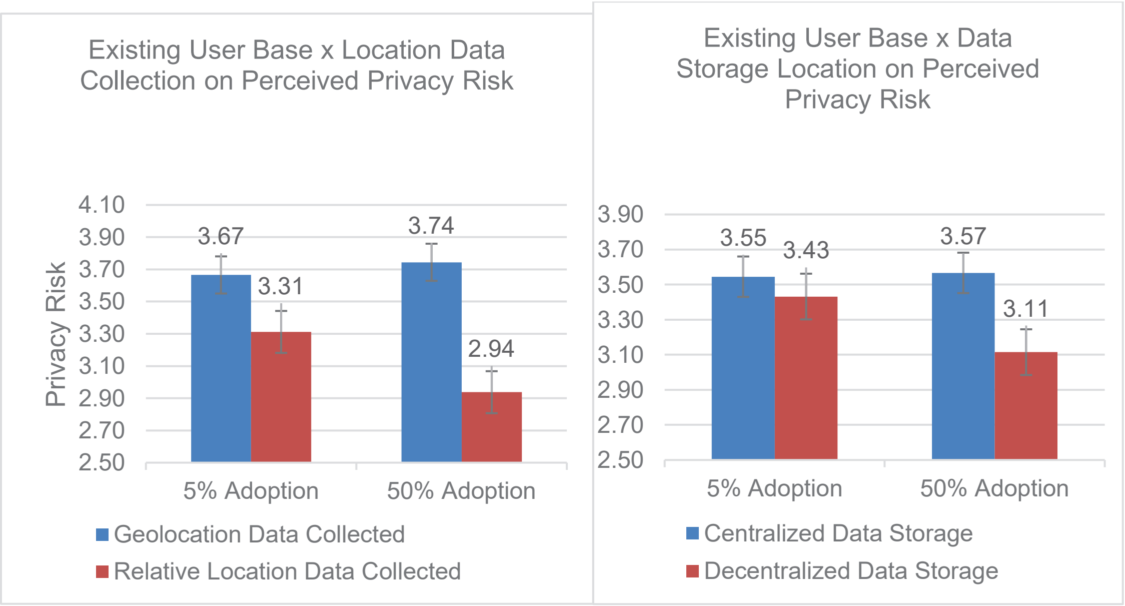
ANOVAs were conducted to test the effects of the two privacy-preserving features and existing user base on users' perceived privacy risk and contact traceability. Results are shown in Table 3-5.

Table 3-5: ANOVA Test – Main and Interaction Effects

Independent Variable	Dependent Variable	df	Mean square	F	p
Location Data Collection	Privacy Risk	1	37.83	38.28	.000
Data Storage Location	Privacy Risk	1	9.05	9.15	.003
Existing User Base	Privacy Risk	1	2.39	2.42	.121
Existing User Base × Location Data Collection	Privacy Risk	1	5.78	5.84	.016
Existing User Base × Data Storage Location	Privacy Risk	1	3.28	3.32	.069
Location Data Collection	Contact traceability	1	0.03	0.07	.798
Data Storage Location	Contact traceability	1	0.19	0.38	.539
Existing User Base	Contact traceability	1	2.40	4.85	.028

Location data collection was shown to significantly influence perceived privacy risk (F(1, 446) = 38.28, $p < 0.001$); that is, users perceived DCT technologies that collect relative location data only to be associated with lower privacy risks compared to DCT technologies that collect both geolocation and relative location data. Hence, H1a was supported. Data storage location was also found to have a significant effect on perceived privacy risk (F(1, 446) = 9.15, $p < 0.01$); that is, when data storage location is decentralized, users perceived significantly lower privacy risk than when data storage location is centralized. Hence, H2a was supported.

There was a positive significant interaction effect between existing user base and location data collection on privacy risk (F(1, 446) = 5.84, $p < 0.05$); that is, the effect of collecting relative location only (vs. geolocation and relative location) data on privacy risk is stronger when there is a larger existing user base than when there is a smaller existing user base. Hence, H3a was supported. We also found a marginally significant positive interaction between existing user base and data storage location on privacy risk (F(1, 446) = 3.32, $p = 0.07$). Hence, H3b was marginally supported. Figure 3-2 and Table 3-6 shows the interaction effects of existing user base and location data on privacy risk.



Note: Error bars represent +1/-1 SE.

Figure 3-2: Interaction Effects between Privacy-preserving Features and Existing User Base

Table 3-6: Means and Standard Deviations of the Eight Conditions

	Centralized data storage				Decentralized data storage			
	5% adoption rate		50% adoption rate		5% adoption rate		50% adoption rate	
Perceived privacy risk								
Collection of geolocation and relative location data	3.73	(0.11)	3.94	(0.14)	3.60	(0.12)	3.55	(0.14)
Collection of relative location data only	3.36	(0.13)	3.19	(0.14)	3.26	(0.13)	2.68	(0.15)
Contact traceability								
Collection of geolocation and relative location data	3.88	(0.10)	3.84	(0.11)	3.72	(0.08)	4.06	(0.08)
Collection of relative location data only	3.81	(0.10)	3.93	(0.10)	3.85	(0.09)	4.00	(0.08)

Contrary to our hypotheses, however, location data collection did not have a significant effect on contact traceability (F(1, 448) = 0.07, $p > 0.1$); hence, H1b was not supported. Data storage location did not affect contact traceability, either (F(1, 448) = 0.38, $p > 0.1$); hence, H2b was not supported. Existing user base was found to significantly increase perceived contact traceability (F(1, 448) = 4.85, $p < 0.05$). Hence, H4 was supported.

3.5.4 Results on Behavioral Intentions

A linear regression analysis was conducted to test the effects of perceived privacy risk and contact traceability on intention to use. Perceived privacy risk was found to have a significant negative effect on intention to use (β = -0.449, $p < 0.001$). Therefore, H5 was supported. Contact traceability was found to have a significant positive effect on intention to use (β = 0.692, $p < 0.001$). Therefore, H6 was supported.

3.6 DISCUSSION

3.6.1 Key Findings

Firstly, our results show that the two privacy-preserving features, namely the collection of relative location data only (vs. geolocation and relative location data) and a decentralized (vs. centralized) architecture for data storage location, can effectively reduce privacy risks for users of DCT technologies. The collection of relative location data only reduces privacy risk because less sensitive information is collected which makes users experience a higher level of anonymity. And a decentralized architecture for data storage location provides users with more control over their data, such that the privacy risk is reduced because they can determine whether and when to upload their information, e.g., encounter log.

However, contrary to our expectations, we found that these two privacy-preserving features do not result in a decrease in contact traceability. In earlier theorization, we argued that contact traceability would be diminished because the accuracy of collected information would be lower if collecting relative location only (vs. geolocation and relative location) data, and the efficiency of conducting the contact tracing process would be lower if data is stored in a decentralized (i.e., on individual users' devices) rather than a centralized (i.e., on a centralized server) way. Although the two mechanisms are believed to be valid and have empirical support in the literature, we posit that for a system aiming at benefiting the whole population e.g., DCT technologies, its utility evaluation based on individual users' subjective perceptions may not be consistent with the actual performance from a technical perspective. For one, users in the general population are usually not very tech-savvy and thus may not be sensitive to marginal changes in technological details. For another, as emphasized before, the DCT technologies are designed to benefit the whole population instead of just individual users. In such cases, it might not be very straightforward for individual users to make an accurate assessment of contact traceability. Therefore, it is reasonable that individual users do not perceive a compromise of the contact traceability of DCT technologies resulting from the design of privacy-preserving features.

Secondly, our results shed light on the role of an important contextual factor, i.e., existing user base, in deploying DCT technologies. We found that, on the one hand, a large existing user base can strengthen the effects of both privacy-preserving features on privacy risk. Specifically, we found that the effectiveness of collecting relative location only (vs. geolocation and relative location) data in preserving users' privacy is higher when there is a larger existing user base than when there is a smaller one. Similarly, the decentralized (vs. centralized) data storage location is also perceived to be more effective in reducing privacy risk when there is a larger existing user base than when there is a smaller one. On the other hand, we found that a larger existing user base can directly enhance the contact traceability of DCT technologies, explained by network effects, i.e., the utility of contact tracing is improved as more people are using the DCT technologies.

Thirdly, our results confirmed the established relationships in privacy calculus, with an emphasis on contextualizing the benefits from a community perspective, i.e., contact traceability. As in previous studies on privacy calculus, privacy risk is found to be negatively related to users' intention to use the DCT technology. Besides, we show that although the intention to use DCT technologies is an individual decision, the community or societal benefit of DCT, i.e., contact traceability, plays a considerable role in users' intention. This highlights the applicability of the privacy calculus perspective beyond a traditionally examined setting where technology is designed for individual users' needs and benefits.

3.6.2 Theoretical Contribution

Our study makes the following important contributions to the literature of both privacy calculus and privacy-preserving design. Firstly, we contribute to privacy calculus literature by examining the effect of design features that have been understudied, specifically, the privacy-preserving features, as antecedents of privacy calculus. The existing literature has examined various types of antecedents of privacy calculus, including individual characteristics (e.g., privacy self-efficacy) (Schade et al. 2018; Wang et al. 2017), contextual factors (e.g., compensation and regulation) (Schade et al. 2018; Wang et al. 2017), cognitive and affective factors (e.g., perceived control and trust) (Schade et al. 2018; Wang et al. 2017), while little research has investigated the effects of specific design features. In this study, we fill this research gap by studying how the two privacy-preserving features, i.e., the collection of relative location data only (vs. geolocation and relative location data) and a decentralized (vs. centralized) architecture for data storage location, can influence users' privacy risk and the functionality of DCT technologies. To the best of our knowledge, this is the first study to investigate the effects of privacy-preserving features on users' privacy calculus.

Secondly, we contribute to the literature on privacy-preserving design which showed that privacy-preserving features can alleviate the risk of privacy invasion (Sutanto et al. 2013) or address users' privacy concerns (Karwatzki et al. 2017). Specifically, although there is a long-held view about the tension between privacy-preservation and functionality (Cheng et al. 2018), e.g., accuracy and efficiency, our results show that the tension may not always be a concern. One important notion is whether the evaluation of privacy risk and utility is made at the same level. Specifically, if they are both evaluated at an individual level, i.e., individual users assess the extent of privacy risk for themselves, and the utility they can get from using a system for themselves, we should expect the existence of such a tension. However, in many cases, the tension involves not just an isolated individual but a group of people. For example, in the DCT context, individual users' privacy is often taken into consideration with the benefit of a large community. In such cases, although individual users may have a clear perception and evaluation about their own privacy risks, they may not be able to accurately evaluate how effective the contact tracing is and how much benefit it can bring to the whole community. Our study shows that in contexts where individual users give up personal privacy for the sake of a collective benefit, the existence of the tension between privacy-preservation and system functionality cannot be taken for granted and should be scrutinized more carefully.

Lastly, the benefits examined in the existing privacy calculus literature focused exclusively on personal benefits (Dinev et al. 2016; Jiang et al. 2013; Xu et al. 2011), while the novel and the unique context of DCT allowed us to theorize users' privacy calculus with an emphasis on community benefits. Different from the well-studied contexts where technologies are designed primarily for individual users, e.g., social media, location-based services, DCT technologies as a public health surveillance system aim to benefit not individual users but the community at large. However, we found little research considering the role of community or collective benefits in privacy calculus. Our findings can be generalized to other contexts where technologies are designed for collective good rather than individual utility.

3.6.3 Practical Implication

Our study also provides some practical implications for DCT design and deployment. Firstly, for developers of DCT technologies, we suggest that designing with privacy-preserving features brings benefits as intended, i.e., reducing users' privacy risk, but it does not necessarily come at the cost of compromising its functionality from individual users' perspective. Specifically, we show such effects of two privacy-preserving features that are particularly relevant to the DCT context, i.e., the collection of relative location data only (vs. geolocation and relative location data) and a decentralized (vs. centralized) architecture for data storage location. Our discussion above elaborated why they appear to be even more beneficial than they are supposed to be.

Secondly, our study suggests that health authorities or governments should spend great efforts in expanding the user base when deploying DCT. A larger existing user base would encourage individuals to use DCT technologies through two mechanisms. One is to strengthen the negative effects of privacy-preserving features on privacy risk, the other is to directly enhance the contact traceability of DCT technologies. Considering these benefits, health authorities and governments should consider persuading more people to use DCT technologies through means such as proactive advertising and public service announcement campaigns.

3.6.4 Limitation

We should acknowledge the following limitation of the current study. First, no actual app was developed so we could not observe the actual app download behaviors after users were exposed to the mock webpage. Although measuring intention is considered informative at the initial adoption stage (Xu et al. 2009), and represents an appropriate proxy for actual behavior (Trang et al. 2020), obtaining users' actual behavior would complement our result with more robust and convincing evidence. Therefore, future research could examine actual user behaviors in response to different privacy-preserving designs.

Second, as our study was conducted on Amazon Mechanical Turk, the subjects we have access to are heavily skewed to the US (89% of our participants). The effects of culture have previously been empirically tested and found to be significant in both privacy calculus (Dinev et al. 2006b) and government surveillance (Dinev et al. 2006a) contexts. Therefore, future research can consider testing our research model in different cultural contexts to increase its generalizability or enrich the theorization by incorporating cultural differences.

Third, the effects of individualism vs collectivism were not studied and could be an important control variable given the public health context of our study. While we could try to proxy for the control variable: individualism vs collectivism by using the originating countries of the subjects, this was not feasible due to data limitations. As discussed in the previous paragraph, 89% of our subjects are from the US, hence there might not be enough variation to tease out the effects of this control variable. Therefore, future research should collect data more evenly from different originating countries so we can use it as a proxy to control for individualism vs collectivism.

CHAPTER 4: CONCLUSION

The two studies in this thesis are focused on the themes of surveillance and privacy that are particularly important in helping us fully understand privacy-surveillance tradeoffs in different contexts. Study One studies the impact on economic outcomes in a retail context by exploring the impact of surveillance technology in an unmanned retail environment on consumer behavior. Study Two studies the impact on public health outcomes in the context of disease control by investigating how incorporating privacy-preserving features into digital contact tracing could impact adoption intentions.

Study One identifies a specific scenario where there could be an economic incentive to installing surveillance technology – unmanned retail shelves. It then proposes a design experiment to study the impact of surveillance technology on behavioral and economic outcomes. Particularly, the study compares the treatment effects of CCTV cameras and sensor greeting bells, which represent formal and informal surveillance respectively. The findings revealed that even though formal surveillance has a stronger deterrence on theft rate as compared to informal surveillance, its positive economic impact is canceled out by the reduction in customer approach rates due to privacy concerns.

Study Two is set against the backdrop of the COVID-19 pandemic and public health surveillance needs that are essential to help contain the virus. This study investigates the impact of privacy-preserving features on perceived privacy risk and contact traceability associated with a digital contact tracing solution, and ultimately the impact on adoption intentions. The findings revealed that these privacy-preserving features reduced perceived privacy risk as intended and that the effects of these privacy-preserving features on privacy risks are strengthened in the presence of a larger user base as compared to a smaller user base. On the other hand, the findings showed that these privacy-preserving features did not negatively impact the contact traceability of the digital contact tracing solution. Perceived privacy risk was found to have a significant negative impact on adoption intentions while contact traceability was found to have a significant positive impact on adoption intentions.

In summary, this thesis aims to uncover *if* and *how* a surveillance technology should be implemented, given its strong privacy implications. Overall, our findings suggest that surveillance technology's benefits may not always outweigh the costs arising from the resultant privacy risks. Hence, it is important that privacy risks be made part of the evaluation criteria for firms or users adopting new surveillance technology. As privacy concerns become an increasingly important consideration in adoption decisions, one solution could be to design privacy-preserving features into the surveillance artifact. Our findings suggest that a well-designed privacy-preserving feature could improve adoption by reducing privacy risk without negatively impacting functionality. Essentially, this thesis shows that to successfully implement surveillance technology for the benefit of society, we need to both understand and manage the associated privacy risks, whether through choosing a technology with inherently lower privacy risks or to directly reduce privacy risk through designing privacy-preserving features into the surveillance artifact.

These two studies have both theoretical and practical implications. First, this thesis contributes to the IS literature on surveillance by exploring how surveillance technology could impact user adoption behavior through multiple mechanisms. Existing research on the impact of surveillance has been largely limited to workplace (Ball 2010; D'Urso 2006; Watkins Allen et al. 2007) or government (Dinev et al. 2006a; Dinev et al. 2008; Reddick et al. 2015) surveillance programs. Hence, these existing studies do not sufficiently investigate the IT artifacts that are central to the act of surveillance. Through a field experiment, Study One investigates the impact on privacy concerns of two IT artifacts with formal and informal surveillance properties respectively. Facilitated by the unmanned context of our study, we were able to investigate the surveillance properties of the IT artifacts without having it been confounded by the presence of experimenters. Our findings revealed that privacy concerns are just one of the many mechanisms through which surveillance technology may impact user behavior. Formal surveillance was found to impact user behavior through assurance and deterrence mechanisms in addition to increased privacy concerns. Informal surveillance was found to impact user behavior through social presence. In Study Two, we studied digital contact tracing (DCT), a form of public health surveillance. Our findings showed that the privacy risk and contact traceability associated with the DCT would impact user adoption. In summary, while the findings may highlight that privacy is indeed a common concern when implementing surveillance technologies, there may also be other properties unique to the surveillance artifact being implemented that could also impact user response. Hence it is important that surveillance technologies are evaluated holistically as an IT artifact for implementation, as opposed to focusing solely on its privacy implications.

Second, this thesis shows that the privacy concerns discussed above can be effectively overcome through better product design. This contribution responds to the proposed research agenda in Plangger and Montecchi (2020)'s study, which noted that further research is needed to understand how consumer privacy concerns can be mitigated to better design products and services. By comparing formal and informal surveillance in Study One, our findings show that informal surveillance, which did not collect identifying information of subjects, did not significantly reduce the approach behavior of subjects. This implies that privacy concerns were successfully mitigated in the informal surveillance design. However, this had come at a cost in terms of functionality, which was reflected in our findings that the informal surveillance design did not significantly deter deviant behavior. This reflects an inherent tension between protecting privacy and enhancing functionality, as discussed in existing literature (Abowd and Schmutte 2019; Dinur and Nissim 2003). We further explored this tension between privacy-preservation and functionality in Study Two. Contrary to Study One, our results for Study Two show that the tension may not always be a concern. Study Two demonstrated that this tension between privacy-preservation and functionality does not necessarily hold when the perceived functionality must be evaluated on a collective scale. Specifically, while individual users may believe that privacy-preserving features reduce privacy risk as expected, the corresponding loss in functionality for the purpose of contact tracing may not be accurately evaluated by them since they are only impacted indirectly. As a result, the loss in functionality as perceived by individual users may be less than the actual lost in functionality to the community. This suggests that it may be possible to implement privacy-preserving features to overcome privacy concerns without compromising on functionality.

Third, we expand on existing literature that assessed tradeoffs between privacy and surveillance (Farivar 2018; Pavone and Esposti 2012; Strauß 2017). Study One enhances the privacy-surveillance tradeoff perspective by empirically testing for deterrence effects of surveillance technology on deviant behavior, providing a better understanding of the effectiveness of electronic surveillance relative to potential drawbacks in terms of privacy concerns. Practically, Study One provides more comprehensive insights to retailers making decisions to implement electronic surveillance. It suggests that the negative economic impact resulting from privacy concerns associated with formal electronic surveillance could outweigh the positive economic impact resulting from a reduction in theft. Thus, even though informal, lightweight surveillance technologies might be less effective in reducing theft rates, they could still lead to better economic outcomes. Study Two also contributes to the privacy-surveillance discussion by adopting a privacy calculus framework to the surveillance context. Study Two expands the privacy calculus framework by examining privacy-preserving features as antecedents of privacy calculus, which distinguishes itself from antecedents studied previously such as individual characteristics, contextual factors, and cognitive and affective factors. The novel context of DCT also allows us to theorize users' privacy calculus with an emphasis on community benefits, as compared to personal benefits in existing privacy calculus literature (Dinev et al. 2016; Xu et al. 2011), thus expanding the privacy calculus framework and contributing to the privacy-surveillance literature.

Overall, technological advances have blurred the distinction between privacy concerns arising from surveillance and information technologies, and the merging of these two fields heightens privacy concerns beyond simple additive effects (Kearns 1998). This is particularly evident in social media, where our personal video and imagery are governed by the same rules as global surveillance technologies and news footage (Flynn and Mackay 2017). Twitter, for example, is not just increasingly integrated with how news reports are written and broadcasted. The manner in which Twitter users engage with news events as they unfold gives Twitter the possibility of tracking the reading habits of users around the web (Higgins 2015).

The mechanisms investigated in this thesis are particularly important to the development and implementation of surveillance systems by expanding our understanding of the impact of different surveillance technologies and privacy-preserving designs on user outcomes. Additionally, given the growing capabilities of information technologies to act as surveillance technologies, understanding these mechanisms is increasingly important to our understanding of not just surveillance systems, but also any IT artifact with surveillance properties.

Despite privacy concerns, surveillance technologies remain critical in meeting future societal challenges. Besides the contexts of consumer retail and public health investigated in this thesis, future studies could evaluate the impact of surveillance technologies in equally important contexts such as public spaces and transport hubs. Additionally, while there has been ongoing research proposing privacy-preserving techniques (Bonetto et al. 2015; Dufaux and Ebrahimi 2008; Oleshchuk 2009), future studies could be carried out to evaluate the effectiveness of these newly developed privacy-preserving techniques in allaying information privacy concerns, as Study Two had done for privacy-preserving techniques identified for digital contact tracing (Bay et al. 2020).

As surveillance technologies become increasingly common in both private premises and public spaces (Koskela 2000), there is also a pressing need for future research to be conducted at the individual subject level. This will contribute to a deeper understanding of the mechanisms through which surveillance technologies maintain discipline or deter deviant behavior, as well as accompanying cues that could lead to information privacy concerns. Ultimately, the existence of privacy-surveillance tradeoffs points to the need for theory-driven design guidelines for the development of future surveillance systems.

Taken together, Study One and Study Two of this thesis enrich our understanding of the privacy-surveillance tradeoff by identifying the underlying mechanisms that lead to different user outcomes. As surveillance technologies become increasingly available and important in managing the growing challenges of society, further research in this direction could ensure that the advancement of surveillance technology does not proliferate into an information privacy threat.

APPENDIX A – ECONOMIC MODEL FOR STUDY I

The possible stages for a subject that passes by our unmanned retail shelf are described in Figure 5-1 below.

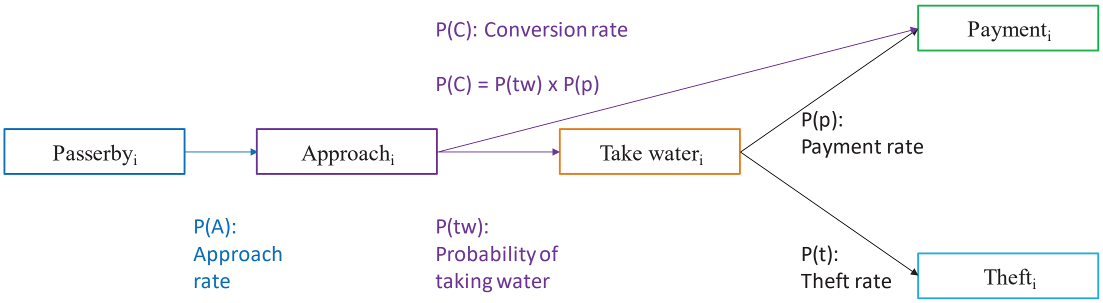


Figure 5-1: Potential Subject Actions

Our model specification for the overall economic impact at an unmanned retail shelf is:

$$\begin{aligned} Gross\ Profit \ &= Passerby_{Total} \times [P(A) \times P(C) \times ABPU \\ &\times (RPB - CPB) - P(A) \times P(tw) \times P(t) \times ABNPU \times (CPB)] \qquad (1) \end{aligned}$$

Where:

ABPU = Average number of bottles taken per paying user

ABNPU = Average number bottles taken per non-paying user

RPB = Revenue per bottle

CPB = Cost per bottle

P(A) = Approach rate

P(C) = Conversion rate

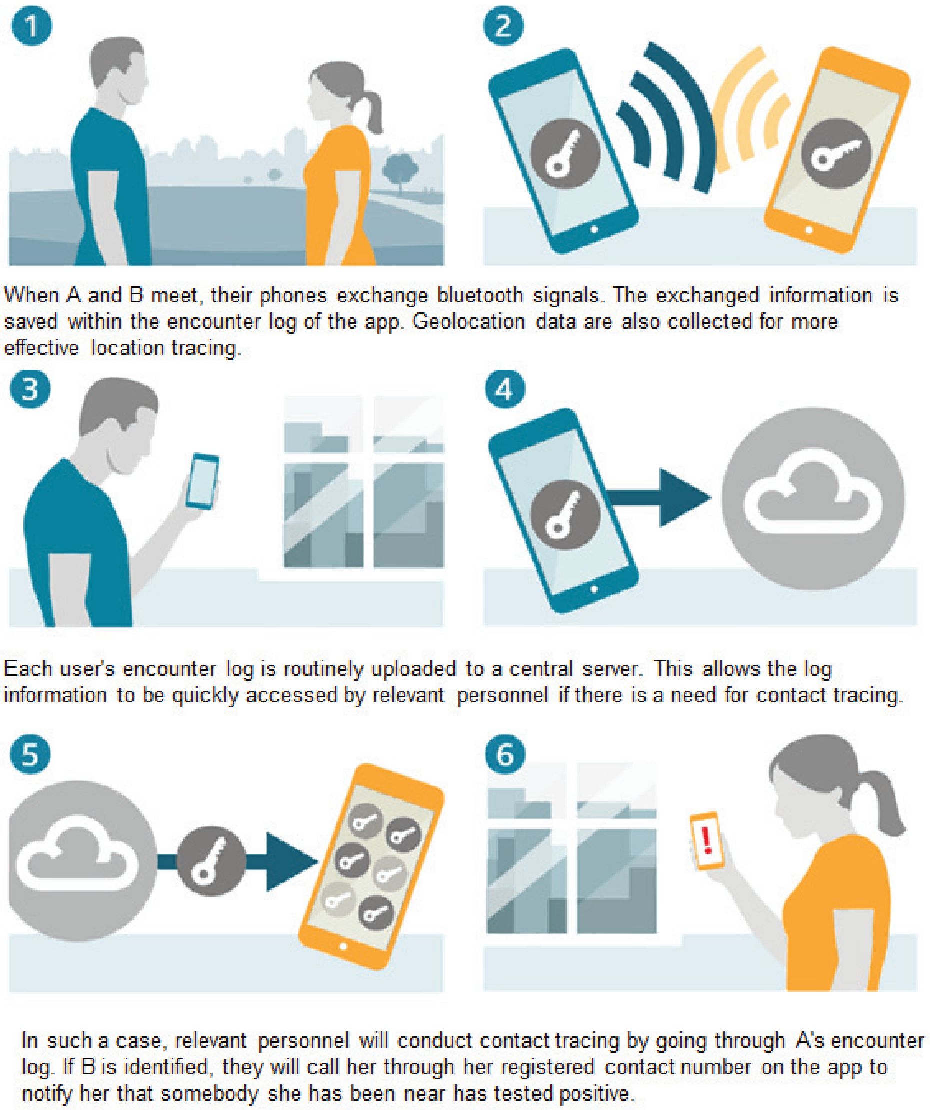
P(t) = Theft rate

P(p) = Payment rate

P(tw) = Take water rate

APPENDIX B – INFOGRAPHIC INTRODUCING COVIDTRAIL

For illustration, Figure 6-1 shows the infographic for the condition with geolocation data collection and centralized data storage location. Message for other conditions was manipulated as in Table 3-2.



When A and B meet, their phones exchange bluetooth signals. The exchanged information is saved within the encounter log of the app. Geolocation data are also collected for more effective location tracing.

Each user's encounter log is routinely uploaded to a central server. This allows the log information to be quickly accessed by relevant personnel if there is a need for contact tracing.

In such a case, relevant personnel will conduct contact tracing by going through A's encounter log. If B is identified, they will call her through her registered contact number on the app to notify her that somebody she has been near has tested positive.

Figure 6-1: Infographic Introducing COVIDTRAIL

APPENDIX C – MEASUREMENT ITEMS FOR STUDY II

Perceived Pandemic Threat Level – Self-developed measurement items

PPTL1: COVID-19 poses a severe threat to my community.

PPTL2: It is important to curb the spread of COVID-19.

PPTL3: Effective social distancing is important in the fight against COVID-19.

PPTL4: I am concerned that I may be susceptible to COVID-19.

PPTL5: There are many confirmed COVID-19 cases in my community.

Dispositional Privacy Concerns – Adapted from Malhotra et al. (2004)

DPC1: It is very important to me that I am aware and knowledgeable about how my personal information will be used.

DPC2: It usually bothers me when I am asked for my personal information online.

DPC3: Online companies should never share personal information with other organizations unless it has been authorized by the individuals who provided the information.

DPC4: In general, I am concerned about threats to my personal privacy today.

DPC5: User privacy is really a matter of users' right to exercise control and autonomy over decisions about how their information is collected, used and shared.

Perceived Privacy Risk – Adapted from Dinev and Hart (2006) and Xu et al. (2009)

PPR1: There is a risk for users of the contact tracing app because personal information (e.g., geolocation and/or contact data) collected by the contract tracing app could be exploited.

PPR2: Allowing the contact tracing app to access my personal information (e.g., geolocation and/or contact data) could involve many unexpected problems.

PPR3: It would be risky to provide my personal information (e.g., geolocation and/or contact data) to the contract tracing app.

PPR4: Disclosing my personal information (e.g., geolocation and/or contact data) to the contact tracing app could incur a high potential of safety, social and psychological losses.

PPR5: I am worried that my personal information is collected when I use this contact tracing app.

Contact traceability – Self-developed measurement items

CT1: The app can effectively trace the infection path of COVID-19 in my community.

CT2: The app can facilitate linking related infected cases since the encounter log stores all incidences of close contact between users.

CT3: If one has been in close contact with another user of the app, the app will always be able to successfully record that encounter.

CT4: As a user of the app, any close contact one has with other app users can be traced through the tracking data saved within the encounter log of the app.

Use Intentions – Adapted from Venkatesh et al. (2003)

Adoption Intention 1: I will seriously consider downloading the contact tracing app.

Adoption Intention 2: I would like to install the contact tracing app on my mobile phone.

Adoption Intention 3: I will likely use the contact tracing app.

Manipulation Check

Manipulation Check 1: Are Bluetooth data collected by COVIDTRAIL?

Manipulation Check 2: Are geolocation data collected by COVIDTRAIL?

Manipulation Check 3: Where are tracking data collected by the COVIDTRAIL stored?

Manipulation Check 4: Based on our assumption, around X% of the people in your local community have already installed COVIDTRAIL.

REFERENCES

Abowd, J. M., and Schmutte, I. M. 2019. "An Economic Analysis of Privacy Protection and Statistical Accuracy as Social Choices," *American Economic Review* (109:1), pp. 171-202.

Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., Seneviratne, A., Hu, W., Janicke, H., and Jha, S. K. 2020. "A Survey of COVID-19 Contact Tracing Apps," *IEEE Access* (8), pp. 134577-134601.

Akers, R. L. 1990. "Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken," *Journal of Criminal Law & Criminology* (81), pp. 653-676.

Akinbi, A., Forshaw, M., and Blinkhorn, V. 2021. "Contact Tracing Apps for the COVID-19 Pandemic: A Systematic Literature Review of Challenges and Future Directions for Neo-Liberal Societies," *Health Information Science and Systems* (9:1), pp. 1-15.

Andenaes, J. 1974. *Punishment and Deterrence*. University of Michigan Press.

Anderson, C. L., and Agarwal, R. 2011. "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information," *Information Systems Research* (22:3), pp. 469-490.

Argo, J. J., Dahl, D. W., and Manchanda, R. V. 2005. "The Influence of a Mere Social Presence in a Retail Context," *Journal of Consumer Research* (32:2), pp. 207-212.

Asher, S. 2020. "Tracetogether: Singapore Turns to Wearable Contact-Tracing COVID Tech." *BBC News*, from https://www.bbc.com/news/technology-53146360

Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization," *MIS Quarterly* (30:1), pp. 13-28.

Ball, K. 2010. "Workplace Surveillance: An Overview," *Labor History* (51:1), pp. 87-106.

Bannister, J. 1979. "Illegal Consumer Activity: An Exploratory Study of Shoplifting," *Quarterly Review of Marketing* (5), pp. 13-22.

Bansal, G., and Gefen, D. 2010. "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online," *Decision Support Systems* (49:2), pp. 138-150.

Barclay, D., Higgins, C., and Thompson, R. 1995. *The Partial Least Squares (PLS) Approach to Casual Modeling: Personal Computer Adoption Ans Use as an Illustration*.

Barkhuus, L., Brown, B., Bell, M., Sherwood, S., Hall, M., and Chalmers, M. 2008. "From Awareness to Repartee: Sharing Location within Social Groups," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 497-506.

Baron, R. M., and Kenny, D. A. 1986. "The Moderator–Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations," *Journal of Personality and Social Psychology* (51:6), pp. 1173-1182.

Bay, J., Kek, J., Tan, A., Hau, C. S., Yongquan, L., Tan, J., and Quy, T. A. 2020. "Bluetrace: A Privacy-Preserving Protocol for Community-Driven Contact Tracing across Borders," in: *Government Technology Agency-Singapore, Tech. Rep*.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017-1042.

Bélanger, F., Hiller, J. S., and Smith, W. J. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *The Journal of Strategic Information Systems* (11:3-4), pp. 245-270.

Bellia, P. L. 2008. "The Memory Gap in Surveillance Law," *University of Chicago Law Review* (75), p. 137.

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.

Blau, P. 1964. "Power and Exchange in Social Life." New York: J Wiley & Sons.

Bonetto, M., Korshunov, P., Ramponi, G., and Ebrahimi, T. 2015. "Privacy in Mini-Drone Based Video Surveillance," *2015 IEEE International Conference and Workshops on Automatic Face and Gesture recognition* IEEE, pp. 1-6.

Buchanan, T., Paine, C., Joinson, A. N., and Reips, U. D. 2007. "Development of Measures of Online Privacy Concern and Protection for Use on the Internet," *Journal of the American Society for Information Science and Technology* (58:2), pp. 157-165.

Campbell, J. E., and Carlson, M. 2002. "Panopticon. Com: Online Surveillance and the Commodification of Privacy," *Journal of Broadcasting & Electronic Media* (46:4), pp. 586-606.

Cappello, L. 2019. *None of Your Damn Business: Privacy in the United States from the Gilded Age to the Digital Age*. University of Chicago Press.

Cayford, M., and Pieters, W. 2018. "The Effectiveness of Surveillance Technology: What Intelligence Officials Are Saying," *The Information Society* (34:2), pp. 88-103.

Cayford, M., Pieters, W., and van Gelder, P. 2019. "Wanting It All–Public Perceptions of the Effectiveness, Cost, and Privacy of Surveillance Technology," *Journal of Information, Communication and Ethics in Society* (18:1), pp. 10-27.

Chandler, A. D., Hikino, T., and Chandler, A. D. 2009. *Scale and Scope: The Dynamics of Industrial Capitalism*. Harvard University Press.

Chen, K., and Rea Jr, A. I. 2004. "Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques," *Journal of Computer Information Systems* (44:4), pp. 85-92.

Chen, S., and Williams, M.-A. 2010. "Privacy: An Ontological Problem," *Pacific Asia Conference on Information Systems, PACIS 2010*.

Chen, S., and Williams, M.-A. 2013. "Grounding Privacy-by-Design for Information Systems," *Pacific Asia Conference on Information Systems, PACIS 2013*, p. 107.

Cheng, H., Rong, C., Qian, M., and Wang, W. 2018. "Accountable Privacy-Preserving Mechanism for Cloud Computing Based on Identity-Based Encryption," *IEEE Access* (6), pp. 37869-37882.

Cheung, C., Lee, Z. W., and Chan, T. K. 2015. "Self-Disclosure in Social Networking Sites," *Internet Research* (25:2), pp. 279-299.

Choi, B., Wu, Y., Yu, J., and Land, L. 2018. "Love at First Sight: The Interplay between Privacy Dispositions and Privacy Calculus in Online Social Connectivity Management," *Journal of the Association for Information Systems* (19:3), pp. 124-151.

Clarke, R. 1988. "Information Technology and Dataveillance," *Communications of the ACM* (31:5), pp. 498-512.

Clarke, R. 1999. "Internet Privacy Concerns Confirm the Case for Intervention," *Communications of the ACM* (42:2), pp. 60-67.

Clarke, R. 2001. "Person Location and Person Tracking-Technologies, Risks and Policy Implications," *Information Technology & People* (14:2), pp. 206-231.

Cox, A. D., Cox, D., Anderson, R. D., and Moschis, G. P. 1993. "Research Note: Social Influences on Adolescent Shoplifting—Theory, Evidence, and Implications for the Retail Industry," *Journal of Retailing* (69:2), pp. 234-246.

Cozens, P., and Love, T. 2015. "A Review and Current Status of Crime Prevention through Environmental Design (CPTED)," *Journal of Planning Literature* (30:4), pp. 393-412.

Cranor, L. F. 1999. "Internet Privacy," *Communications of the ACM* (42:2), pp. 28-38.

Culnan, M. J. 1993. ""How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3), pp. 341-363.

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.

D'Alto, J. 1992. "A Lock on the Market: The Growing Demand for Security Systems in Europe," *The Journal of European Business* (3:5), p. 46.

D’Urso, S. C. 2006. "Who’s Watching Us at Work? Toward a Structural–Perceptual Model of Electronic Monitoring and Surveillance in Organizations," *Communication Theory* (16:3), pp. 281-303.

Dinev, T., Albano, V., Xu, H., D’Atri, A., and Hart, P. 2016. "Individuals’ Attitudes Towards Electronic Health Records: A Privacy Calculus Perspective," in *Advances in Healthcare Informatics and Analytics*. Springer, pp. 19-50.

Dinev, T., Bellotto, M., Hart, P., Russo, V., and Serra, I. 2006a. "Internet Users' Privacy Concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences between Italy and the United States," *Journal of Global Information Management* (14:4), pp. 57-93.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006b. "Privacy Calculus Model in E-Commerce–a Study of Italy and the United States," *European Journal of Information Systems* (15:4), pp. 389-402.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.

Dinev, T., Hart, P., and Mullen, M. R. 2008. "Internet Privacy Concerns and Beliefs About Government Surveillance–an Empirical Investigation," *The Journal of Strategic Information Systems* (17:3), pp. 214-233.

Dinur, I., and Nissim, K. 2003. "Revealing Information While Preserving Privacy," *Proceedings of the Twenty-Second ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, pp. 202-210.

Dootson, P., Lings, I., Beatson, A., and Johnston, K. A. 2017. "Deterring Deviant Consumer Behaviour: When 'It's Wrong, Don't Do It'doesn't Work," *Journal of Marketing Management* (33:15-16), pp. 1355-1383.

Doumbouya, A., Camara, O. T., Mamie, J., Intchama, J. F., Jarra, A., Ceesay, S., Guèye, A., Ndiaye, D., Beibou, E., and Padilla, A. 2017. "Assessing the Effectiveness of Monitoring Control and Surveillance of Illegal Fishing: The Case of West Africa," *Frontiers in Marine Science* (4), p. 50.

Driver, F. 1985. "Power, Space, and the Body: A Critical Assessment of Foucault's Discipline and Punish," *Environment and Planning D: Society and Space* (3:4), pp. 425-446.

Dufaux, F., and Ebrahimi, T. 2008. "Scrambling for Privacy Protection in Video Surveillance Systems," *IEEE Transactions on Circuits and Systems for Video Technology* (18:8), pp. 1168-1174.

Dufaux, F., Ouaret, M., Abdeljaoued, Y., Navarro, A., Vergnenègre, F., and Ebrahimi, T. 2006. "Privacy Enabling Technology for Video Surveillance," *Mobile Multimedia/Image Processing for Military and Security Applications*, p. 62500M.

Eastlick, M. A., Lotz, S. L., and Warrington, P. 2006. "Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment," *Journal of Business Research* (59:8), pp. 877-886.

Economics, L. 2010. "Study on the Economic Benefits of Privacy-Enhancing Technologies (Pets): Final Report to the European Commission, Dg Justice, Freedom and Security."

Ekblom, P. 1986. *The Prevention of Shop Theft: An Approach through Crime Analysis*. Home Office London.

Fairchild, A., Gostin, L., and Bayer, R. 2020. "Vexing, Veiled, and Inequitable: Social Distancing and the "Rights" Divide in the Age of COVID-19," *The American Journal of Bioethics* (20:7), pp. 55-61.

Fairweather, N. B. 1999. "Surveillance in Employment: The Case of Teleworking," *Journal of Business Ethics* (22:1), pp. 39-49.

Farivar, C. 2018. *Habeas Data : Privacy Vs. The Rise of Surveillance Tech*. Melville House Publishing.

Farkas, C., Brodsky, A., and Jajodia, S. 2006. "Unauthorized Inferences in Semistructured Databases," *Information Sciences* (176:22), pp. 3269-3299.

Flechais, I., Riegelsberger, J., and Sasse, M. A. 2005. "Divide and Conquer: The Role of Trust and Assurance in the Design of Secure Socio-Technical Systems," *Proceedings of the 2005 Workshop on New Security Paradigms*, pp. 33-41.

Flynn, S., and Mackay, A. 2017. *Spaces of Surveillance: States and Selves*. Springer.

Foucault, M. 1977. *Discipline and Punish: The Birth of the Prison. Tr. A. Sheridan*.

Foucault, M. 1980. *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977*. Vintage.

Fox, G. 2020. "“To Protect My Health or to Protect My Health Privacy?” a Mixed-Methods Investigation of the Privacy Paradox," *Journal of the Association for Information Science and Technology* (71:9), pp. 1015-1029.

Friedman, B. A., and Reed, L. J. 2007. "Workplace Privacy: Employee Relations and Legal Implications of Monitoring Employee E-Mail Use," *Employee Responsibilities and Rights Journal* (19:2), pp. 75-83.

Fulk, J., Steinfield, C. W., Schmitz, J., and Power, J. G. 1987. "A Social Information Processing Model of Media Use in Organizations," *Communication Research* (14:5), pp. 529-552.

Fyfe, N. R., and Bannister, J. 1996. "City Watching: Closed Circuit Television Surveillance in Public Spaces," *Area* (28:1), pp. 37-46.

Gao, Y., Li, H., and Luo, Y. 2015. "An Empirical Study of Wearable Technology Acceptance in Healthcare," *Industrial Management & Data Systems* (115:9), pp. 1704-1723.

Garrison, D. R., Anderson, T., and Archer, W. 2001. "Critical Thinking, Cognitive Presence, and Computer Conferencing in Distance Education," *American Journal of Distance Education* (15:1), pp. 7-23.

Garza, A. d. l. 2020. "Contact Tracing Apps Were Big Tech's Best Idea for Fighting COVID-19. Why Haven't They Helped?" *Time*, from https://time.com/5905772/covid-19-contact-tracing-apps/

Gates, K. 2010. "The Tampa “Smart Cctv” Experiment," *Culture Unbound* (2:1), pp. 67-89.

Gefen, D. 1997. *Building Users' Trust in Freeware Providers and the Effects of This Trust on Users' Perceptions of Usefulness, Ease of Use and Intended Use of Freeware*. Georgia State University.

Gefen, D., and Straub, D. 2003. "Managing User Trust in B2c E-Services," *e-Service* (2:2), pp. 7-24.

Gefen, D., and Straub, D. W. 2004. "Consumer Trust in B2c E-Commerce and the Importance of Social Presence: Experiments in E-Products and E-Services," *Omega* (32:6), pp. 407-424.

Gelman, A. 2005. "Analysis of Variance—Why It Is More Important Than Ever," *The Annals of Statistics* (33:1), pp. 1-53.

Gerdo, V. 2020. "Russia Develops Coronavirus Contact-Tracing App." *The Moscow Times*, from https://www.themoscowtimes.com/2020/11/17/russia-develops-coronavirus-contact-tracing-app-a72068

Gibbs, J. P. 1968. "Crime, Punishment, and Deterrence," *The Southwestern Social Science Quarterly* (48:4), pp. 515-530.

Gill, M. 2007. "Shoplifters on Shop Theft: Implications for Retailers."

Guadagno, R. E., Blascovich, J., Bailenson, J. N., and McCall, C. 2007. "Virtual Humans and Persuasion: The Effects of Agency and Behavioral Realism," *Media Psychology* (10:1), pp. 1-22.

Guerin, B. 1986. "Mere Presence Effects in Humans: A Review," *Journal of Experimental Social Psychology* (22:1), pp. 38-77.

Guffey, H. J., Harris, J. R., and Laumer, J. F. 1979. "Shopper Attitudes toward Shoplifting and Shoplifting Preventive Devices," *Journal of Retailing* (55:3), pp. 75-89.

Gupta, A., Kannan, K., and Sanyal, P. 2018. "Economic Experiments in Information Systems," *MIS Quarterly* (42:2), pp. 595-606.

Harrison, G. W., and List, J. A. 2004. "Field Experiments," *Journal of Economic Literature* (42:4), pp. 1009-1055.

Hayes, A. F. 2009. "Beyond Baron and Kenny: Statistical Mediation Analysis in the New Millennium," *Communication Monographs* (76:4), pp. 408-420.

Heimbach, I., and Hinz, O. 2018. "The Impact of Sharing Mechanism Design on Content Sharing in Online Social Networks," *Information Systems Research* (29:3), pp. 592-611.

Higgins, P. 2015. "Twitter Axes Accountability Projects, Sparing Politicians Embarrassment." Electronic Frontier Foundation.

Hoadley, C. M., Xu, H., Lee, J. J., and Rosson, M. B. 2010. "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry," *Electronic Commerce Research and Applications* (9:1), pp. 50-60.

Holmes, A. 2020. "Singapore Is Using a High-Tech Surveillance App to Track the Coronavirus, Keeping Schools and Businesses Open. Here's How It Works." *Business Insider*, from https://www.businessinsider.com/singapore-coronavirus-app-tracking-testing-no-shutdown-how-it-works-2020-3

Hong, W., and Thong, J. Y. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Quarterly* (37:1), pp. 275-298.

Horton, J. J., and Chilton, L. B. 2010. "The Labor Economics of Paid Crowdsourcing," *Proceedings of the 11th ACM Conference on Electronic Commerce*, pp. 209-218.

Hui, K.-L., Teo, H. H., and Lee, S.-Y. T. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly* (31:1), pp. 19-33.

Hunt, N. C., and Scheetz, A. M. 2019. "Using MTurk to Distribute a Survey or Experiment: Methodological Considerations," *Journal of Information Systems* (33:1), pp. 43-65.

James, T. L., Warkentin, M., and Collignon, S. E. 2015. "A Dual Privacy Decision Model for Online Social Networks," *Information & Management* (52:8), pp. 893-908.

Jiang, Z., Heng, C. S., and Choi, B. C. 2013. "Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions," *Information Systems Research* (24:3), pp. 579-595.

Jones, M., Johnson, M., Shervey, M., Dudley, J. T., and Zimmerman, N. 2019. "Privacy-Preserving Methods for Feature Engineering Using Blockchain: Review, Evaluation, and Proof of Concept," *Journal of Medical Internet Research* (21:8), p. e13600.

Kajalo, S., and Lindblom, A. 2011. "An Empirical Analysis of Retail Entrepreneurs’ Approaches to Prevent Shoplifting," *Security Journal* (24:4), pp. 269-282.

Kajalo, S., and Lindblom, A. 2016. "The Role of Formal and Informal Surveillance in Creating a Safe and Entertaining Retail Environment," *Facilities* (34:3/4), pp. 219-232.

Karwatzki, S., Dytynko, O., Trenz, M., and Veit, D. 2017. "Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization," *Journal of Management Information Systems* (34:2), pp. 369-400.

Katz, M. L., and Shapiro, C. 1986. "Technology Adoption in the Presence of Network Externalities," *Journal of Political Economy* (94:4), pp. 822-841.

Kearns, T. B. 1998. "Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns," *William & Mary Bill of Rights Journal* (7), pp. 975-1011.

Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus," *Information Systems Journal* (25:6), pp. 607-635.

Kennedy, K. C. 1983. "A Critical Appraisal of Criminal Deterrence Theory," *Dickinson Law Review* (88), pp. 1-13.

Klein, O., Doyen, S., Leys, C., Magalhães de Saldanha da Gama, P. A., Miller, S., Questienne, L., and Cleeremans, A. 2012. "Low Hopes, High Expectations: Expectancy Effects and the Replicability of Behavioral Experiments," *Perspectives on Psychological Science* (7:6), pp. 572-584.

Kordzadeh, N., Warren, J., and Seifi, A. 2016. "Antecedents of Privacy Calculus Components in Virtual Health Communities," *International Journal of Information Management* (36:5), pp. 724-734.

Koskela, H. 2000. "'The Gaze without Eyes': Video-Surveillance and the Changing Nature of Urban Space," *Progress in Human Geography* (24:2), pp. 243-265.

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), pp. 109-125.

Krasnova, H., Veltri, N. F., and Günther, O. 2012. "Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture," *Business & Information Systems Engineering* (4:3), pp. 127-135.

Kumar, N., and Benbasat, I. 2006. "Research Note: The Influence of Recommendations and Consumer Reviews on Evaluations of Websites," *Information Systems Research* (17:4), pp. 425-439.

Kummer, T.-F., Ryschka, S., and Bick, M. 2018. "Why Do We Share Where We Are? The Influence of Situational Factors on the Conditional Value of Check-in Services," *Decision Support Systems* (115), pp. 1-12.

Lankton, N. K., McKnight, D. H., and Tripp, J. F. 2019. "Understanding the Antecedents and Outcomes of Facebook Privacy Behaviors: An Integrated Model," *IEEE Transactions on Engineering Management* (67:3), pp. 697-711.

Lee, E. 2017. "Top 10 Chinese Unmanned Stores in 2017." *Technode*, from https://technode.com/2017/12/27/top-10-chinese-unmanned-stores-2017-2/

Li, H., Gupta, A., Zhang, J., and Sarathy, R. 2014. "Examining the Decision to Use Standalone Personal Health Record Systems as a Trust-Enabled Fair Social Contract," *Decision Support Systems* (57), pp. 376-386.

Li, T., Faklaris, C., King, J., Agarwal, Y., Dabbish, L., and Hong, J. I. 2020. "Decentralized Is Not Risk-Free: Understanding Public Perceptions of Privacy-Utility Trade-Offs in COVID-19 Contact-Tracing Apps," in: *arXiv Preprint arXiv:2005.11957*.

Li, X., and Ouyang, Y. 2012. "Reliable Traffic Sensor Deployment under Probabilistic Disruptions and Generalized Surveillance Effectiveness Measures," *Operations Research* (60:5), pp. 1183-1198.

Liang, F., Das, V., Kostyuk, N., and Hussain, M. M. 2018. "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure," *Policy & Internet* (10:4), pp. 415-453.

Lin, B., Hastings, D. A., and Martin, C. 1994. "Shoplifting in Retail Clothing Outlets," *International Journal of Retail & Distribution Management* (22:7), pp. 24-29.

Lin, K.-Y., and Lu, H.-P. 2011. "Why People Use Social Networking Sites: An Empirical Study Integrating Network Externalities and Motivation Theory," *Computers in Human Behavior* (27:3), pp. 1152-1161.

Lindblom, A., and Kajalo, S. 2011. "The Use and Effectiveness of Formal and Informal Surveillance in Reducing Shoplifting: A Survey in Sweden, Norway and Finland," *The International Review of Retail, Distribution and Consumer Research* (21:2), pp. 111-128.

Liu, C., Marchewka, J. T., Lu, J., and Yu, C.-S. 2005. "Beyond Concern—a Privacy-Trust-Behavioral Intention Model of Electronic Commerce," *Information & Management* (42:2), pp. 289-304.

Lo, L. 1994. "Exploring Teenage Shoplifting Behavior: A Choice and Constraint Approach," *Environment and Behavior* (26:5), pp. 613-639.

Lucky, R. W. 2008. "Zero Privacy [Reflections]," *IEEE Spectrum* (45:7), pp. 20-20.

Luhmann, N. 1979. *Trust and Power*. John Wiley & Sons.

Lyon, D. 2001. *Surveillance Society: Monitoring Everyday Life*. McGraw-Hill Education (UK).

Lyon, D. 2008. "Surveillance Society." Talk for Festival del Diritto, Piacenza, Italia.

Ma, Y. 2019. "Market Share of Mobile Payments in China from 2011 to 2018." *Statista*, from https://www.statista.com/statistics/1050151/china-market-share-of-mobile-payments/#:~:text=In%202018%2C%20the%20market%20share,their%20main%20means%20of%20payment.

Machanavajjhala, A., Kifer, D., Gehrke, J., and Venkitasubramaniam, M. 2007. "L-Diversity: Privacy Beyond K-Anonymity," *ACM Transactions on Knowledge Discovery from Data (TKDD)* (1:1), pp. 3-es.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.

Mason, R. O. 1986. "Four Ethical Issues of the Information Age," *MIS Quarterly* (10:1), pp. 5-12.

Matsueda, R. L., Kreager, D. A., and Huizinga, D. 2006. "Deterring Delinquents: A Rational Choice Model of Theft and Violence," *American Sociological Review* (71:1), pp. 95-122.

McKnight, D. H., Cummings, L. L., and Chervany, N. L. 1998. "Initial Trust Formation in New Organizational Relationships," *Academy of Management Review* (23:3), pp. 473-490.

Moffatt, R. 1983. "Crime Prevention through Environmental Design - a Management Perspective," *Canadian Journal of Criminology and Criminal Justice* (25), p. 19.

Moncrieff, S., Venkatesh, S., and West, G. A. 2009. "Dynamic Privacy in Public Surveillance," *Computer* (42:9), pp. 22-28.

Morosan, C. 2019. "Disclosing Facial Images to Create a Consumer's Profile," *International Journal of Contemporary Hospitality Management* (31:8), pp. 3149-3172.

Nelson, A. L., Bromley, R. D., and Thomas, C. J. 1996. "The Geography of Shoplifting in a British City: Evidence from Cardiff," *Geoforum* (27:3), pp. 409-423.

Newman, O. 1972. *Defensible Space: People, and Design in the Violent City*. Macmillan New York.

Newman, O. 1973. *Defensible Space: Crime Prevention through Urban Design*. Collier Books New York.

Ng, Y., Li, Z., Chua, Y. X., Chaw, W. L., Zhao, Z., Er, B., Pung, R., Chiew, C. J., Lye, D. C., and Heng, D. 2020. "Evaluation of the Effectiveness of Surveillance and Containment

Measures for the First 100 Patients with COVID-19 in Singapore--January 2–February 29, 2020," *Morbidity and Mortality Weekly Report* (69:11), pp. 307-311.

Norris, C. 2005. "From Personal to Digital: Cctv, the Panopticon, and the Technological Mediation of Suspicion and Social Control," in *Surveillance as Social Sorting*. Routledge, pp. 263-295.

Nöteberg, A., Christiaanse, E., and Wallage, P. 1999. "The Role of Trust and Assurance Services in Electronic Channels: An Exploratory Study," *International Conference on Information Systems, ICIS 1999*, p. 49.

Nowak, G. J., and Phelps, J. 1995. "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When "Privacy" Matters," *Journal of Direct Marketing* (9:3), pp. 46-60.

Nugier, A., Niedenthal, P. M., Brauer, M., and Chekroun, P. 2007. "Moral and Angry Emotions Provoked by Informal Social Control," *Cognition and Emotion* (21:8), pp. 1699-1720.

Oetzel, M. C., and Spiekermann, S. 2014. "A Systematic Methodology for Privacy Impact Assessments: A Design Science Approach," *European Journal of Information Systems* (23:2), pp. 126-150.

Oleshchuk, V. 2009. "Internet of Things and Privacy Preserving Technologies," *2009 International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology*: IEEE, pp. 336-340.

Overstreet, J., and Clodfelter, R. 1995. "Safety and Security Concerns of Shopping Center Customers and the Effect of These Concerns on Shopping Behavior," *Journal of Shopping Center Research* (2:1), pp. 91-109.

Paefgen, J., Staake, T., and Thiesse, F. 2012. "Resolving the Misalignment between Consumer Privacy Concerns and Ubiquitous IS Design: The Case of Usage-Based Insurance," *International Conference on Information Systems, ICIS 2012*.

Pavone, V., and Esposti, S. D. 2012. "Public Assessment of New Surveillance-Oriented Security Technologies: Beyond the Trade-Off between Privacy and Security," *Public Understanding of Science* (21:5), pp. 556-572.

Peer, E., Vosgerau, J., and Acquisti, A. 2014. "Reputation as a Sufficient Condition for Data Quality on Amazon Mechanical Turk," *Behavior Research Methods* (46:4), pp. 1023-1031.

Plangger, K., and Montecchi, M. 2020. "Thinking Beyond Privacy Calculus: Investigating Reactions to Customer Surveillance," *Journal of Interactive Marketing* (50), pp. 32-44.

Pridmore, J., and Zwick, D. 2011. "Marketing and the Rise of Commercial Consumer Surveillance," *Surveillance & Society* (8:3), pp. 269-277.

Rai, A. 2020. "Editor's Comments: The COVID-19 Pandemic: Building Resilience with IS Research," *MIS Quarterly* (44:2), pp. iii-vii.

Ray, S., Ow, T., and Kim, S. S. 2011. "Security Assurance: How Online Service Providers Can Influence Security Control Perceptions and Gain Trust," *Decision Sciences* (42:2), pp. 391-412.

Reddick, C. G., Chatfield, A. T., and Jaramillo, P. A. 2015. "Public Opinion on National Security Agency Surveillance Programs: A Multi-Method Approach," *Government Information Quarterly* (32:2), pp. 129-141.

Redmiles, E. M. 2020. "User Concerns & Tradeoffs in Technology-Facilitated Contact Tracing," in: *arXiv preprint arXiv:2004.13219*.

Reynald, D. M., and Elffers, H. 2009. "The Future of Newman's Defensible Space Theory: Linking Defensible Space and the Routine Activities of Place," *European Journal of Criminology* (6:1), pp. 25-46.

Riemer, K., Ciriello, R., Peter, S., and Schlagwein, D. 2020. "Digital Contact-Tracing Adoption in the COVID-19 Pandemic: It Governance for Collective Action at the Societal Level," *European Journal of Information Systems* (29:6), pp. 731-745.

Schade, M., Piehler, R., Warwitz, C., and Burmann, C. 2018. "Increasing Consumers' Intention to Use Location-Based Advertising," *Journal of Product & Brand Management* (27:6), pp. 661-669.

Schlosser, A. E., White, T. B., and Lloyd, S. M. 2006. "Converting Web Site Visitors into Buyers: How Web Site Investment Increases Consumer Trusting Beliefs and Online Purchase Intentions," *Journal of Marketing* (70:2), pp. 133-148.

Shapiro, S. P. 1987. "The Social Control of Impersonal Trust," *American Journal of Sociology* (93:3), pp. 623-658.

Shapland, J. 1995. "Preventing Retail-Sector Crimes," *Crime and Justice* (19), pp. 263-342.

Shaw, N., and Sergueeva, K. 2019. "The Non-Monetary Benefits of Mobile Commerce: Extending Utaut2 with Perceived Value," *International Journal of Information Management* (45), pp. 44-55.

Short, J., Williams, E., and Christie, B. 1976. *The Social Psychology of Telecommunications*. John Wiley & Sons.

Shukla, M., Lodha, S., Shroff, G., and Raskar, R. 2020. "Privacy Guidelines for Contact Tracing Applications," in: *arXiv preprint arXiv:2004.13328*.

Silberman, M. 1976. "Toward a Theory of Criminal Deterrence," *American Sociological Review* (41:3), pp. 442-461.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1016.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), pp. 167-196.

Soliman, K. S., Affisco, J. F., Belanger, F., and Hiller, J. S. 2006. "A Framework for E-Government: Privacy Implications," *Business Process Management Journal* (12:1), pp. 48-60.

Solove, D. J. 2004. *The Digital Person: Technology and Privacy in the Information Age*. NyU Press.

Spears, J. L., Barki, H., and Barton, R. R. 2013. "Theorizing the Concept and Role of Assurance in Information Systems Security," *Information & Management* (50:7), pp. 598-605.

Strauß, S. 2017. "A Game of Hide-and-Seek?: Unscrambling the Trade-Off between Privacy and Security," in *Surveillance, Privacy and Security*. Routledge, pp. 255-272.

Sutanto, J., Palme, E., Tan, C.-H., and Phang, C. W. 2013. "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users," *MIS Quarterly* (37:4), pp. 1141-1164.

Taylor, N. 2002. "State Surveillance and the Right to Privacy," *Surveillance & Society* (1:1), pp. 66-85.

Teubner, T., and Flath, C. M. 2019. "Privacy in the Sharing Economy," *Journal of the Association for Information Systems* (20:3), p. 2.

Trang, S., Trenz, M., Weiger, W. H., Tarafdar, M., and Cheung, C. M. 2020. "One App to Trace Them All? Examining App Specifications for Mass Acceptance of Contact-Tracing Apps," *European Journal of Information Systems* (29:4), pp. 415-428.

Tsai, J. Y., Kelley, P. G., Cranor, L. F., and Sadeh, N. 2010. "Location-Sharing Technologies: Privacy Risks and Controls," *I/S: A Journal of Law and Policy for the Information Society* (6:2), pp. 119-151.

Tsakanikas, V., and Dagiuklas, T. 2018. "Video Surveillance Systems-Current Status and Future Trends," *Computers & Electrical Engineering* (70), pp. 736-753.

Van Slyke, C., Shim, J., Johnson, R., and Jiang, J. J. 2006. "Concern for Information Privacy and Online Consumer Purchasing," *Journal of the Association for Information Systems* (7:6), pp. 415-444.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425-478.

Von der Puetten, A. M., Krämer, N. C., Gratch, J., and Kang, S.-H. 2010. "“It Doesn’t Matter What You Are!” Explaining Social Effects of Agents and Avatars," *Computers in Human Behavior* (26:6), pp. 1641-1650.

Walsh, A. 2020. "Coronavirus: Contact Tracing 'Still Key' to Controlling Pandemic," in: *DW News*.

Wang, L., Yan, J., Lin, J., and Cui, W. 2017. "Let the Users Tell the Truth: Self-Disclosure Intention and Self-Disclosure Honesty in Mobile Social Networking," *International Journal of Information Management* (37:1), pp. 1428-1440.

Wang, T., Duong, T. D., and Chen, C. C. 2016. "Intention to Disclose Personal Information Via Mobile Applications: A Privacy Calculus Perspective," *International Journal of Information Management* (36:4), pp. 531-542.

Watkins Allen, M., Coopman, S. J., Hart, J. L., and Walker, K. L. 2007. "Workplace Surveillance and Managing Privacy Boundaries," *Management Communication Quarterly* (21:2), pp. 172-200.

Welsh, B. C., and Farrington, D. P. 2004. "Evidence-Based Crime Prevention: The Effectiveness of Cctv," *Crime Prevention and Community Safety* (6:2), pp. 21-33.

WHO, W. H. O. 2020. "Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing: Interim Guidance, 28 May 2020," World Health Organization.

Wood, D. M., Ball, K., Lyon, D., Norris, C., and Raab, C. 2006. "A Report on the Surveillance Society."

Xu, H., Luo, X. R., Carroll, J. M., and Rosson, M. B. 2011. "The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing," *Decision Support Systems* (51:1), pp. 42-52.

Xu, H., Teo, H.-H., Tan, B. C., and Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135-174.

Xu, H., Teo, H.-H., Tan, B. C., and Agarwal, R. 2012. "Research Note—Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services," *Information Systems Research* (23:4), pp. 1342-1363.

Yaniv, G. 2009. "Shoplifting, Monitoring and Price Determination," *The Journal of Socio-Economics* (38:4), pp. 608-610.

Zhang, X., Hao, X., Liu, S., Wang, J., Xu, J., and Hu, J. 2019. "Multi-Target Tracking of Surveillance Video with Differential Yolo and Deepsort," *Eleventh International Conference on Digital Image Processing (ICDIP 2019)*: International Society for Optics and Photonics, p. 111792L.

Zhao, L., Lu, Y., and Gupta, S. 2012. "Disclosure Intention of Location-Related Information in Location-Based Social Network Services," *International Journal of Electronic Commerce* (16:4), pp. 53-90.

Zhu, L., Benbasat, I., and Jiang, Z. 2010. "Let's Shop Online Together: An Empirical Investigation of Collaborative Online Shopping Support," *Information Systems Research* (21:4), pp. 872-891.

Zlatolas, L. N., Welzer, T., Heričko, M., and Hölbl, M. 2015. "Privacy Antecedents for Sns Self-Disclosure: The Case of Facebook," *Computers in Human Behavior* (45), pp. 158-167.

Zuboff, S. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.

Zucker, L. G. 1986. "Production of Trust: Institutional Sources of Economic Structure, 1840-1920," *Research in Organizational Behavior* (8), pp. 53-111.

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346 USA