THE EFFECT OF PRIVACY RISK AND HEALTH BENEFIT ON INFORMATION DISCLOSURE IN A POSSIBLE OUTBREAK SITUATION

By

Yumi Jung

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

Information and Media—Doctor of Philosophy

2018

ABSTRACT

THE EFFECT OF PRIVACY RISK AND HEALTH BENEFIT ON INFORMATION DISCLOSURE IN A POSSIBLE OUTBREAK SITUATION

By

Yumi Jung

An individual's privacy is not a static state; rather it is a decision process encompassing both privacy risks and benefits that the individual encounters in situations requiring information disclosures. Also, privacy is multi-level, including both individual as well as group concerns. The purpose of this dissertation was to understand how much individuals disclose personal information when different dimensions of privacy risks and benefits were present, and to what extent information disclosure affected privacy concerns. This dissertation manipulated the situation where an individual met privacy risk and health security benefits, a situation of gaining security but losing privacy, or vice versa. The two proposed studies in this dissertation performed to better understand this tension. Each study manipulated different situations of benefits and risks, and encouraged participants to make a decision regarding their privacy in a health security context. Study 1 manipulated dimensions of privacy risks (i.e. access by others and control over information distribution) and benefits of information disclosures on either an individual or public level across risk conditions. To tackle the issue of privacy as a socially negotiated condition, study 2 manipulated recipient levels of risks and benefits (i.e. individual vs. community vs. public). Both studies also investigated the relationship between information disclosure and privacy concern. The results showed that there was a negative relationship between information disclosure and privacy concern. Also, trust was a meaningful factor to decrease privacy concern. There was an interaction effect of privacy risk and benefit. Risk and benefit worked differently in different conditions. Especially, high control over personal information decreased the amount of

information disclosure. Also, participants were willing to disclose more information when they had community level benefit compared to individual level benefit, but they were less willing to disclose personal information with individual level privacy risk compared to community or public level privacy risk. This research contributes to discussions of privacy and information disclosure by examining the relationships between privacy tension, information disclosure, and privacy concern using an experimental design. As such, this research has implications for policy, as well as the design of interfaces for obtaining private information, which in turn has applications in venues of government, as well as industry.

To my father

ACKNOWLEDGEMENTS

I would never have been able to finish my doctoral studies without the guidance of my committee members, help from friends, and support from family. I am most grateful to my advisor, Dr. Emilee Rader, for her emotional and financial support. Especially I appreciate her patience throughout all the way to graduation. I also would like to thank, one of my committee member, Dr. Rick Wash for his continuous support and inspiration. Hours of conversation with him were both helpful and memorable. Without his support, this dissertation would have been literally impossible. I also would like to express my special thanks to Dr. Rabindra Ratan and Dr. Nora Rifon for all the detailed and helpful comments in the completion of this dissertation. I also want to express my special thanks to the BIT Lab. It was lucky to have the opportunity to work at BIT Lab. The BIT Lab family encouraged and inspired me through discussions. I could not have reached this point without the generous financial support of the Department of Media and Information and dissertation fellowship from the Graduate School. Thanks also go out to my mentors and colleagues, Dr. Jinsuk Kim, Dr. Hyun Jung Oh, Janine Slaker, CK Park, Jina Yu and many others for their supports. Last but not least, I owe my deepest gratitude to my family and friend. I thank my parents and my dear friend, Hong for supporting me all the time. I would like to thank my husband, Dr. Yeonjei Jung, and my son, Sean, for their love and support. I cannot imagine my life without you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

In our global world, we are faced with situations that demand us to sacrifice privacy for the sake of public security. After the September 11th attacks in 2001, many U.S. airports sought to improve security by using full-body scanners. These scanners create an image of a passenger's naked body. While this is argued as a necessity of public security it is not a pleasant experience for individual passengers when strangers see private parts of their bodies. Acts such as 9/11 are extreme. However, it lends insight into why full-body scanners are contentions because its benefits and risks cannot be compatible.

We can also see the argument of societal vs. individual privacy in debates of the FBI requests to Apple, insisting the company make their encryption technology available when investigating crime suspects. In 2016, the FBI captured an iPhone from a suspected criminal but could not open the phone because this version of iPhone would clear their data after ten attempts with wrong passcodes. A federal magistrate judge in California ordered Apple to help the FBI by creating software to foil the encryption. However, Apple refused the demand because they thought it would be the start of threatening customers' privacy (Lichtblau & Wingfield, 2016; Nakashima, 2016).

Additionally, we see situations where disclosing personal information concerns public health, such as during the spread of Ebola to the U.S. and the MERS virus to South Korea. The Ebola virus arrived to the U.S. in 2014 and the U.S. government was able to limit the contagion by tracking the travel history of professionals' who traveled to areas known to have an Ebola outbreak, and publicly releasing patients' and hospitals' information about the virus to the public. Overall, this level of information control contributed to limiting the contagion where the

violation of a few was taken as a needed risk for public health security but at the cost of challenging the right of patients (Florance, Carafano, & Kaniewski, 2015; Ornstein, 2015).

In contrast, when addressing the spread of the MERS virus in South Korea in 2015, which resulted in 186 infections and 36 deaths, the Korean government struggled with containing the outbreak in part due to their refusal to reveal information about infected patients and hospitals where the patients visited at the onset. Specifically, information concerning individuals diagnosed with MERS and the hospitals that treated them was withheld. The government claimed that releasing too much information about these individuals would cause panic. As a result, the government failed to contain the outbreak in its early stages (Choe, 2015).

These examples highlight a tension between security and privacy that burgeons when a security system collects personal information and creates a situation of increasing public safety but at the cost of decreasing individual privacy, or vice versa. One aspect of this tension is derived from individuals not having full opportunities to control the information collected, or how information collected about them is used. For example, individuals who opt-out of full-body scans at the airport are faced with longer waiting periods in security lines. Further, opting out may signify suspicion, which can require them to provide lengthy explanations as to why they do not want to be scanned.

The tension between security and privacy is not only linked to individual benefits and risks, but also public benefits and risks. While Apple's decision is good for protecting individual privacy, their decision can be harmful for public safety. Individuals who were at risk for the viruses knew the importance of doing self-reports in order to receive treatment and prevent further contagion, but were reluctant to do so because they were concerned about public backlash (McGrath, 2015; Lee, 2015). When the U.S. and Korean governments decided to release patient

records to control the outbreaks (this included personally-identifiable information and pre- and post-infection travel history), the patients became vulnerable not just to the effects of the virus, but to social blame and recrimination. As a result, they and their families were ostracized. Therefore, privacy is not individual, but situational, and encompasses an individual's right to privacy and the individual's responsibility to their society. What remains consistent is the difficulty of balancing risk of privacy violation to the benefits of information transparency.

This tension is truly not a matter of choosing privacy over security or vice versa, but rather a complex relationship between the two in which the weight of both are constantly in fluctuation. On one hand, if governments are transparent (i.e. sharing patient information with the public) then there is a high possibility of quickly controlling an emergency. On the other hand, patients whose information is shared suffer individual violations of privacy. Further, information disclosed can increase the risk of social panic, and individuals who may cause health concerns may not report themselves due to fear of being ostracized.

If suspected patients do not report themselves, there is no issue of privacy violation, but the risk to public is increased. This presents a social dilemma in which healthy individuals who wish to avoid risking exposure may ask a government to share all possible information even if it means violating the privacy of individuals. However, it is suspected that if those same individuals were to be at risk themselves, their willingness to have personal information disclosed would be radically altered. In sum, privacy is a matter of self-interest, but this becomes more complex as it involves others—not only at the level of other individuals, but others within a community—as well as national security.

Although privacy has been defined as the ability to control personal information (Westin, 1970), it becomes clear that privacy is no longer fully controllable. We are required to disclose

personal information in many cases, and our digitized personal details have been used and transferred by countless government agencies and corporations. Not surprisingly, 91% of participants in a 2015 Pew survey agreed that consumers have lost control over their personal information, such as contact information and credit card numbers (Madden, 2015). Specifically, individuals are concerned about the possibility of privacy risks, such as who can access our information or how well their information is protected.

From an individual's standpoint, privacy is more than the ability to control personal information as it is about the process in which an individual considers the benefits and risks of disclosing information. Benefits and risks vary depending on the situation and how these features may affect individuals' decisions of information disclosure and their privacy concerns. For example, if an individual understands only limited authorized organizations can access a person's identifiable information and she can get a clear benefit of provided services, then the individual is likely to disclose personal information and will not have much concern about privacy violations. In other words, if an individual thinks public safety is more important than individual liberty, she is may disagree with Apple's decision of not cooperating with the FBI. However, the individual's privacy preference is situational and changes depending on information of risks and benefits. For example, this same person can worry about the possibility of phone surveillance in a different context (i.e. hacking from anonymous others or workplace surveillance). In other words, for individuals, privacy includes considerations of benefits and risks by information disclosures and concerns about the consequences from this decision.

Although individuals may agree with personal information being collected for the sake of public safety, this does not mean that they are free from individual privacy concerns. Previous privacy studies have focused on whether or not individuals disclose their information and how

decisions of information disclosure are made (Christofides, Muise, & Desmarais, 2009; Special & Li-Barber, 2012). Information disclosure is the key question for online service providers and is considered as a variable negatively correlated to privacy concern. For example, Andrade, Kaltcheva, and Weitz (2002) explain that individuals are willing to provide personal information for the benefits of self-disclosure in online commercial contexts, but privacy concern is a factor to impede the disclosure behavior. However, there is not enough discussion on specific kinds of risks/benefits as it affects privacy concern for people, and what privacy concerns are after individuals disclose information.

Therefore, the purpose of this dissertation was to address how different dimensions of privacy risks and benefits affected individuals' information disclosure decisions and the level of privacy concerns afterwards within a health security context. If information disclosure is unavoidable, there should be consideration of how to deal with people's privacy concerns. By knowing the effects from consideration of risks and benefits on information disclosure and privacy concerns, we can develop better policies and design better systems to assist in the management of large-scale health-security risks. The following overall research questions were constructed to address such as an issue (the full research questions are listed in the conclusion of the lit review, p. 26):

- *What is the relationship between the amount of information disclosure and the level of privacy concerns?*
- *What are individuals' privacy concerns and information disclosures when the individuals encounter different information of privacy risks and health benefits?*

Figure 1 Conceptual map of the study

Note. Study 1 and Study 2 had the same conceptual design. The difference was the experimental manipulation for health benefit and privacy risk.

I designed two experimental studies to answer these questions. The two studies investigated individuals' willingness to disclose personal information when they anticipated health benefits but privacy risk in the context of a possible public health outbreak. Figure 1 shows the conceptual map of the studies. Study 1 focused on individuals' information disclosures and privacy concerns when the individuals encountered individual or public health benefits from their information disclosure, and their privacy risks under differing conditions of access and control. Access was the boundary of information release when the outbreak occurs. Large or small access condition referred that the system released participants' information to public or only governmental agencies respectively in emergency. Control was the right of permission on information distribution. High or low control condition referred that participants had or did not have permission on their information distribution before the government's action. Study 2 focused on individuals' information disclosures and privacy concerns when they expected public, community, or individual level health benefits and privacy risks. Overall, Study 1 and Study 2 had the same conceptual design but used different information of privacy risks and benefits.

Throughout the studies, I intended to look at the relationship between the amount of disclosed information and the degree of privacy concern within a health security system. By

controlling other factors such as previous experience in the health system, this study investigated more direct effect of information disclosure on privacy concern. This study adopted a possible outbreak situation because health security is one of the most significant issues in daily life. In health emergency, it is very important for government agency to collect individuals' information with less concern of privacy violation. For individuals, it is important to let the government know what kind of risks or benefits they are concerned with. This study tried to find how different risks and benefits influenced individuals' endorsement or reluctant to provide their information such as contact information and health status. This information will be helpful to design a health security system which reduces individuals' privacy risk but increases their willingness to disclose information. Results from the experiments can help system providers and governments alike figure how to construct systems that have the flexibility to shift what information is being asked of people that still provides a mean to mitigate public-health outbreaks. These studies also contribute to broader literature on the topic of privacy decisions by showing how the effects of risks and benefits shift on information disclosure.

2 LITERATURE REVIEW

2.1 Information Disclosure and Privacy Concern

2.1.1 Information disclosure

Information disclosure is defined as both the breadth and depth of personal information that an individual provides to another (Jourard, 1971). Information disclosure has been discussed in social media studies because users are not only consumers who visit an online platform to read others' posts, but are also content creators as well in social media (Berthon, Pitt, Plangger, & Shapiro, 2012). It is critical for social media to encourage users to disclose personal information to their online databases. Many social media and online marketing studies have investigated effective ways to increase the amount of information disclosures from users.

Information disclosure is also helpful to understand users' decisions regarding privacy. It is one of the most commonly studied variables as an outcome of privacy decision in privacy related studies (see Smith, Dinev, & Xu, 2011). When an individual decides to disclose a certain amount of information to an online service, the decision is based on the consideration of possible risks and benefits from the information disclosure (Xu et al., 2009). The actual amount of disclosed information shows how the individual takes seriously provided information about risks and benefits (Brandimarte, Acquisti, & Loewenstein, 2013).

Early privacy studies measured 'intention' to disclose personal information as a proxy of actual disclosure behavior, with a belief that intention is a reliable antecedent variable of actual behavior, or because of methodological limitations (Norberg, Horne, & Horne, 2007). Norberg et al. (2007) looked at the relationship between intention to disclose and actual disclosure behavior, and found there was a significant difference between the two measures. In their study, the level of actual disclosure was much higher than the level of intention to disclose.

Individuals may report cautious attitudes regarding their decisions of privacy when it comes to intent, but other cues such as habits formed from previous experience or different information about risk might actively affect their actual behaviors (Acquisti & Loewenstein, 2011). Although intention is an important variable in understanding individuals' perceptions of privacy, John, et al. (2011) found that measuring actual behavior is more relevant to understanding individuals' privacy decisions. As a result of work like this, an increasing number of studies try to measure actual information disclosure behavior in a given context (e.g. Brandimarte, Acquisti, & Loewenstein, 2013; John, Acquisti, & Loewenstein, 2011). Following the advice of previous researchers, this study measured actual disclosure behavior in a health security context controlled with privacy risks and health benefits.

2.1.2 Privacy concerns

Privacy concern has mostly been used to evaluate one's psychological perception of privacy (Malhotra, Kim, & Agarwal, 2004; Smith et al., 2011). Privacy concern refers to an individual's worries about possible privacy violations, such as unauthorized collection of personal information and secondary usage (Malhotra et al., 2004; Smith, Milberg, & Burke, 1996; Wang, Lee, & Wang, 1998). Privacy violations can occur in any process of information collection, processing, and dissemination (Solove, 2006). Therefore, privacy concerns imply an individual's worries about possible privacy violations during any stage of the information disclosure process. Previous studies have tried to capture the different dimensions of privacy concerns affected from different privacy violations.

For example, Smith et al. (1996) hypothesized four dimensions of privacy concern that are related to the information process: 1) collection; 2) errors; 3) secondary use; and 4) improper access. Collection refers to an individual's concern about the amount of data collected (Miller,

1982). Errors is defined as the degree to which accidental errors happen while processing data (Smith et al., 1996). Secondary usage refers to the degree to which a person is concerned that personal information is used for purposes other than the original reason for collecting information (Hong & Thong, 2013; Malhotra et al., 2004; Smith et al., 1996). Improper access implies a person is concerned that his or her personal information is available to other parties who are not authorized to view or work with the data (Hong & Thong, 2013; Malhotra et al., 2004; Smith et al., 1996).

People who use digital technology, especially when connected to the Internet, cannot fully control their information once they share it with online service companies. Thus, users worry about the usage of their information when online companies are involved. The lack of control increases individual privacy concerns especially in an online context (Phelps, Nowak, & Ferrell, 2000). Additionally, online users have consistently expressed that they want more control over personal information shared with online companies (Nowak & Phelps, 1995). This has brought some attention to the concepts of control and awareness with some researchers arguing that each should be considered in the contexts involving the investigation of privacy concern (Malhotra et al., 2004). Control is the degree to which a person is concerned that she does not have adequate control over her personal information held by websites. Awareness refers to how well informed the person is about the use of personal information by online companies (Malhotra et al., 2004).

Therefore, it would be reasonable to use multi-dimensional privacy concern measures because information privacy includes different dimensions of its meaning and each dimension may have different effects (Hong & Thong, 2013; Malhotra et al., 2004). To understanding

various aspects of privacy concerns, this study adopted four dimensions of privacy concern: collection, secondary use, improper access, and control.

2.1.3 Privacy paradox

Privacy concern and information disclosure are indicators of how individuals understand their privacy status. Scholars have examined the relationship between the two concepts. Privacy concern was frequently used to estimate the amount of information disclosure but the effect of privacy concern on information disclosure has not been consistent. While privacy concern has been considered as a major factor in anticipating users' information disclosures, studies have shown inconsistent influence of privacy concern on users' information disclosure.

For example, Liu, Ang, and Lwin (2013) surveyed 780 adolescents who were Facebook users and showed that adolescents with high privacy concern decreases his or her willingness to disclose information. Another Facebook study showed that college students those who had a high level of privacy concern were less willing to disclose personal information on Facebook (Young & Quan-Haase, 2009). The negative relationship between privacy concern and information disclosure has been also found in consumer research. Schoenbachler and Gordon (2002) found that consumers who were less concerned about their privacy were willing to provide their personal information and, in this case, trust played an important role in decreasing consumers' privacy concern. However, other researchers have demonstrated that there was no statistically negative relationship between the two (Mothersbaugh, Foxx, Beatty, & Wang, 2011). More so, privacy paradox studies argue that people disclose lots of personal information even when they have high privacy concerns (Awad & Krishnan, 2006; Wilson & Valacich, 2012).

The privacy paradox that individuals who have high privacy concern are not reluctant to disclose personal information is interesting because it is not a rational behavior. Two estimations

have sought to explain why the privacy paradox happens. Acquisti et al. (2015) pointed out that the uncertainty of information individuals yields irrational privacy decisions. When individuals need a certain benefit, and the benefit is relatively clear, they decide to disclose information without enough information of privacy risk. For example, an individual gets an email that promotes to use a new car insurance website. It says when the individual gets a quote from the website, s/he will get a $50 discount coupon for a car insurance. In this case, the benefit is obvious but it is not clear how the website uses his or her information used for the quote. When individuals provide their personal information for momentary rewards or a specific service, the benefit is clear and the return is relatively quick, but the risk from information disclosure is not specific and may happen in the distant future (Acquisti, 2004).

However, people do not always have complete information of the benefit and may have incomplete information regarding the privacy risk. For example, full-body scanners in airports are installed for public security, but to someone, the privacy risk more apparent than the benefit of having more security (Mironenko, 2011; Accardo, & Chaudhry, 2014). As such, various contexts can influence whether the privacy risk is more tangible than the benefit from disclosing information.

Many privacy concern studies surveyed social media users or online consumers from existing websites. This was problematic because existing participants who already disclosed their information to websites generated a base that was arguably biased. Studies based on a sample of individuals who were familiar with online interactions with the targeted platform could significantly alter results (Bansal, Zahedi, & Gefen, 2010), because the experience effect for the participants would be positive.

Also, there was a discrepancy between the boundary of information disclosure and the boundary of privacy concern. Many social media studies measured information disclosure by only counting the number of items disclosed on users' profiles but measured privacy concern as related to overall usage on the targeted platform. In turn, users could show various levels of privacy concern and information disclosure within one social media platform. For example, it is possible that individuals have concern for the possibility of unknown others viewing their Facebook profiles, but less concern for sharing information with anticipated audiences via their posts. Thus, if we were to measure a set of information disclosure and privacy concern on the specific information disclosure, the relationship between information disclosure and privacy concern would be clearer.

Rather than concluding individuals perform paradoxical behaviors: high concern and high information disclosure, I argue that individuals disclose more information when they have less privacy concern for the information disclosure. In other words, there would be a negative relationship between information disclosure and privacy concern. It is more reasonable to ask users about their privacy concerns regarding their actual disclosures in a specific situation. I investigated the following research question and hypothesis.

RQ1: What is the relationship between the amount of information disclosure and the level of privacy concern?

H1: Individuals those who disclose more information has lower privacy concern.

2.2 Trust Effect

Trust has been frequently mentioned in privacy related research as an antecedent variable of privacy concerns or information disclosures (Smith et al., 2011). Most studies have demonstrated that individuals perceived trust of service providers has a statistically negative relationship with privacy concerns about the targeted sites (Eastlick, Lotz, & Warrington, 2006; Taddei & Contena, 2013). Studies have also shown that individuals perceived trust of online service have a statistically positive relationship with their information disclosures on the sites of service adoptions (Metzger, 2004; Krasnova & Spiekermann et al., 2010). For example, Krasnova et al. (2010) selected two popular social networking sites and asked its users about their trust in service providers and other members, perceived privacy risk, and the degree of self-disclosure using an online survey. They found that users' trust in service providers negatively affected their perceived privacy risks, but trust in other users did not affect their perceived privacy risks. Also, users who had lower perceived privacy risk were willing to disclose more information in the social networking sites.

When studies use existing online platforms as a study context, users' trust in the websites had been built before their involvement in the studies. Thus, the study participants' trust might be mixed of trust to the platform, trust to the people they are interact with in the platform, or trust built from general social networking sites usages including other sites which the study did not ask about. In the Krasnova et al. (2010)'s study, only trust in service provider mattered on perceived privacy risk and information disclosure while trust in other users had no effect on it. For this reason, different types of trust should have different effects on information disclosure and privacy concerns. To test this claim, this study created a new online system designed to manage the outbreak of disease in which participants reliant on information provided during the

studies. In this case, trust to the website could not fully developed during the experiment, but trust to a general health information website would matter. For this reason, different types of trust would have different effects on information disclosure and privacy concern.

This dissertation included two types of trust in the privacy decision model to look at its effect on privacy concern.

RQ2: What is the effect of trust on information disclosure and privacy concerns?

H2_1: Individuals who have higher trust to the government agencies lower privacy concern when they disclose the same amount of information.

H2_2: Individuals who have higher trust to the Outbreak Alert System report lower privacy concern when they disclose the same amount of information.

2.3 Privacy Decision Model

Empirical studies have explained information disclosure as a decision process where an individual estimates the weight of risks and benefits to make a decision of information disclosure (Hann, Hui, Lee, & Png, 2002; H. Xu, Teo, Tan, & Agarwal, 2009). The decision process is influenced by various factors. This section of the literature review includes concepts in the privacy decision process and the influence of various factors on information disclosure.

2.3.1 Perceived privacy risk

Individuals perceived privacy risk is their subjective evaluative potential of negative outcomes from information disclosure (Featherman et al., 2010; Dai, Forsythe, & Kwon, 2014; Rindfleisch, 1997). Individuals perceived privacy risk is one of the most important factors for understanding decision making processes of information disclosure as it relates to privacy concern (Featherman & Pavlou, 2003). Previous research on the relationship between the perceived privacy risk and information disclosure shows positive correlations between the two

(Dinev et al., 2006; Xu, Michael, & Chen, 2013). For example, in an experimental study, Tsai et al. (2011) found that participants were more likely to pay for products from buyers who had better privacy protection that implied lower privacy risk.

Previous privacy studies measured general privacy risk by asking individuals perception on the degree of uncertainty on provided information. For instances, Kim and Lennon (2013) measured consumers' perceived risk in online website with survey items regarding uncertainty such as "I do not trust that my credit card number will be secure at this web site", "It is difficult to judge quality of a product/service on this web site", "I do not trust that my personal information will be kept private." The limitation of the measure of general privacy risk is that it is hard to figure out the effects of sub-dimensions of privacy risks such as control over risk and severity of consequences (e.g., Fischhoff, Slovic, Lichtenstein, Read, & Combs, 1978).

Im, Kim, and Han (2008) measured perceived risk on communication technology such as Webboard, MSN Messenger and wireless PDA. They used survey items which measured five risk factors: financial (worth the cost), performance (effectiveness), social (changes in work), psychological (frustration), and physical (comparison to other products). For example, "It is probable that MSN Messenger would not be worth its cost", "it is probable that MSN Messenger would frustrate me because of its poor performance", and "it is uncertain whether MSN Messenger would be as effective as I think." Other studies focused more on sub-dimensions of perceived privacy risk, such as how much users think they can control their information (e.g., Klein & Kunda, 1994; Xu, 2007) and how large users imagine the boundary of information access by others (e.g., Brandimarte, Acquisti, & Loewenstein, 2013).

Control means how much individuals change the probability distribution of unwanted outcomes (R. Miller & Lessard, 2001). This factor is used to define the nature of a risky

situation. A low level of control is associated with privacy risk where little can be done to change the probability of occurrence, and a high level of control is associated with the occurrence that can be changed by a subject's efforts (Fan, Lin, & Sheu, 2008).

Cho, Lee, & Chung (2010) pointed out the importance of control on judgments of privacy risks. They showed that individuals judged themselves less vulnerable to privacy risks than others when they had more control over their personal information. Brandimarte, Acquisti, & Loewenstein (2013) conducted a series of experiments to look at individuals' willingness to disclose personal information for an online community profile when they have low or high perceived control over how information is released. They designed their experiments based on the argument that people are less willing to disclose their personal information when they feel they have lower control over information management. However, their manipulation of control is not based on an accurate estimation of information release. In their experiments, participants encountered a condition which gave less control over information released but less uncertainty or a condition which gave more control but more uncertainty. Participants in the high control condition were told that all information they entered would be published to their profiles while participants in the low control condition were told that only a half of information they entered would be published to their profiles. Although the absolute amount of disclosed information for the low control condition is less than the other condition, the uncertainty factor would affect participants' decisions.

Social media has adopted the control factor to increase users' psychological privacy. In 2006, Facebook changed their News Feed features. The News Feed started to include users' recent posts and personal profile information. Most of this information was previously placed under sub-menus. This meant that the first page of a user's Facebook contained more personal

information than before. It yielded Facebook users to make an outcry about violations of privacy, although Facebook excused such concerns by arguing the amount of information the system delivered was the same (Hoadley, Xu, Lee, & Rosson, 2010). Hoadley et al. (2010) examined why the change made users upset by asking survey questions to 172 Facebook users. Most of the participants expressed an uncomfortable feeling with the change of News Feed even though they knew that the amount of information disclosed was the same. They were uncomfortable that others could more easily access their information whether or not the users desired to see it. The participants surveyed felt they were losing control over their information. This example shows that control is an important factor for users to understand their privacy.

Access refers to the people and stakeholders who have access personal information (Bellotti & Sellen, 1993). When individuals decide the amount of information disclosure, the individuals expect who may see their information (Palen & Dourish, 2003). Once the individuals provide his or her personal information to companies or governmental agencies, however, they lose control over who can access it. It is difficult to estimate whether the information is available to particular groups, certain persons only, or just to oneself in technology mediated interactions (Bellotti & Sellen, 1993).

Logically, privacy risk increases when the boundary of information access expands. For example, Brandimarte, Acquisti, & Loewenstein (2013) looked at how individuals' behavior of information disclosure changes when faced with low (vs. high) information access by others. When the individual had increased access by others, they were less willing to disclose personal information. Additionally, studies investigating online consumer behavior showed that consumers' privacy concern increased when the consumers expected that their information would be shared with third parties in addition to the original websites to where they provided

their information (Miyazaki & Fernandez, 2001; Olivero & Lunt, 2004).

RQ3_1: What are the effects of risks (control and access) on information disclosure?

H3_1a. Effect of control: Individuals who have high control will disclose more information than individuals who have low control.

H3_1b. Effect of access: Individuals who are in the small access condition will disclose more personal information than individuals who are in large access condition.

2.3.2 Benefits of information disclosures

Research findings suggest that in order for users to disclose personal information they have to think that information disclosed is worth the benefits provided by the services (Hann et al., 2002). Benefits refer to rewards that an individual receives as an outcome of social exchange whereas cost refers something that the individual yields for the benefits (Kankanhalli, Tan, & Wei, 2005). Benefits have been operationalized as time saving (Hann et al., 2002), a personalized service (Milne, Rohm, & Bahl, 2004), a money reward for disclosing the information, and a benefit to social relationships (Special & Li-Barber, 2012). In other words, when users disclose personal information it is done so through a process of exchange in which disclosure yields benefits to the user, such as monetary compensation, convenience (Hann et al., 2002; Knijnenburg & Kobsa, 2013; Xu et al., 2009) and social capital (Christofides et al., 2009; Special & Li-Barber, 2012).

Acquisti & Grossklags (2005) have referred to this process of exchange as 'privacy trade-offs' and have pointed out that users tend to have insufficient information when they are in these situations. It is true that when users sign up for a website or hand over their information to a website, the users have limited information which is provided by the websites. It is hard for them to visualize how their information would be used by the website and what kind of risk they

would have. In most cases, however, the users are clearly informed about benefits because they visit the website with a need for its service, though they have unclear information about risk.

There are different types of benefits which encourage individuals to disclose personal information. Privacy benefit has been discussed as a benefit for an individual, such as momentary value or specific service (Hann et al., 2001; Xu et al., 2005). However, in current social issues, like virus outbreaks and terrorist attacks, gathering personal information by government agencies is not only an individual matter but also a public matter because the benefit or risk from information disclosure is not limited to an individual. For this reason, this study manipulated the types of benefits with a social boundary, such as individual, community and public. The next section discusses more about privacy argument between public and individual.

RQ3_2: What are the effects of individual or public benefit on information disclosure?

H3_2: Individuals who are informed of an individual benefit will disclose more information than individuals who are informed of a public benefit.

Based on the privacy decision model, this study looked at an individual's privacy decisions regarding information disclosure with different information of privacy risks and individual benefits and its interaction effects.

RQ3_3: What are the interaction effects of risks and benefits on information disclosure?

H3_3: Interaction of control and access will be different for the public and individual benefits conditions.

2.4 Public vs. Individual Frame

Most studies of privacy decision have focused on the individual level of benefits and risks because privacy is an individual right, which relates to personal dignity (Solove, 2007; Bélanger & Crossler, 2011). However, privacy is also social because the appropriate boundary of

privacy is socially constructed (Patil & Kobsa, 2009). Additionally, when people think about privacy, there is a negotiation between individual interests and public interests (Ursin, 2010). The examples of outbreaks, full-body scanners, and Apple's response to the FBI show individual privacy decision is not only related to individual's interests but also related to public interests. This study focuses on individuals' privacy decision with conflict interests of individual and public in a health security context.

Public security includes economic, food, health, environmental, personal, community, and political security (Kusar, 2015), and these are related to human rights and welfare. One means of ensuring public security is in ensuring information security, which can be thought of as a tool to protect important information against unauthorized disclosure, transfer, modification, or destruction (Bozsak et al., 2002). The key role of information security is gathering and maintaining information, and providing access to the information when the information is desired (Khalfan, 2004). It is necessary to collect individual information to increase security, and the collected individual information is secured by information security systems.

Thus, information security systems are always related to privacy issues. The fact that security systems can operate based on individuals' information is the basis of the tension between privacy and security. Although studies have discussed how individuals deal with their benefits and risks on privacy decisions, it would be possible that the individuals decide information disclosure for public benefits, taking individual risk, or for public risks, scarifying individual benefit. This section discusses different situations of public or individual privacy risks and benefits.

2.4.1 Public Security and Individual Privacy

There are on-going debates concerning the priority of security or privacy (Pavone & Esposti, 2010). As many as 52% of Americans are concerned about government surveillance with 65% of Americans believing inadequate limits on surveillance are in place (Calo, 2015; Rainie & Madden, 2015). In the same survey, 54% of respondents believed it is acceptable to monitor communications from foreign citizens, with 57% believing it is not acceptable to monitor communications from U.S citizens.

While a security system is an important part of securing safety for society, the problem concerning potential risks of such systems is underestimated. Surveillance studies have been a thorough outlet of research regarding this problem. With the rapid growth of face recognition technology, high-tech video surveillance has been a concern (Bowyer, 2004). Surveillance cameras blur the boundary of private and public spaces with great danger of misuse (Norris, McCahill, & Wood, 2002; Wagner, 2010). This might be a new version of the Panopticon (Kandias, Mitrou, Stavrou, & Gritzalis, 2013).

This increasing mobility of surveillance (Adey, 2002) is further related to the tradeoff between public security and individual privacy. In a situation of global terrorism, a society needs to prepare for almost unpredictable crimes. Thus, society heavily relies on surveillance-oriented security technologies (Pavone & Esposti, 2010). Also, different monitoring systems share collected surveillance data to predict risks (Zureik & Salter, 2013).

2.4.2 Selfish Individual and Public Risks

Sometimes, individuals' behaviors can hurt public safety. For example, a common social dilemma is one referred to as the 'free-ride problem' which is described when a public benefit is available to all citizens whether the citizen contributes to the public good or not (Thorn &

Connolly, 1987). When we have a critical number of individuals who choose individual benefits rather than public benefits, we cannot reach public safety. For example, governments encourage people to receive vaccinations to improve public health, but individuals may make different decisions. They may think that it costs too much money or they are safe because everyone else is vaccinated (Fine & Clarkson, 1986), or distrust the effectiveness of vaccines (D. L. Miller, Alderslade, & Ross, 1982). Realistically, the acceptance rate of whooping cough vaccines declined dramatically in the 1970s in Britain, for example, and it caused increased death rates by cough (Miller et al., 1982). In this situation, the individuals' decisions threaten overall public health.

2.4.3 Individual Benefits and Privacy Risks

There is always a tradeoff between individual benefits and individual privacy. Individuals use technology for conveniences, but the technology can be used for surveillance. Kang, Shilton, Estrin, Burke, and Hansen (2011) explain this concept as "self-surveillance," which is when privacy threats can arise from the technologies in our pockets. For example, we may carry a smartphone at anytime and anywhere to be online for interpersonal communication and information searches. Meanwhile, our smartphone can be used as a tool to track and monitor our movements for any purposes.

Viscusi and Zeckhauser (2003) examined individuals' preferences regarding civil liberties and terrorism risks in an airport targeted screening context. After the 9/11 terrorist attack, it was common to do screenings of targeted groups of passengers who are considered a high risk, usually targeting based on race or ethnicity, and there was an issue of whether it was appropriate to define a passenger in a high-risk group. The researchers defined the situation as a tradeoff of civil liberties for terrorism risk reduction. They conducted a simple survey to ask

whether or not participants are willing to trade off their liberties by taking targeted screenings. Overall, participants were more likely to agree with the screening when they had enough time. Among the participants, non-whites, who may have had past experiences with such targeting, are less willing to get the screenings. For them, individual privacy was more important than terrorism risk. However, whites were more willing to trade off civil liberties for terrorism risks (Viscusi & Zeckhauser, 2003). It shows that those who have different experiences and situations make different decisions of privacy preferences even for the same benefit (Metzger, 2004; Taddei & Contena, 2013).

2.5 Health Information and Privacy

Health studies support ideas of health information exchange (HIE), which means different health parties or organizations share patients' personal information electronically (Kaelber & Bates, 2007; Wen, Kreps, Zhu, & Miller, 2010). The benefits of the HIE system is to give helpful information quickly to clinicians for better diagnosis and to reducing unnecessary testing (Shapiro et al., 2006), but there is always risk of information breach (McGraw, Dempsey, Harris, & Goldman, 2009).

Privacy has been mentioned in health record studies as a challenge in building effective health information systems (Vest & Gamm, 2010), but most discussions focus on technical improvement, such as key schemes and authentication, and access control (Fernández-Alemán, Señor, Lozoya, & Toval, 2013). Some studies investigated users' perspectives of health information exchange and electronic access to personal health records. According to the Health Information National Trends Study, older people were more likely to rate HIE as important (Ancker, Edwards, Miller, & Kaushal, 2012). Overall, patients understand the need of exchanging health information between health organizations, but they are also concerned about

unexpected privacy breach and misuse of individual health data (Simon, Evans, Benjamin, Delano, & Bates, 2009).

The limitation of these studies is that the conclusion is too general. People know the benefit of HIE or health records but also have concerns about privacy violations. Based on the review of privacy concepts we know that the sensitivity of personal information is context dependent. Therefore, to generate effective health systems it is important to know what makes individuals worried and what their actual privacy decisions might be under certain context.

2.5.1 Public and Community Health

The goal of health organizations or agencies is to enhance public/community health security (Proenca, 1998). Community is a sub-dimension of a public health program where prevention and intervention are applied while public health is often indicated at national levels (Diallo, D. D & Frew, P. M., 2014; MacQueen, et al., 2001). The definition of community is varied depending on the goal of health intervention and the intervention settings include worksites, healthcare facilities, religious organizations, schools, neighborhoods, and so on (Pearson et al., 2013).

Community context is an important factor of health outcomes under certain interventions (MacQueen et al., 2001). On a researcher or a health agency side, the definition of community is obvious because the boundary of community is determined by the purpose of the proposed intervention. Because of the unique context of a defined community, it is hard to estimate health outcomes and the effect of interventions in general communities. On an individual side, the boundary of community is not clear. MacQueen et al. (2001) conducted an interesting interview study to understand the definition of community from the perspectives of general individuals. They interviewed 118 participants from different locations and socio-demographic backgrounds.

The interviewees answered the question “The word 'community' means different things to different people. What does the word community mean to you? What is a community?” From the interviews, they found five elements when people define community: identity, sense of place, sharing perspectives, social ties, and diversity. Although they narrowed down the meaning of community to the five elements, still it is quite broad and context dependent. It shows that it is critical to deliver a clear definition of community to individuals when researchers investigate individuals’ perspectives on community related issues.

This study applied the concept of local community to the research question and looked at how individuals’ privacy decisions differed depending on their perception of local community. The way of defining local community would be a cue how the person conceptualize community or public. RQ4 compared the effects of risk and benefit on information disclosure at different levels: individual, community, and public with considering the concept of local community.

RQ4: How do the amount of information disclosure and the degree of privacy concern change when participants encounter different levels of risks and benefits at the individual, community, and public levels, and how does individuals’ perception on local community affect their information?

2.6 Research Questions and Approach

The goal of this dissertation was to understand how different dimensions of privacy risks and benefits were related to individuals’ information disclosures, and how privacy concern changed with their disclosure behaviors. The two studies in this dissertation adopted the privacy decision process, which explains information disclosure behaviors based on the calculation of risks and benefits. I asked the following specific research questions:

RQ1: What is the relationship between the amount of information disclosure and the level of privacy concern? (Study 1 & Study 2)

H1: Individuals who disclose more information have lower privacy concern.

RQ2: What is the effect of trust on information disclosure and privacy concerns?

H2_1: Individuals who have higher trust to U.S. government agencies report lower privacy concern when they disclose the same amount of information.

H2_2: Individuals who have higher trust to the Outbreak Alert System report lower privacy concern when they disclose the same amount of information.

RQ3: What are the effects of risks (control and access) and benefit (individual and public) on information disclosure? What interaction effects of risks and benefit on information disclosure? (study 1)

RQ3_1: What are the effects of risks (control and access) on information disclosure?

H3_1a. Individuals who have high control will disclose more information than individuals who have low control.

H3_1b. Individuals who are in the small access condition will disclose more personal information than individuals who are in the large access condition.

RQ3_2: What are the effects of individual or public benefit on information disclosure?

H3_2: Individuals who are informed of an individual benefit will disclose more information than individuals who are informed of a public benefit.

RQ3_3: What are the interaction effects of risks and benefits on information disclosure?

H3_3: Interaction of control and access will be different for the public and individual benefits conditions.

RQ4: How does the amount of information disclosure change when participants encounter different levels of risks and benefits at the individual, community, and public levels? In this process, how does individuals' perception on local community affect their information

disclosure? (Study2)

To investigate these research questions, I designed two experimental studies that allowed for the examination of the amount of information disclosure and privacy concerns in different benefit and risk conditions, using a possible outbreak situation as the context for the experiment. To manipulate the situation of information disclosures, the two studies used the Outbreak Alert System created for this experiment to collect individuals' personal information. Participants were informed that the website was created for collecting and disseminating information regarding virus outbreaks, including personal information, and that they would receive benefits in a health emergency in return for their participations. They were encouraged to sign-up for the website by filling out a registration form online. The sign-up form contained items to measure information disclosures.

Previous privacy decision studies have mainly considered benefits and risks at the individual-level. From real world examples of public security, we have observed that public-level benefits and risks can also influence individuals' decisions about information disclosure. Studies about social dilemmas show individuals' choices when they have conflict situations of individual interests and others' interests (Fehr & Fischbacher, 2003). The two experiments emphasized the tension of benefits and risks at different levels (i.e., individual, community, and public). I invited participants in a situation of competing interests between individual and others, and encouraged them to make a decision of privacy in the situations.

Study 1 manipulated individual and public levels of health benefits and individual levels of privacy risk. It follows previous privacy studies, which applied different information for privacy risks with the same benefit across different conditions. Study 1 also included a public level health benefit condition in addition to an individual level benefit condition with different

conditions for risks. Alternately, study 2 manipulated both health benefits and privacy risks with different levels of information: individual vs. community vs. public.

The reason for including the community level in study 2 was to understand the effects of different information about benefits and risks on privacy decisions, which is relevant to public health contexts. Specifically, health literatures often differentiate community health from individual or public health (Israel, Schulz, Parker, & Becker, 1998). Community has diverse meanings such as local, organization, and ethnicity. To make it clear, this study uses "local community" and asks participants to define "local community" prior to the experiment by giving them five definitional options to choose from: 1) state, 2) county, 3) city, 4) neighborhood, or 5) none of them (specify). It is important for individuals to describe community as they understand it, because decisions regarding information disclosure have been shown to vary depending on how one defines "community." Moreover, a virus usually starts from a location and spreads out geographically. In this way, geographical boundary location is critical to controlling an outbreak situation. This is where local community comes into play, because community safety is highly related to the safety of individuals living in a given area.

The two studies measured privacy concern with survey items after the information disclosure. Studies showed that individuals disclose their personal information despite their level of privacy concern. Thus, it is possible that privacy concern is not a strong predictor of information disclosure, because users are forced to disclose their information to get benefits from specific services. Privacy concern is one of the most important variables to understanding users' perceptions regarding their worries about disclosed information. This study was interested in understanding users' privacy concern for specific items of information they choose or do not choose to disclose. The following method section explains the details of these approaches.

3 METHODS

3.1 Online Experiment: Outbreak Alert System

The study created an online health platform, the Outbreak Alert System, which ostensibly aimed to manage future outbreaks. It was important to design the Outbreak Alert System in a way that ensured participants perceived they were engaging with (e.g. registering, reading content) a real website. If they thought they were participating in an experimental study, it would bias their responses. To increase perception that the platform was real, I created a new domain only for the website: outbreakhealth.org and designed the website accessible by both laptops and mobiles. Also, I recruited sample from general population with a range in age, gender, and ethnicity to increase external validity and generalize the results back to the population.

Figure 2 The main page of the Outbreak Alert System

Note. The main page of the OAS system. When participants visited the system from Qualtrics, they directly went to the enrollment page. They could access the system using any digital device.

Although the website was created and operated like as a real website as far as possible, there were necessary processes which were not quite same to a real website such as a consent form, survey items, and recruiting advertisement. To avoid unnecessarily doubt on these procedures, I set the experiment circumstance as a beta-testing of governmental website. The recruiting advertisement stated that the U.S government created the Outbreak Alert System, which was currently in need of beta-testing before its official launch. Participants were informed that the alert system was created for collecting and disseminating information regarding viral outbreaks, including personal information, and that they would receive benefits in a health emergency in return for their participations. However, the advertisement and consent form did not specify possible privacy risk which was related to the experimental manipulation because it might cause bias on the study. Also, I minimized information about the agents of the website. I chose the Federal Emergency Management Agency (FEMA) and the Department of Human and Services as the operators of the website. I considered organizations which implies general federal services and public emergency management rather than pointing out specific services. It was approved by the IRB with providing debriefing at the end of experiment.

Compared to other real websites, the structure of the experimental website was very simple to prevent a participant read too much information inside of the website. Participants were forwarded directly to the enrollment page, and when they tried to move on other pages, they had a message which said, "You can read further information after logging in."

There were participants who were not quite persuaded by the setting. To exclude answers from those participants, I measured how much participants believed they were interacting with a real website at the end of the experiment.

Overall, the experiment website included background information of the site, registration, post-survey after the registration, and debriefing. Through the beta-test, participants read different privacy policies depending on experimental conditions and filled out a registration form. After signing up, they answered questions about privacy concern for the registration process and trust to the system.

3.2 Sample

When an outbreak occurs, it can affect a country's entire populations regardless of demographic differences (e.g. age, gender, or income). For this reason, this study derived a sample from the general population of the U.S. in which the only inclusion criteria was that they were 18 years or older, and who were the Internet users to interact with the Outbreak Alert Sytem. To acquire diverse sample, I recruited participants through the Qualtrics Online Panel service using quotas from the 2010 U.S Census: gender (Male: 49%) and age (18-24:15.6%, 25-34:22.1%, 35-44:20.3%, 45-54: 21.6%, 55-64: 20.4%, 65+:23.9%). I paid Qualtrics $5 per participant, of which $2 cash equivalent incentive was paid to the participants.

3.3 Study 1: Different Privacy Risk with Public or Individual Benefit

3.3.1 Study 1 design

Study 1 looked at the degree of individuals' information disclosure as privacy decision behavior when the individuals encountered different situation of health benefits and privacy risks. The study used a fully crossed 2 (benefits: individual benefit vs. public benefit) by 2 (access: large boundary of recipients - public vs. small boundary of recipients – governmental agencies) by 2 (control: high control - getting permission before distribution vs. low control - no permission before distribution) independent groups experimental design with one control group.

The benefit conditions were manipulated into public and individual benefits to see how

the different information of benefits affect individuals' privacy decisions when they had different information of privacy risks. Study 1 operationalized two types of risk factors: control and access. Control refers to the possibility of changing the privacy risk by a subject of personal information, and the experiment uses two conditions to measure control: high and low. In the high control condition, the system could not release participants' information without their permissions while in the low control condition, the system could release participants' information without their permissions.

The other condition was boundary access by others, which means the spectrum of access to an individual's personal information by others. Study 1 manipulated two boundaries of access by others: only governmental agencies and governmental agencies as well as the public. In the small access condition, only governmental agencies access have participants' information in an emergency but in the large access condition, not only governmental agencies but also public could access participants' information in an emergency. Table 1 shows all conditionas and the numbers of participants in each condition.

Table 1 Study 1 design tables with numbers of participants in each condition

High Control

	Individual Benefit	Public Benefit
Large Access	35	36
Small Access	40	36

Low Control

	Individual Benefit	Public Benefit
Large Access	37	36
Small Access	34	36

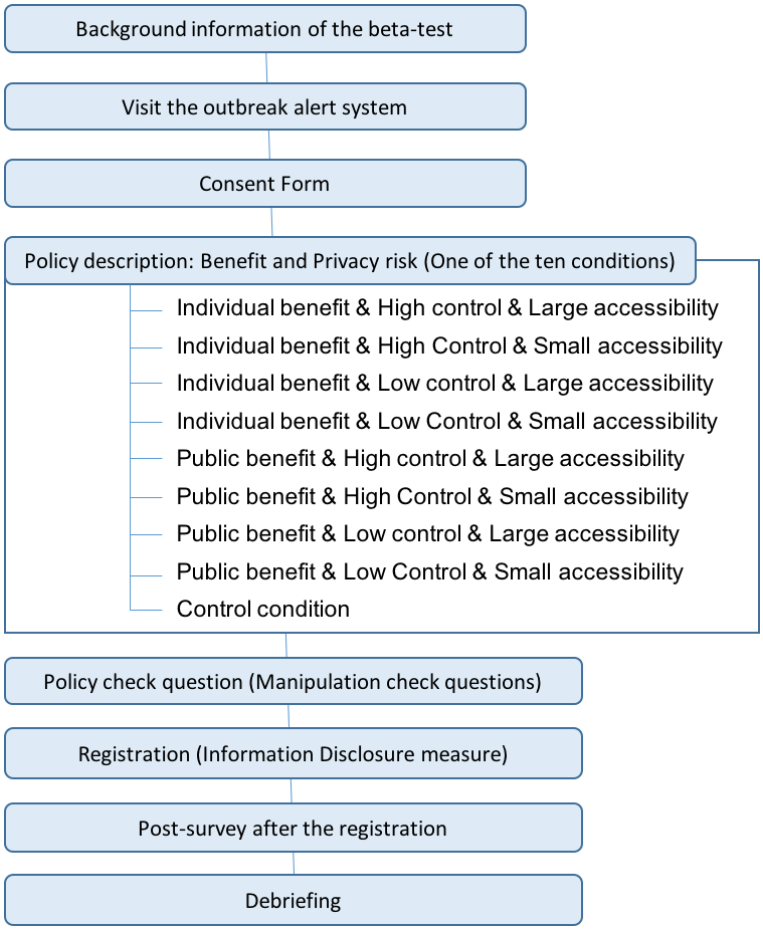
Control condition : 36

Note. Study 1 had a 2 x 2 x 2 factorial design with one control condition. A total of 326 participants participated in the study and they were randomly assigned to each condition. Each participant read privacy policy manipulated with one of the two control conditions, one of the two access conditions, and one of the benefit conditions.

3.3.2 Study 1 Procedure

Figure 3 shows the process of Study 1. Participants who were recruited through Qualtrics Online Sample Service received a link to a pre-screen survey, which provided them background information about the beta-testing of the Outbreak Alert System, as well as asked them their age, gender, and ethnicity to ensure a diverse sample population. Following, eligible participants were forwarded to the enrollment page of the Outbreak Alert System. Once the participants agreed to sign up for the system, they first completed and signed an informed consent form, which also included background information and other IRB related information. After the participants provided consent, they were randomly assigned to one of nine conditions. Once assigned, they read a description of each condition that explained recent virus breakouts and the benefits and possible risks of the system. The description of benefits and possible risks were different depending on condition. Following, participants were asked three true or false questions about the description for a manipulation check purpose. For example, "My information can be released without my permission." If they answered correctly, they were allowed to proceed. If they did not answer correctly, they had one more chance to restart the experiment from the beginning.

Figure 3 Study 1 process



Note. Participants were informed that they were going to join a beta-test of a new Outbreak Alert System. They read the background information of the system and visited the system. After they read the consent form, they were randomly assigned to one of the nine conditions.

Participants, who passed the manipulation check moved to the sign-up page. They filled out a registration form. The registration form consisted of questions about health status, demographic information, and identifying information such as name, address, and phone number. When they finished signing up, a "next" button brought them to the post-survey. The post-survey included individuals' privacy concern regarding the signup process, trust to the system, and general privacy concern after registration. The post-survey included two attention check questions such as "please check 'Strongly agree'."

3.3.3 Study 1 manipulation

Participants were assigned to either individual or public health benefit conditions. Participants in the individual health benefit condition, were informed that the benefit of registering with OSA was that if an emergency occurs then, a health agency would contact them directly if they are in a high-risk patient group based on their profile information. In the public health benefit condition, they were informed that "anyone" would receive the benefit instead of indicating "you" in the description.

After the participants read the benefits of the health portal, they read how their profile information would be used. The information policy was a manipulation of the different dimensions of privacy risk in the experiment. The experimental control group did not have any information about benefit and risk.

a) Individual benefit:

You will gain direct, certified alerts and information from the Outbreak Alert System (OAS) when outbreaks occur. If you are in a high-risk group for exposure, then the OAS will contact you directly and monitor your symptoms.

b) Public benefit:

The public will gain direct, certified alerts and information from the Outbreak Alert System (OAS) when outbreaks occur. The OAS will provide direct contact and symptom monitoring for those who are in a high-risk group exposure.

c) Risk_ Access – large group:

We share your personal information with not only governmental health agencies but also with public in outbreak situations.

d) Risk_ Access – Small group:

We share your personal information with only governmental health agencies.

e) Risk_Control – high control:

If you are in a high-risk group for exposure, we may release your information to control disease with your permission.

f) Risk_Control – low control:

If you are in a high-risk group for exposure, we may release your information to control disease without your permission.

3.4 Study 2: Individual, Community, and Public Risk and Benefit

3.4.1 Study 2 design

Study 2 expanded upon the privacy argument in Study 1 to include both the community and public level for both benefit and risk. Specifically, Study 1 looked at only individual level risk, and individual and public level health benefits. Study 2 examined individuals' information disclosures and privacy concerns when they have different information on boundaries of benefits and risks; individual, community or public levels of benefits and risks. Study 2 used crossed 3 (benefit: individual benefit vs. community vs. public benefit) by 3 (risk: individual risk vs. community vs. public risk) independent group experimental design including one control group.

Table 2 Study 2 design table with numbers of participants in each condition

	Individual Risk	Community Risk	Public Risk
Individual Benefit	33	31	31
Community Benefit	30	32	34
Public Benefit	29	31	31

Control Condition: 31

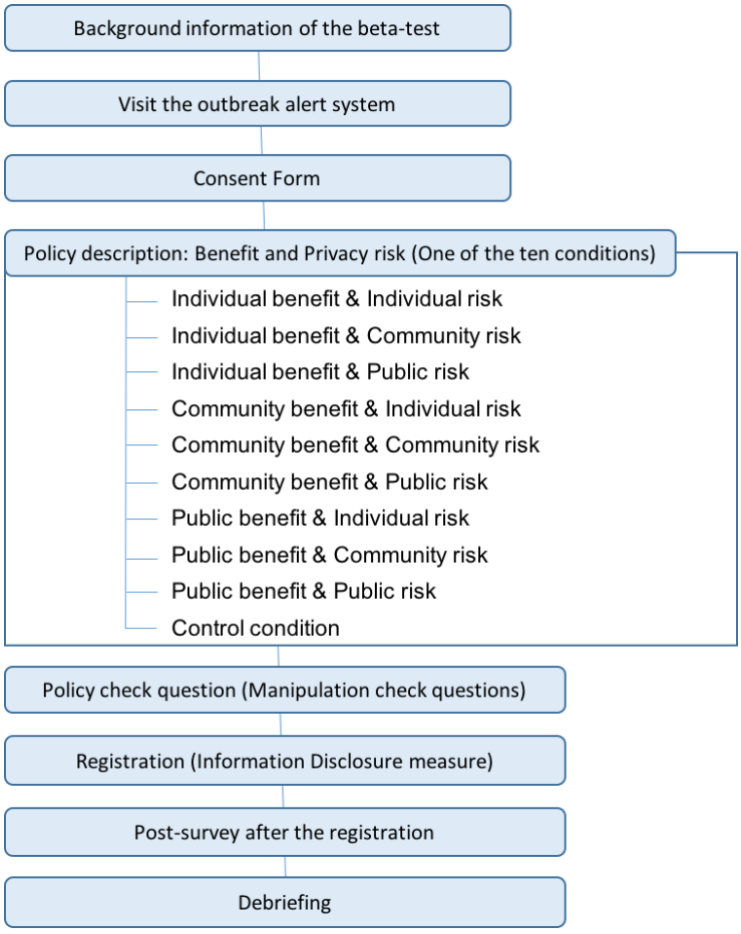
Note. Study 2 had a 3x3 factorial design with one control condition. A total of 313 participants participated in the study and they were randomly assigned to one of ten conditions including the control condition. Each participant read privacy policy manipulated with one of the three benefit conditions and one of the tree benefit conditions.

3.4.2 Study 2 procedure

The experimental context of the Study 2 was the same as in Study 1. Participants first answered questions regarding their age, gender, and ethnicity for a pre-screen purpose. Following, participants were forwarded to the enrollment page of the Outbreak Alert System. On the enrollment page, participants were asked to provide consent first. Once they agreed to the consent form, participants were randomly assigned to one of ten conditions including one control condition, and read a description of each condition. After seeing the description, participants were asked three true or false questions, which acted as the manipulation check. If they answered incorrectly, it meant they did not pay attention to the descriptions, so they were given one more chance to restart the experiment from the beginning. If a participant failed to pass the manipulation check the second chance then the participant was excluded from the study.

Participants who passed the manipulation check moved on the sign-up page where they were asked to fill out a registration form. The registration form consisted of questions about health status, demographic information, and identifying information such as names, address, and phone number. All questions were not required to check the amount of self-disclosure. At the end of the experiment, they were asked to answer the definition of community with a sense of place. This question was to understand how participants defined local, which was important for their privacy decisions in associated with community benefit and risk.

Figure 4 Study 2 process



Note. The process of Study 2 was same to Study 1. The difference was the condition part. Participants were informed that they were going to join a beta-test of the Outbreak Alert System. They read the background information of the system and visited the system. After they read the consent form, they were randomly assigned to one of the ten conditions.

3.4.3 Study 2 manipulations

Study 2 used the same Outbreak Alert System which was used for study 1. In the beginning of the experiment, the system explained to participants that it was important to collect information of suspected patients for managing outbreaks in an emergency. The description stated that the system was designed to control future outbreak situations and they were invited to participate as beta-testers before the official release of the platform. In the individual benefit condition, participants were informed that if an outbreak emergency were to occur, a health

agency will contact “you” directly if “you” are in a high-risk patient group, which is determined by the information in “your” profile. In the community benefit condition and public benefit condition, the description stated the “community” or the “public” could get the benefit instead of indicating “you”. Participants were informed about different benefits as well as different risks depending on their assigned conditions. The experimental control group did not have any information about benefit and risk. Specifically:

a) Individual benefit:

You will gain direct, certified alerts and information from the Outbreak Alert System (OAS) when outbreaks occur. If you are in a high-risk group for exposure, then the OAS will contact you directly and monitor your symptoms.

b) Community benefit:

Your local community will gain direct, certified alerts and information from the Outbreak Alert System (OAS) when outbreaks occur. If your local community is in a high-risk group for exposure, then the OAS will contact your community directly and monitor symptoms in your community.

c) Public benefit:

The public will gain direct, certified alerts and information from the Outbreak Alert System (OAS) when outbreaks occur. The OAS will provide direct contact and symptom monitoring nationally for those who are in a high-risk group exposure.

d) Individual privacy risk:

If you are exposed to virus, your personal information can be shared with others to prevent further contagion in outbreak situations. Others are able to check who you are and where you live.

e) Community privacy risk:

If your local community is exposed to virus, your community information can be shared with others to prevent further contagion in outbreak situations. Others are able to check who the infected people are and where they live in your community.

f) Public privacy risk:

If the public is exposed to virus, personal information of infected public can be shared with others to prevent further contagion in outbreak situations. Anyone can check who are infected and where they live in.

3.5 Common Measures

Information disclosure. Actual disclosure has been measured with a total number personal information items subjects supplied (Norberg et al., 2007; Special & Li-Barber, 2012). This study followed suit in which Information disclosure was measured by totaling the number of items answered by participants in the sign-up form of the system. I developed the measure for information disclosure based on criteria that they reflect typical online disclosure requests in a health portal service, which is related to outbreak situation, and they reflect specific types of information ranging from lower to higher sensitivity of information. To develop the information items, I searched health-related literatures and health portals, and listed an initial 34 information items related to contact information and health status. The initial 34 items were reduced to 30 via a pretest (N=175), in which I measured how much individuals think each question is sensitive on a 1 (not at all sensitive) to 5 (very sensitive) scale.

Privacy concern. The measure for privacy concern measure was adopted from Hong and Thong (2013), which consists of four sub dimensions: collection, secondary usage, improper access, and control (full items are listed in Appendix 1). The measure was modified to the

context of the experiment. All the privacy concern items were measured with Likert-type questions with a 7-point response format (1: Strongly disagree, 7: Strongly agree).

Trust. The trust measures were adopted from Fogel and Nehmad (2009) and consisted of three-items constructs for both trust to the system and trust to government. The items were measured with Likert-type questions with a 7-point response format (1: Strongly disagree, 7: Strongly agree).

3.6 Manipulation Check

Three manipulation check questions were presented to each participant. All questions were true-or-false questions to test whether the participants were aware of the conditions they were involved in. For example, a participant in Study 1 assigned to the individual benefit, high control, and small access condition, were asked, "You will get direct symptom monitoring from the OAS when you are in a high-risk for exposure," "Your information can be released without your permission", and "Your information can be shared with only health agencies." The manipulation questions were different depending on conditions, and the answers were "yes" or "no." Full questions are presented in Appendix 1.

3.7 Pretest

3.7.1 Sensitivity test

The measure for information disclosure consists of a number of item related to personal information. Personal information is detailed to distinguishing individual identity such as full name, home address, email address, phone number, date of birth and so on. All personally identifiable information should be protected under privacy laws, but there are different levels of sensitivity to each individual. For example, a person may easily share his or her email address, but may not share his or her phone number as easily as the email address.

To include a fair number of items which have diverse levels of information sensitivity, I conducted a pretest to check sensitivity of personal information. First, I created a list of 34 personal items based on examples from registration forms of health-related portals and virus checklist. A list of full questions was attached in the Appendix. In the pretest, I recruited 208 participants from MTurk and paid $0.7 for less than 10 min survey. MTurk is a crowdsourcing platform that allows researchers to post human intelligence tasks (HITs) such as participating surveys and decoding record files. Participants (workers) can register and complete the tasks for compensation. I explained the study background first, and asked how much sensitivity participants felt with each question in the context of possible outbreak on a scale of 1-5 (1: not sensitive – 5: very sensitive).

The average was 2.54 (Lowest:1.51-highest:3.99). I divided into four groups based on the sensitivity levels (1: under 2.00 2: between 2.01-2.49 3: between 2.50-2.99 4: over 4.00). I selected 7 or 8 items from each group to include those question to the registration form. From the pretest, I removed some questions which were too sensitive to ask and were not appropriate for health portal such as “what is your SSN?” and “what is your date of birth?” Also, I removed a couple of questions which were similar to other questions. For the question “what is your emergency contact information (name, relationship, phone number)?”, I separate it to individual three questions. The final number of questions was 30 and those questions were included to the registration form in the Outbreak Alert System as the measure of information disclosure.

Because I changed a couple of question after the pre-test, I conducted another pre-test to measure sensitivity of each question after finishing the experiment to include sensitivity in analysis. I recruited 82 participants through MTurk and all process was same to the first sensitivity pre-test.

3.7.2 Manipulation check test

I conducted a test to find an appropriate number of chances for the manipulation check. Participants read privacy policies in each condition and needed to answer manipulation check questions to go forward. The experiments contained three manipulation check questions. I gave another chance for those who did not pass the first manipulation check. For example, if a participant does not pass one of the manipulation check questions, the system takes the participant back to the privacy policy page, offering another chance to answer the manipulation questions.

The test was conducted with MTurk users to check how many participants passed the manipulation check at the first chance, second or third chance. A total of 71 MTurk users completed the test and 24 of them passed manipulation check questions on the first chance, 5 of them passed it at the second chance and 7 of them passed it at their third attempt. The rest passed the test with over three tries or gave up during repeated tests. It turned out that giving several chances did not make a dramatic change on success rate. Those who did not read the privacy policy carefully did not tend to change their attitude with additional changes. I decided to give just one more chance to participants who did not pass at the first chance.

3.7.3 Experiment beta-test

I recruited 107 participants for Study 1 and 101 participants for Study 2 through the community paid pool on SONA to conduct the final pre-test to check whether the experiment had no issue to run. The SONA system is an online management system which researchers can recruit participants. The community paid pool has broader range of participants than regular pool on SONA which includes faculty members, staff, and other people around local community in addition to college students. On the system, about 55% participants were not undergraduate

students. For the experiment, each participant received $5 for their participation. The beta-test was conducted between Sep 20, 2016 and Sep 23, 2016 for both Study 1 and Study 2.

4 RESULTS

Following are the results for both Study 1 and Study 2. The objective of Study 1 was to investigate how individuals' privacy preference changed when they had different types of privacy risk and different types of boundaries of privacy benefit. The objective of Study 2 was to investigate how individuals' privacy preferences changed when they had different boundaries of privacy risk and benefit. Both studies were designed to examine the relationship between information disclosure and privacy concern and the effect of different information of privacy risk and benefit on individuals' privacy preferences. The two studies shared the same research questions, but each had a different design to aid in the manipulation of different situations of privacy risk and benefit.

4.1 Study 1: Permission on Information Distribution

4.1.1 Sample distributions

The online experiment for Study 1 was open from November 4, 2016 to December 6, 2016. Participants were removed from the experiment if they were unable to answer the two attention check questions or did not complete the entirety of the experiment. A total of 1670 participant completed the experiment but only 326 participants passed the attention check questions. There were nine experimental conditions, including the control group. The average number of participant for per condition was 34. The lowest number was 30 and the highest number was 34. There were a fairly equal number of males and female consistent across conditions. (See Table 1)

Table 3 Demographics (N=326)

	N(%)
Gender	
Male	161(49.7)
Female	163(50.3)
Ethnicity	
White	*222*(68.1)
Black	*34(10.4*)
Hispanic	21(6.4)
American Indian	*21*(6.4)
Asian	*19(5.8*)
Others	7(2.1)
Age	1
18-24 years old	33(10.1)
25-34 years old	59(18.1)
35-44 years old	64(19.6)
45-54 years old	63(19.3)
55-64 years old	68(20.9)
65 years or older	37(11.3)

Note. The data was collected through Qualtrics Nov 4 2016 through Dec 6 2016 with quotas from 2015 US Census. It was hard to recruit non-white and 65 years or older sample because of the composition of Qualtrics panels. The data included two missing cases. Participants answered their demographics first and Qualtrics forwarded them to the main experiment after checking the quotas. In this process, demographics information of two participants could not be forwarded to the main experiment. However, the two participants completed the experiments.

4.1.2 Variables

Privacy concern and trust. Table 4 shows measures of privacy concern and trust. I adopted privacy concern measure from previous studies which used multi-dimensional privacy concern measures (e.g. Hong & Thong, 2013, Malhotra et al., 2004; smith et al.,1996). The measure included four sub-dimensions of privacy concern: collection, secondary usage, improper access, and control. There dimensions specified different causes of privacy concern during the process of information collection and usage.

Table 4 Descriptive of included variables (N=326)

	Reliability	Mean(SD)
Privacy concern	.973	4.43(1.62)
(Collection) - It bothered me when the Outbreak Alert System asked me for personal information. - When the Outbreak Alert System asked me for personal information, I thought twice before providing it. - I was concerned that the Outbreak Alert System was collecting too much personal information about me.		
(Secondary Usage) - I'm concerned that when the Outbreak Alert System would use the information for other reasons. - I'm concerned that the Outbreak Alert System would sell my personal information in their computer databases to other organizations. - I'm concerned that the Outbreak Alert System would share my personal information with other organizations without my authorization.		
(Improper Access) - I'm concerned that the Outbreak Alert System database that contains my personal information is not protected from unauthorized access. - I'm concerned that the Outbreak Alert System does not devote enough time and effort to preventing unauthorized access to my personal information. - I'm concerned that the Outbreak Alert System does not take enough steps to make sure that unauthorized people could not access my personal information in their database.		
(Control) - It bothers me that I do not have control of personal information that I provided to the Outbreak Alert System. - It bothers me that I do not have control or autonomy over decisions about how my personal information was collected, used, and shared by the Outbreak Alert System. - I'm concerned when control is lost or unwillingly reduced as a result of information sharing with the Outbreak Alert System.		
Trust to the OAS	.906	4.65(1.09)
- The Outbreak Alert System is a trustworthy system. - I can count on the Outbreak Alert System to protect my privacy. - The Outbreak Alert System can be relied on to keep its promises.		
Trust to the Governments	.930	3.76(1.56)
- I trust Government Agencies. - I trust Government Agencies keep my best interests in mind.		

Note. Measures of privacy concern and trust variables. Privacy concern consisted of 12 items. Two types of trust were measured: trust to the system and trust to U.S. government agencies.

The Principal Component Factor analysis extracted only one factors from all 12 items with the item loading ranging from .839 to .932. All the items were integrated into a single privacy concern variable. The reliability of the items was .973. The mean of privacy concern was 4.43 (SD=1.62).

Two types of trust were measured: trust to the Outbreak Alert System and trust to U.S. government agencies. The mean of trust to the Outbreak Alert System was 4.65 (SD=1.09). The mean of trust to U.S. government agencies was 3.76 (SD=1.56). Overall, participants exhibited higher trust to the system than trust to U.S. government agencies.

Information disclosure. Information disclosure was measured by all adding up the number of questions each participant answered on the registration form during the experiment. The registration form consisted of a total of 30 questions (Table 5).

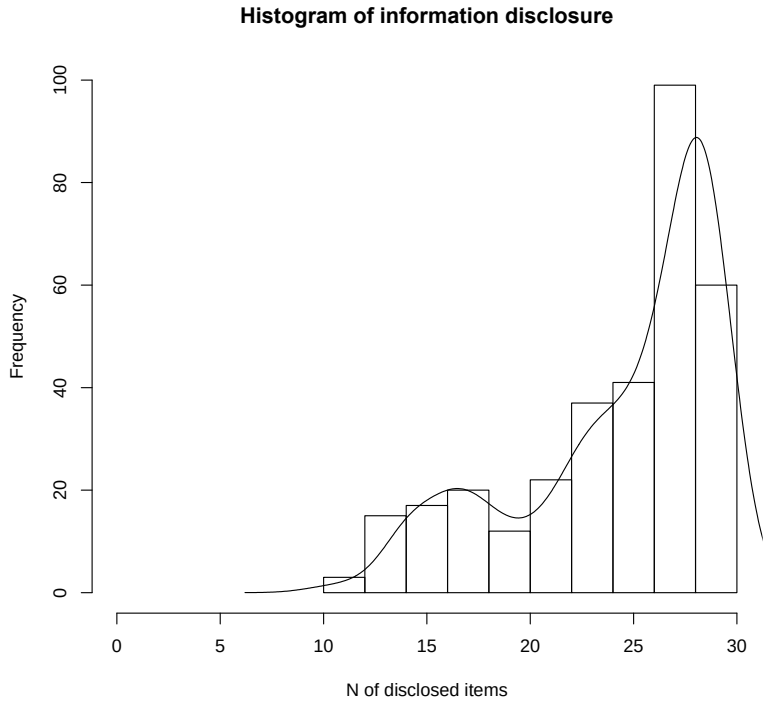
Table 5 Measures of information disclosure

Questions	Sensitivity	Frequency (N=326)	
	Mean(SD)	Answered	Not answered
Have you experienced a fever during the last 2 weeks?	1.53(0.88)	324	2
Have you traveled to South America or Africa in the last two months?	1.47(1.03)	324	2
Do you have household members who traveled to South America or Africa in the last two months?	1.55(1.05)	325	1
In the last 2 weeks, did you feel sick to your stomach?	1.57(0.98)	324	2
Have you experienced brain fog (confusion, forgetfulness, or trouble concentrating) in the past 4 weeks?	1.79(1.10)	322	4
Did you experience a unusual/new rash during the last 2 weeks?	2.05(1.26)	319	7
What is your Blood type?	1.81(1.05)	181	145
Have you had sex in the past 2 weeks?	4.02(1.08)	314	12
Do you use birth control?	3.41(1.30)	319	7
Are you currently in a relationship?	2.48(1.17)	318	8
Do you find yourself 'eating emotionally': eating unhealthy foods when you're not hungry, as a response to stress?	2.53(1.33)	322	4
How often do you drink alcohol?	2.40(1.20)	297	29
Have you gained more than 5 pounds in weight in the last two months?	2.53(1.35)	321	5
Are you disabled?	2.64(1.21)	319	7
Have you ever had a blood test taken?	1.86(1.12)	318	8
Are you pregnant?	2.86(1.38)	321	5
What is your current weight?	2.83(1.34)	313	13
What is your insurance company?	3.02(1.54)	222	104
What is your first name?	2.24(1.50)	273	53
What is your last name?	3.02(1.64)	263	63
What is your address?	4.72(1.44)	232	94
What is your zip code?	2.48(1.47)	265	61
What is your phone number?	3.50(1.49)	202	124
What is your email address?	3.28(1.44)	252	74
What city do you live in?	2.24(1.23)	257	69
What state do you live in?	1.72(1.06)	268	58
Where do you work? (Name of the place)	3.57(1.30)	198	128
What is your emergency contact information? - name	3.31(1.44)	200	126
- relationship	3.09(1.48)	190	136
- phone number	3.47(1.40)	173	153

Note. Questions for the information disclosure measure presented to participants on the Outbreak Alert System registration form. Frequency was determined by counting the number of participants who answered or did not answer each question.

The mean of answered question for the information disclosure measure was about 24 (out of 30 questions) (SD=4.79). Such a high mean exhibits the willingness of participants to disclose their personal information across conditions. Figure 5 presents a histogram of the number of disclosed items. All participants disclosed their personal information on more than 10 items and the data was left skewed.

Figure 5 Distribution of information disclosure



Note. Distribution of disclosed information across conditions. Participants disclosed personal information an average 24 times with the distribution of disclosure skewed to the left.

4.1.3 Information disclosure, privacy concern, and trust

One of the goals of this research was to describe the relationship between information disclosure and privacy concern (RQ1). In both Study 1 and Study 2, information disclosure was measured by frequency of items answered on the registration form of the Outbreak Alert System with privacy concern measured by pointing out the specific behavior of information disclosure via survey items following the manipulation.

A regression was performed for privacy concern with information disclosure included as a predictor to test Hypothesis 1: Individuals who disclose more information have lower privacy concern (see Model 1; Table 6). Information disclosure was mean centered to make the interpretation of parameter estimates easier. In model 1, people who disclosed 24 items (mean) report 4.43 points of privacy concern ($\beta = 4.43$, $SE = .08$, $p < .001$). There was a negative relationship between information disclosure and privacy concern. When participants disclosed one more item, privacy concern decreased 0.13 point ($\beta = -.13$, $SE = .02$, $p < .001$). Results from Model 1 provide support for Hypothesis 1, therefore, it was accepted.

Table 6 Regressions for privacy concern

	Model 1 B (SE)	Model 2 B (SE)
Intercept	4.43 (.08)***	4.43 (.07)***
Information disclosure (N of disclosed items)	-.13 (.02)***	-.10 (.02)***
Trust to the OAS system		-.57 (.09)***
Trust to government		-.06 (.06)
R^2	.14	.30
F	54.81***	48.01***

Note. $p < 0.001$, '***'; $p < 0.01$, '**'; $p < 0.05$, '*'; $p < 0.10$, '•'
Regressions for privacy concern with information disclosure and trust. There was a negative relationship between information disclosure and privacy concern, and trust to the system decreased privacy concern.

Research question 2 was constructed to further understand the relationship between information disclosure and privacy concern by including the influence of trust, specifically: What is the effect of trust on information disclosure and privacy concerns? Two types of trust were measured as trust of U.S. government Agencies as well as trust of the Outbreak Alert System. It was hypothesized that individuals who have higher trust of government agencies would report lower privacy concern when they disclosed the same amount of information

(H2_1). It was also hypothesized that individuals who have higher trust of the Outbreak Alert System would report lower privacy concern when they disclosed the same amount of information (H2_2).

A regression was performed with information disclosure, trust to U.S. government agencies, and trust to the Outbreak Alert System as predictors for privacy concern to test H2_1 and H2_2 (see Model 2; Table 4). Trust values were mean centered to make the interpretation of estimates easier. Results indicate that people who disclosed 24 personal information items and had a mean of trust to the Outbreak Alert System (4.65) and U.S. government agencies (3.76) reported 4.43 point of privacy concern ($\beta = 4.43$, $SE = .07$, $p < .001$). Further, as people disclosed one more personal item, their privacy concern decreased by 0.10 point ($\beta = -.10$, $SE = .02$, $p < .001$). It was also found that when trust to the Outbreak Alert System increased one unit, privacy concern decreased by -0.57 points when information disclosure and trust to U.S. government agencies were held as mean ($\beta = -.57$, $SE = .09$, $p < .001$). Therefore, hypothesis 2_1 was not supported and hypothesis 2_2 was supported. Trust to U.S. government agencies also had a negative relationship with privacy concern, but it was not statistically significant.

4.1.4 The amount of information disclosure with different privacy risk and benefit

A further goal of this research was to estimate the effects of control over the distribution of information (i.e. participant's providing permission or not before personal information is released); the boundary of access to information (i.e. if personal information is released to the public or only government agencies); and benefits (i.e. whether the participant or the public will receive direct benefit if there is a possible outbreak) on privacy concern. It was hypothesized that a) individuals who had high control of their personal information would disclose more information than individuals with low control (H3_1a); and b) individuals in the small access

condition (i.e. government access only) would disclose more personal information than individuals in the large access condition (i.e. public access) (H3_1b). It was also hypothesized that individuals who were informed of an individual benefit would disclose more information than individuals who were informed of a public benefit (H3_2).

Tobit regression was used to test these hypotheses because it is a regression type that is designed to estimate when the linear relationship between variables and its dependent variable is either left or right censored. Information disclosure was the dependent variable that was right censored (The maximum value was 30).

Table 7 Tobit regression for information disclosure

	B (SE)
Intercept	22.38 (1.42)***
Benefit:	
Individual (0)	
Public (1)	.14 (.05)
Access	
Small access (0)	
Large access (1)	.21 (1.07)
Control	
Low control (0)	
High control (1)	-2.13 (1.03)*
Trust to the OAS	.71 (.25)**
Privacy concern	-1.02 (.23)***
Public benefit:Large access	-2.09 (1.48)
Public benefit:High Control	.56 (1.48)
Large access:High Control	-1.47 (1.47)
Public benefit:Large access:High Control	3.52 (2.08)•
Log-likelihood	-832.3031
DF	569

Note. $P< 0.001$, '***' ; $P< 0.01$, '**' ; $P<0.05$, '*'; $p<0.10$, '•'
Interactions of benefit, access, and control were included. Trust and privacy concern were control variables. Benefit, access, and control were coded with 0 or 1 and trust and privacy concern were coded from 1 to 7.

Table 7 shows the results from the Tobit regression. The regression included interaction effects among benefit (individual or public), information access by others (small or large access

by others), and the degree of risk control (low or high control) and along with the control effect of trust and privacy concern.

When participants were presented with individual benefit, small access of information (i.e. government only), and low control (i.e. information distributed without permission) then participants disclosed about 22 personal-information items in the registration form when he or she had no trust to the system and mean of privacy concern ($\beta = 22.38$, $SE = 1.42$, $p < .001$).

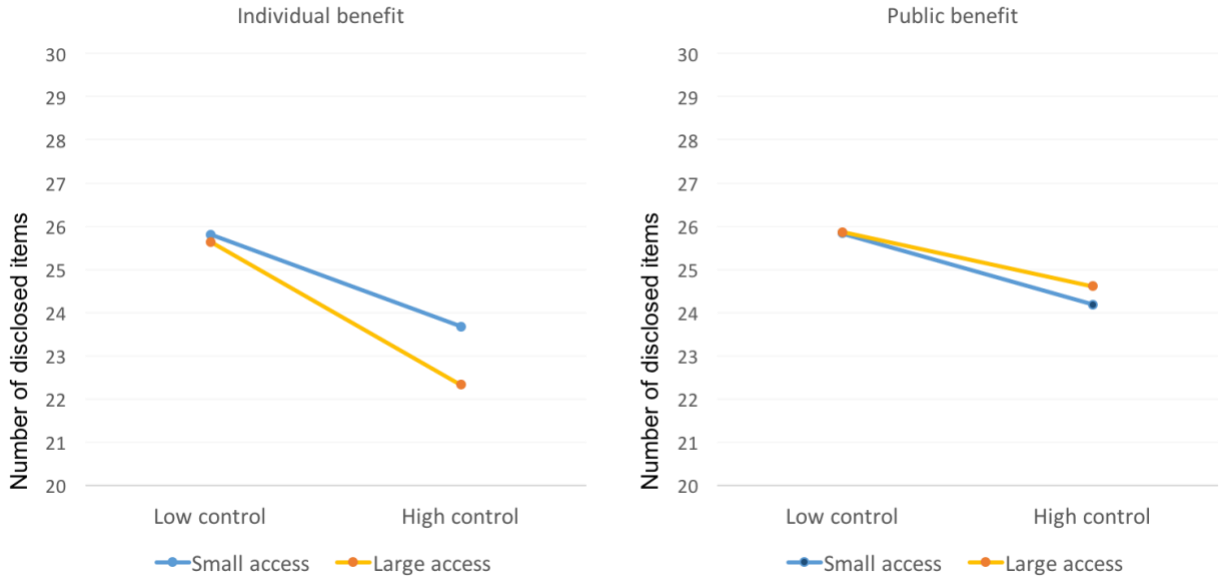
When participants had the information of individual benefit, small access of information (i.e. government only), and high control (i.e. permission required for information distribution) then participants disclosed 20 personal-information items with no trust and mean general concern ($\beta = -2.13$, $SE = 1.03$, $p < .05$). In other words, participants disclosed two fewer items when they encountered high control conditions compared to low control conditions when other factors were the same. Therefore, H3_1a was rejected as individuals with high control of their personal information did not disclose more information than individuals who had low control.

I expected that individuals disclosed more information when they had more control over their information distribution because more control would give less privacy risk. However, participants disclosed less information with more control. It would be because that the level of control of information distribution was not directly related to perceptions of privacy risk different from the relationship between trust and privacy risk. Lastly, access and benefit did not have statistically significant main effects on information disclosure. Therefore, H3_1b and H3_2 were rejected.

Further, it was hypothesized that the interaction effect between control and access would be different for the public benefit condition and the individual benefit condition (H3_3). Figure 6 shows the interaction among benefit, access, and control conditions. When individuals had high

control of information distribution (i.e. participants had permission of information distribution), they disclosed less personal information compared to participants who did not have permission of information distribution. Therefore, H3_3 was supported.

Figure 6 Interaction effect among risk and benefit on information disclosure



Note. Overall, participants disclosed less information when they had high control. When they had individual benefit, they disclosed less information with large access condition compared to small access condition. When they had public benefit, they disclosed less information with small access condition compared to large access condition.

Along with high control, in the condition indicating individual benefit (i.e. the participant would receive a direct benefit of providing personal information versus the public), participants disclosed more personal information when their information would be shared only with government agencies (i.e. small access) compared to information shared with the public (i.e. large access). Further, in the public-benefit condition, presented with large access disclosed more information compared to individuals who were in the small access condition when control was high (i.e. having permission before information distribution).

When the benefit was individual, participants disclosed less personal information with high privacy risk. However, the benefit affected public health, participants were willing to take

privacy risk more than individual benefit condition. It might be because that participants were more sensitive to privacy risk when it regarded only individual interests.

4.1.5 Sensitivity of question for information disclosure

A pre-test was conducted to determine the level of sensitivity of information-disclosure questions, which allowed an even sensitivity distribution among the items presented to participants. Information-disclosure questions were either of a yes/no format or required the participant to enter a text response. The types of questions were highly related to the sensitivity of questions. Questions that asked for a yes/no response were not as sensitive as questions requiring a text-based response. For example, questions that asked participants to provide their phone number or emergency contract information were considered more sensitive than yes/no questions because it required more effort to answer, which may affect the level of information disclosed.

A logit regression, which estimated the probability of answering personal information questions, was conducted to determine how likely a participant was to provide their information depending on the type and sensitivity of questions asked. First, I coded whether or not each individual answered each question: 0= yes or no type and 1=text response type. The sensitivity of each question was measured through the pre-test:1(low sensitive) though 5 (high sensitive) with a mean of 2.57. Table 8 summarizes Logistic regression for answering individual questions.

Table 8 Logistic regression for answering personal information

	coef (Std.)	Exp(coef)
Intercept	3.90 (.14)***	49.50
Format (fill out)	-1.79 (.08)**	.17
Sensitivity	-.38 (.04)***	.68
Model χ^2 = 1088.538***		
R^2 = .18		
N = 9780		

Note. *P*< 0.001, '***' ; *P*< 0.01, '**' ; *P*<0.05, '*'; p<0.10, '•'
Format was a dummy variable while sensitivity was a continuous variable. The dependent variable was the probability of answering questions in the registration form presented to participants on the Outbreak Alert System.

The log odds of answering a question changed by -0.79 when participants met a question asking for a text-based response versus a yes/no answer. In other words, the odds of answering yes/no type question increased by .17. The probability of answering questions decreased when they were asked to provide a text-based response. Additionally, for every one unit change in sensitivity, the log odds of answering a question decreased by -38. In other words, participants tended to provide their information when they were presented a yes/no question, and questions with lower sensitivity.

4.1.6 Summary of Study 1

Study 1 looked at the relationship between information disclosure and privacy concern, and the effect of risk and benefit on information disclosure. The results showed that there was the statistically negative relationship between information disclosure and privacy concern. Lower privacy concern related to more information disclosure. When individuals who had high trust to the system, they disclosed more information while trust to government agencies did not have any effect on information disclosure on the system. Among the benefit and risk factors, only high control condition had a statistically significant effect on the amount of information disclosure. When individuals had permission of information distribution before the system released

participants' personal information, they disclosed less personal information compared to low control condition which participants did not have permission to information distribution. It was interesting that individuals were more passive to disclose their information when they had high permission control. It would be possible that when individuals had more control to their information, they tended to be strict in deciding information disclosure. While considering higher trust was related to more information disclosure, giving more control was not directly related to the trust to the system. Also, considering lower privacy concern yielded more information disclosure, more control did not directly affect the level of privacy concern.

4.2 Study 2: Information Disclosure with Individual, Community, and Public Risk and Benefit

4.2.1 Sample distributions

I recruited a separate group of participants for study 2. The online experiment was open from Nov 14, 2016 to Nov 29, 2016. Two attention check questions were included in the experiment, and participants who answered these questions incorrectly were removed. A total of 937 participants finished the experiment but only 313 participants passed the manipulation check questions. The Study 2 experiment was consisted of ten manipulation conditions including one control group. The lowest number of participants in a condition was 29, the highest number was 34, and the average was 32. Female participants made up 54% of the participants and 77.3% were white.

Table 9 Demographics of Study 2 (N=313)

	N(%)
Gender	
Male	147(47)
Female	166(53)
Ethnicity	
White	242(77.3)
Black	32(10.2)
Hispanic	10(3.2)
American Indian	8(2.6)
Asian	17(5.4)
Others	4(1.3)
Age	
18-24 years old	35(11.2)
25-34 years old	69(22.0)
35-44 years old	54(17.3)
45-54 years old	59(18.8)
55-64 years old	53(16.9)
65 years or older	43(13.7)

Note. The data was collected through Qualtrics November 14 2016 through November 29 2016 with quotas from 2010 US Census. Due to the composition of the Qualtrics panels, individuals who were non-white and 65 years of older were under-represented. Therefore, the composition did not meet the quota.

4.2.2 Variables

Table 10 shows descriptive information of variables in Study 2. The variables used the same measurement as study 1. Mean values had a similar pattern with values from Study 1. The mean of privacy concern was 4.21 (SD=1.75). I also used two types of trust: Trust to the Outbreak Alert System and Trust to U.S. government agencies. The mean of trust to the system was 4.88 (SD=1.10), and trust to government agencies was 4.04 (SD=1.63).

Table 10 Descriptive of included variables (N=313)

	Reliability	Mean(SD)
Privacy concern (1 - 7) (Collection) - It bothered me when the Outbreak Health Portal website asked me for personal information. -When Outbreak Health Portal website asked me for personal information, I thought twice before providing it. -I was concerned that Outbreak Health Portal website was collecting too much personal information about me. (Secondary Usage) -I'm concerned that Outbreak Health Portal website would use the information for other reasons. -I'm concerned that Outbreak Health Portal website would sell my personal information in their computer databases to other organizations. -I'm concerned that Outbreak Health Portal website would share my personal information with other organizations without my authorization. (Improper Access) -I'm concerned that Outbreak Health Portal database that contains my personal information is not protected from unauthorized access. -I'm concerned that Outbreak Health Portal website does not devote enough time and effort to preventing unauthorized access to my personal information. -I'm concerned that Outbreak Health Portal website does not take enough steps to make sure that unauthorized people could not access my personal information in their database. (Control) -It bothers me that I do not have control of personal information that I provided to Outbreak Health Portal website. -It bothers me that I do not have control or autonomy over decisions about how my personal information was collected, used, and shared by Outbreak Health Portal website. -I'm concerned when control is lost or unwillingly reduced as a result of information sharing with Outbreak Health Portal website.	.977	4.21(1.75)
Trust to the OAS (1 - 7) -The Outbreak Health Portal is a trustworthy system. -I can count on the Outbreak Health Portal to protect my privacy. -The Outbreak Health Portal can be relied on to keep its promises.	.874	4.88(1.10)
Trust to the Governments (1 - 7) -I trust Government agencies. -I trust government agencies keep my best interests in mind.	.948	4.04(1.63)

Note. Measures of privacy concern and trust variables. Participants showed higher trust to the OAS than general U.S. government agencies.

4.2.3 The relationship between information disclosure and privacy concern

Study 2 shared RQ 1 and RQ 2 regarding the relationship between information disclosure and privacy concern as to see whether or not the relationship was consistent. As with Study 1, I conducted regressions for privacy concern with information disclosure and trust with data from Study 2. The two studies had different privacy risk and benefit and it would affect participants' privacy concern and trust differently. Study 1 looked at privacy risk regarding management of personal information such as permission to information distribution and boundary of information distribution. Study 2 looked at different targets of privacy risk and benefit: individual, local community and public.

Table 11 Regressions for privacy concern

	Model 1 B (SE)	Model 2 B (SE)
Intercept	4.22(.09)***	4.21(.08)***
Information disclosure (N of disclosed items)	-.13(.02)***	-.06(.02)**
Trust to the OAS system		-.78(.09)***
Trust to government		-.04(.06)
R^2	.34	.35
F	54.32***	54.32***

Note. $P < 0.001$, '***' ; $P < 0.01$, '**' ; $P<0.05$, '*'; $p<0.10$, '•'
Model 1 only included the number of information disclosure for privacy concern and model 2 added trust for privacy concern. Only trust to the system was statistically significant.

Table 11 presents summarized regressions for privacy concern. Information disclosure and trust variables were mean centered to make the interpretation of parameter estimates easier. As with Study 1, there was a negative relationship between information disclosure and privacy concern. In model 1, those who disclosed 26 items (mean) reported 4.22 points of privacy concern (β = 4.22, SE = .09, p < .001). When they disclosed one more item, their privacy concern decreased 0.13 points (β = -.13, SE = .02, p < .001). Two types of trust were included in model 2:

trust to the Outbreak Alert System and trust to the government in general. People who disclosed 26 personal information items and had the average level of trust to the Outbreak Alert System (M=4.88) and government agencies (M=4.01) reported 4.21 points of privacy concern (β = 4.21, *SE* = .02, $p < .001$).

Regarding RQ1 (What is the relationship between the amount of information disclosure and the level of privacy concern?), I hypothesized that individuals who disclosed more information had less privacy concern when other factors were controlled (H1). Results indicate that as people disclosed one more personal item, their privacy concern decreased .13 point (β = -.13, *SE* = .02, $p < .001$), which lends evidence that privacy concern decreased as the number of disclosed items increased. This result is the same as indicated in Study 1.

Regarding RQ2 (What is the effect of trust on information disclosure and privacy concerns?), I hypothesized that individuals who had higher trust in the Outbreak Alert System would report lower privacy concern when they disclosed the same amount of information (H2_2). Results indicate that for every one unit increase in trust to the Outbreak Alert System, the predicted value for privacy concern decreased by -0.78 points (β = -.78, *SE* = .09, $p < .001$) when information disclosure and trust to Government were held as mean. Therefore, H2_2 was supported. Trust to Government was not statistically significant on privacy concern when they disclose the same amount of information. Therefore, H2_1 was not supported. The relationship between information disclosure and privacy concern was consistent throughout Study 1 and Study 2. The negative relationship between information disclosure and privacy concern was consistent in different privacy risk conditions and the effect of trust on the relationship was also consistent.

4.2.4 Interaction effects of benefit and risk

The main goal of Study 2 was to know the effect of individual, local community, and public risks and benefits on information disclosure. Individual benefit indicated the participant would get direct help from the OAS in an emergency, and individual risk manipulated a situation when the participant would be infected, his or her information could be shared with others. Local community benefit implied that the participant's local community would directly benefit from the OAS in an emergency situation, and local community risk condition explained that if someone in the local community would be infected the patient's personal information could be shared with anyone in the community. Public benefit indicated that the public would directly benefit from the OAS, and public risk implied that if anyone is infected the patient's information could be shared with anyone.

Study 2 performed a 3 by 3 factorial design experiment. Each level of (individual, local community, or public) benefit and risk manipulated different boundaries of privacy risk and benefits from information disclosure. Individuals may have different perceptions on the boundary of their local communities, and the perception may affect their understanding for significance on benefit and risk. At the end of the experiment for the effect of individual, local community, or public privacy risk and benefit, participants answered to question, "*The word 'local community' means different things to different people. When we use the word community to indicate a sense of place of your local community, what the word community mean to you? (1) My neighborhood (2) The city I live in (3) The county I live in (4) The state I live in (5) The country I live in.*" 112 participants indicated local community meant "*my neighborhood*", and 128 participants indicated it was, "*the city I live in*". To make the categories simple, I combined option 3, "*the county I live in*" (N=55) and option 4, "*the state I live in*" (N=15). No participant

responded, "*the country I live in*". In summary, responses indicated three categories in the order of the boundary of community beginning with neighborhood, then city, and then county/city.

To answer RQ4 (How does the amount of information disclosure change when participants encounter different levels of risks and benefits at the individual, community, and public levels?), specifically, how do individuals' perception on local community affect their perception of their information uses, I included the interaction effects among benefit, risk and the boundary of local community. Table 12 shows Tobit regressions for information disclosure with the three levels of benefits and risks with the meaning of local community to individual participants.

Table 12 Tobit regression for information disclosure

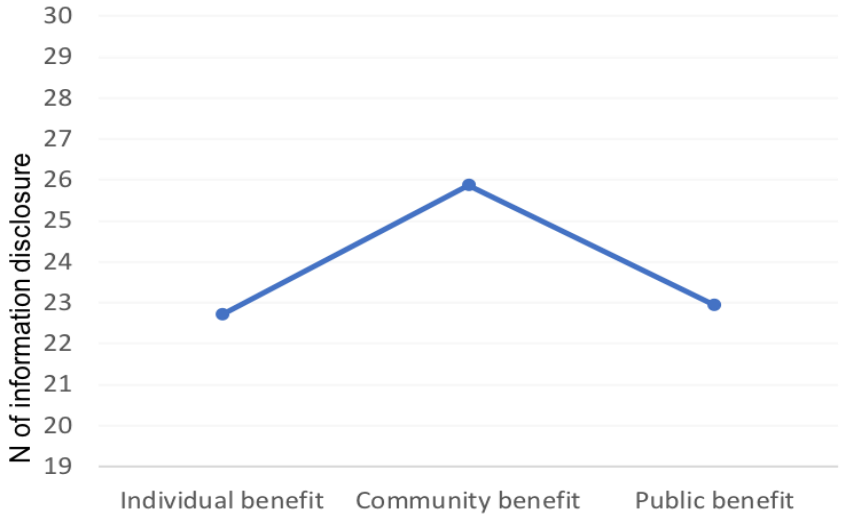
	B (SE)
Intercept	22.72 (2.04)***
Benefit:	
Individual (0)	
Community (1)	3.16 (1.76)•
Public (2)	.23 (1.61)
Risk	
Individual (0)	
Community (1)	3.66 (1.57)*
Public (2)	1.71 (1.47)
Community	
Neighborhood (0)	
City (1)	3.32 (1.48)*
County+State (2)	3.61 (1.85)•
Trust to the OAS	.63 (0.26)*
Privacy concern	-.47 (0.17)**
Community benefit:Community risk	-4.11 (2.33)•
Public benefit:Community risk	-1.66 (2.33)
Community benefit:Public risk	-1.25 (2.28)
Public benefit:Public risk	-2.40 (2.18)
Community benefit:City	-3.77 (2.21)•
Public benefit:City	-2.83 (2.19)
Community benefit:County+State	-4.78 (2.85)•
Public benefit: County+State	-5.21 (2.59)*
Community risk:City	-4.65 (2.18)*
Public risk:City	-1.60 (2.13)
Community risk: County+State	-5.20 (2.56)*
Public risk: County+State	-1.87 (2.61)
Community benefit: Community risk: City	6.09 (3.19)•
Public benefit: Community risk: City	3.08 (3.13)
Community benefit: Public risk: City	1.70 (3.09)
Public benefit: Public risk: City	3.82 (3.08)
Community benefit: Community risk: County+State	5.55 (3.72)
Public benefit:Community risk: County+State	7.70 (3.75)*
Community benefit:Public risk: County+State	.62 (3.75)
Public benefit:Public risk: County+State	5.66 (3.66)
Log-likelihood	-773.02
DF	552

Note. $P< 0.001$, '***' ; $P< 0.01$, '**' ; $P<0.05$, '*'; $p<0.10$, '•'

The regression included three conditions each of benefit, risk and the boundary of local community. The model included interaction factors among the three variables along with trust and privacy concern as control variable.

First, there was the main effect of benefit. Figure 7 shows the differences between individual benefit, community benefit, and public benefit when other categories were hold as baseline (individual risk and neighborhood). Participants disclosed 3.16 more personal information when they had community benefit compared to individual benefit ($\beta = 3.16$, $SE = 1.61$, $p < .10$). They were willing to disclose more information when more people would get benefit from their information disclosure. With the public benefit, participants disclosed 0.23 more personal information compared to individual benefit, but the increase was not statistically significant. It showed that individuals were altruistic when their behaviors could help more people but it was helpful to specify the boundary of others rather than pointing to the general public.

Figure 7 The main effect of benefit

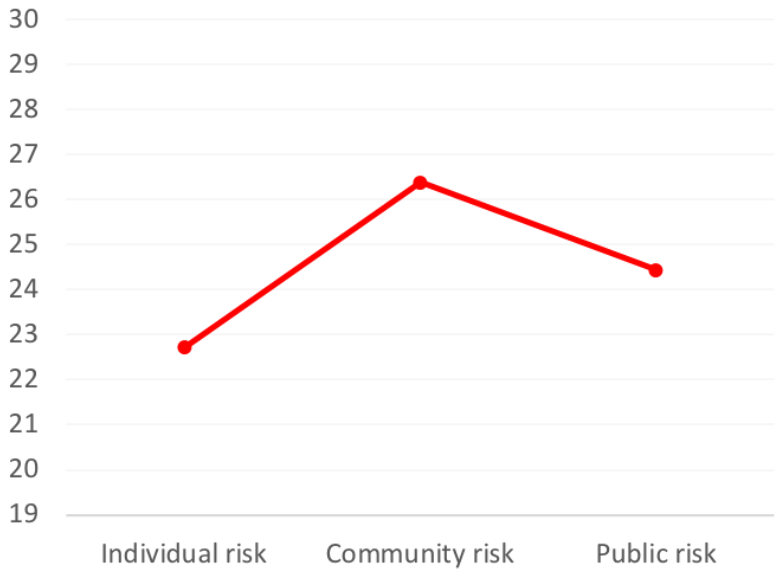


Note. The baseline categories were individual benefit, individual risk, and Neighborhood.

Regarding the risk effect, when participants encountered the community risk condition, they disclosed 3.66 more items compared to participants in the individual risk condition when the benefit was hold as individual level ($\beta = 3.66$, $SE = 1.57$, $p < 0.05$). In other words, participants were reluctant to disclose personal information when they had individual privacy

risk even though community risk could affect more people. Participants who had public risk condition disclosed 1.71 more personal information compared to participants who had individual risk, but the difference was not statistically significant.

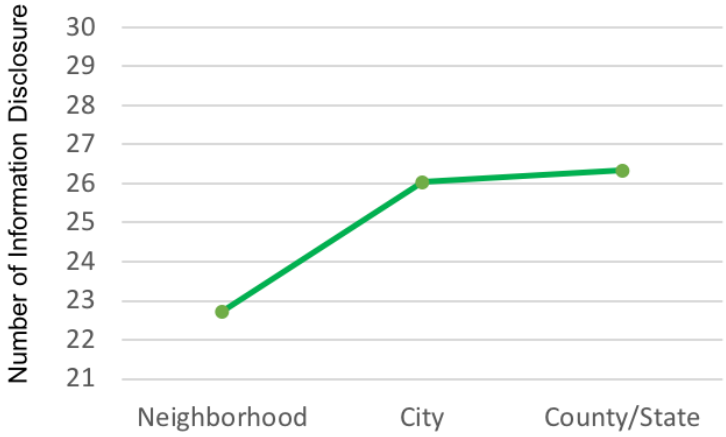
Figure 8 The main effect of risk on information disclosure



Note. The baseline categories were individual risk, individual benefit, and Neighborhood.

Figure 9 shows the main effect of the perception on local community. Regarding the boundary of local community, participants who defined local community as the city that they live in disclosed more personal information comparted to participants who defined local community as neighborhood ($\beta = 3.32$, $SE = 1.48$, $p < 0.05$). Similarly, participants who defined local community as the county or state they lived in disclosed more information than participants who defined local community as their neighborhood ($\beta = 3.61$, $SE = 1.85$, $p < 0.10$). Participants who understood local community with broader boundary disclosed more personal information when they had individual benefit and risk.

Figure 9 The main effect of the perception on local community

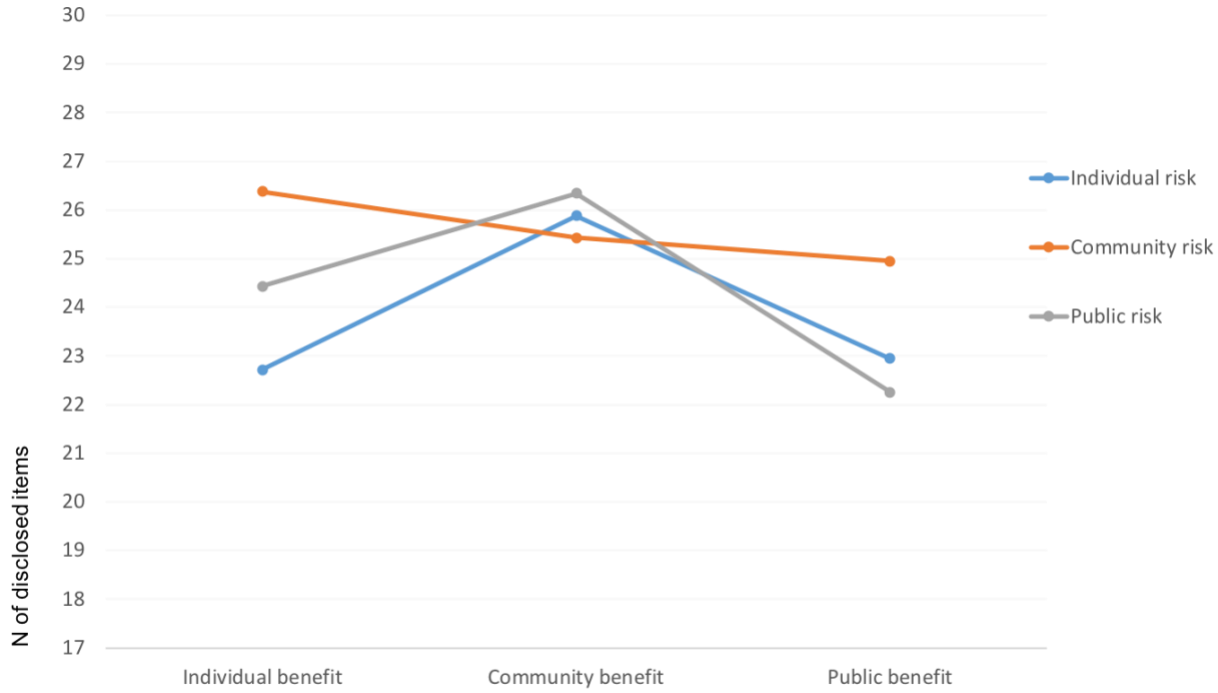


Note. The amount of information disclosure of participants who defined local community differently. Neighborhood was the baseline category along with individual benefit and individual risk.

Trust had a statistically positive effect on information disclosure. For every one unit increase in trust, the predicted value for information disclosure increased by .63 (β = .63, *SE* = 0.26, $p < 0.05$). Privacy concern had a statistically negative effect on information disclosure. For every one unit increase in privacy concern, the predicted value for information disclosure decreased by .47 (β = -.47, *SE* = 0.17, $p < 0.01$).

Figure 10 shows the interaction effect of benefit and risk when trust and privacy concern were held as zero and community was defined as neighborhood, and Table 11 shows values from the interactions. Overall, participants tended to disclose more information with community benefit compared to individual benefit when risk was hold as individual and public level. When comparing condition 1 and condition 2 in Table 11, participants disclosed more personal information when they themselves would get direct benefit from the system but privacy risk was related to local community (β = 3.66, *SE* = 1.57, $p < 0.01$), compared to others who would get direct benefit but risk was related to themselves.

Figure 10 The interaction effect of benefit and risk



Note. The effect of risk and benefit on information disclosure at different levels when the definition of local community was neighborhood. Community risk and individual benefit was highest and public benefit and public risk was lowest value.

Similarly, comparing condition 1 and condition 4 in Table 13, when their information disclosure would help their local community, they were willing to disclose more personal information than when it was only related to individual benefit in spite of taking their own privacy risk ($\beta = 3.16$, $SE = 1.76$, $p < 0.10$). It showed that when participants were presented with a decision of comparing individual and community benefit, they tended to take more seriously community benefit rather than individual benefit.

Table 13 The average number of information disclosure in each condition when the perception on local community is neighborhood.

1.Individual Benefit & Individual Risk	2. Individual Benefit & Community Risk	3. Individual Benefit & Public Risk
22.72	26.38	24.43
4. Community Benefit & Individual Risk	5. Community Benefit & Community Risk	6. Community Benefit & Public Risk
25.88	25.43	26.34
7. Public Benefit & Individual Risk	8. Public Benefit & Community Risk	9. Public Benefit & Public Risk
22.95	24.95	22.26

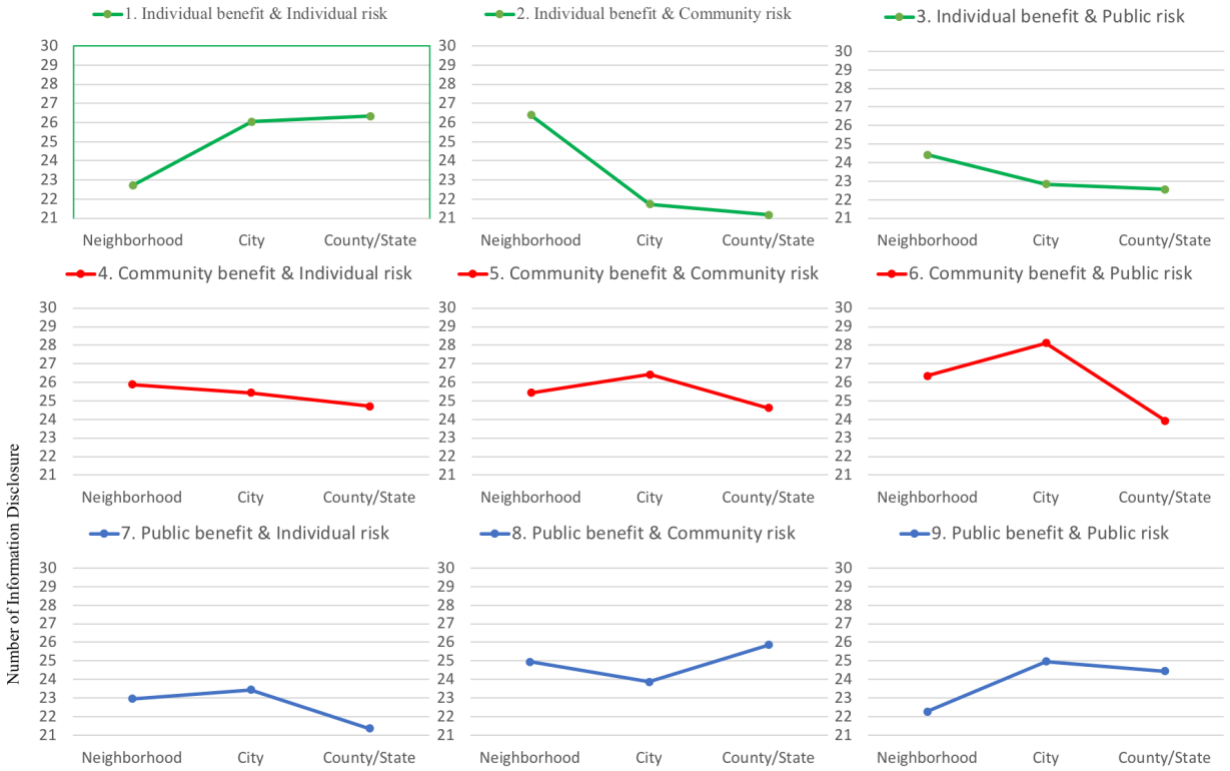
Note. The number of information disclosure in each condition. The numbers indicate each condition. The perception on local community was hold as neighborhood.

Figure 11 shows interactions among benefit, risk and perception on local community, and Table 14 shows corresponding values from each graph from Figure 11. Earlier, I observed that participants disclosed more personal information when they had direct benefits from the system while privacy risk was related to their local community compared to privacy risk was limited to individual. It varied depending on participants' perception on local community (graph no.2 in Figure 11). Among the group of participants who encountered individual benefit and community risk, participants who defined community as city or county/state disclosed less personal information compared to participants who defined local community as their neighborhood. When participants understood local community within a broader boundary, they would take privacy risk for the local community more seriously.

Comparing graph 4, 5, and 6 in Figure 11, participants who defined local community as county/state disclosed less personal information compared to participants who defined local

community as neighborhood regardless of risk condition. When participants considered local community benefit, the community benefit was more important to participants who defined local community as their neighborhood rather than people who had broader perception on local community.

Figure 11 Interaction effect of benefit and risk with different concept of local community



Note. Each graph shows information disclosure in each condition. For example, graph 1 indicate that among participants who entered the individual benefit and individual risk condition, and the comparison between participants who defined local community as neighborhood versus city or county/state. Neighborhood is the baseline in all graphs.

Table 14 Numbers of information disclosures in each condition with different perceptions on local community

1.Individual Benefit & Individual Risk			2. Individual Benefit & Community Risk			3. Individual Benefit & Public Risk		
Neighborhood	City	County/State	Neighborhood	City	County/State	Neighborhood	City	County/State
22.72	26.04	26.33	26.38	21.73	21.18	24.43	22.83	22.56
4. Community Benefit & Individual Risk			5. Community Benefit & Community Risk			6. Community Benefit & Public Risk		
Neighborhood	City	County/State	Neighborhood	City	County/State	Neighborhood	City	County/State
25.88	25.43	24.71	25.43	26.42	24.61	26.34	28.11	23.92
7. Public Benefit & Individual Risk			8. Public Benefit & Community Risk			9. Public Benefit & Public Risk		
Neighborhood	City	County/State	Neighborhood	City	County/State	Neighborhood	City	County/State
22.95	23.44	21.35	24.95	23.87	25.85	22.26	24.97	24.45

Note. No.1 – No.10 indicate each privacy policy condition. Neighborhood, city, and county/state imply participants' perceptions on the boundary of local community. Numbers are the average of disclosed personal information in each condition.

4.2.5 Summary of the results from Study 2

In comparison to Study 1, Study 2 focused more on the social versus individual boundaries of privacy risk and benefit regarding decision of information disclosure. Study 2 examined how individuals' privacy decision changed when they had individual, community, or public benefit and risk in a situation that described a future outbreak, which was related to RQ4 (*How does the amount of information disclosure change when participants encounter different levels of risks and benefits at the individual, local community, and public level? In this process, how does individuals' perception on local community affect their information disclosure?).*

Regarding privacy risk, individuals tended to disclose less information when they had individual-level risk compared to community or public risk. For example, when participants read privacy policy which stated, "If you are infected, your personal information can be shared with

others in outbreak situations. Others are able to see who you are and where you live," they disclosed less information comparted to participants who read, "If someone in your local community is infected, the infected people's personal information can be shared with your local community in outbreak situations. Your local community is able to check who the infected people are and where they live." It showed that individuals were more sensitive with individual privacy risk regarding information disclosure.

Regarding benefit from information disclosure, individuals who were informed of community benefit (i.e. "Your community will gain direct, certified alerts and information from the HHS when outbreaks occur. If your neighbors are in a high-risk group for exposure then HHS will contact your neighbors directly and monitor their symptoms"), disclosed more information compared to individuals who were informed of individual benefit (i.e. "You will gain direct, certified alerts and information from the HHS when outbreaks occur. If you are in a high-risk group for exposure then HHS will contact you directly and monitor your symptoms.").

It was interesting to know that individuals were more altruistic when they considered benefits from information disclosure but they were less altruistic when they considered privacy risk from information disclosure. When I looked at interactions among benefit, risk and definition of local community, this tendency varied depending on the participants' definition of local community. For example, among participants who had individual benefit and community risk, participants who defined local community as neighborhood disclosed more information than participants who defined community as city or county/state. Also, participants were not sensitive to community risk as much as individual privacy risk but for those who considered local community as city or county took more seriously community risk than others who defined local community as neighborhood.

4.3 Summary of the Results

The high-level goal of this dissertation was to better understand how different dimensions of privacy risks and benefits change individuals' decisions regarding information disclosure, as well as their privacy concerns after the disclosures. I designed two experimental studies to manipulate different characteristics of risk and benefit which could affect privacy decisions. Additionally, I looked at the relationship among trust, privacy concern and information disclosure.

4.3.1 The relationship between information disclosure and privacy concern

In both Study 1 and Study 2, there was a statistically-significant negative relationship between information disclosure and privacy concern. Individuals who disclosed more information reported less privacy concern. Individuals who reported low privacy concern also indicated more willingness to disclose personal information. Overall, the privacy paradox, which suggests that individuals disclose much personal information even when they have high-privacy concern, was not observed in the results of this research. Information disclosure was first measured using the registration form in the Outbreak Alert System then participants were later asked about their privacy concern regarding the information disclosure. The sequence of the experiment could not support a causal relationship between the two variables, but it was effective to limit privacy concern to the specific disclosure behavior.

I measured two types of privacy concern: privacy concern to the system and general privacy concern regarding Internet usage. Participants reported lower privacy concern to the system than their general Internet privacy concern, For example, In study 1, the average of privacy concern to the system was 4.48 and general privacy concern was 5.12. Statistically, both privacy concern variables affected information disclosure.

4.3.2 The effect of trust on information disclosure and privacy concern

There was a strong relationship between privacy concern and trust to the OAS. When individuals had high trust to the system, they reported lower privacy concern to the system. Trust and privacy concern to the system affected information disclosure individually but when they were included in one model, one variable neutralized the other variable. In Study1, privacy concern to the system did not have any effect on information disclosure while the trust variable was statistically significant in the same model. However, general privacy concern had a negative effect on information disclosure in the same model. General privacy concern might not be related to trust to the system. It inferred that there was a negative relationship between and privacy concern trust to the system, and it was related to information disclosure on the website. It shows that when we discuss the relationship between information disclosure and privacy concern, we should pay attention to how trust is related to the relationship.

4.3.3 Study 1: Control and access effect with individual or public benefit

Study 1 examined the effect of control over information distribution (i.e. permission before information release or no permission), boundary of access (i.e. public would access personal information in emergency or only government would access the information), benefit (i.e. the participant would get direct benefit or public would get benefit from the system) on information disclosure.

The permission on information release made a significant difference on the amount of information disclosure. When participants had high control (i.e. having permission) over their information release, they disclosed less information compared to those who had low control over their information release. It would be because that the high control did not decrease perceived privacy risk. The individual and public benefit did not have main effects on information

disclosure, but there was an interaction effect with privacy risk. Participants disclosed less information with high control and it decreased more when they had individual benefit compared to public benefit.

4.3.4 Study 2: Individual, local community, and public risks and benefits

Study 2 mainly focused on the social versus individual boundaries of privacy risks and benefits to answer the research question (RQ 4): How does the amount of information disclosure change when participants encounter different levels of risks and benefits at the individual, community, and public levels? In this process, how does individuals' perception on local community affect their information?

Participants were more sensitive to their personal privacy risk than their own benefit from information disclosure when they had individual privacy risk and individual-health benefit. However, when their information disclosures were related to community-health benefit, there were more likely to disclose personal information compared to a situation where their information disclosures were only related to individual-privacy risk.

In contrast, when their information disclosures were related to community-privacy risk while they had individual health benefit, they were more willing to disclose personal information. However, this tendency varied depending on participants' perceptions on local community. Participants who considered local community as neighborhood disclosed more information than participants who considered local community as city or county while they had the same information regarding community privacy risk. When individuals had a broader boundary of who was included in the local community, they were more sensitive to the effect of privacy risk on the local community.

5 DISCUSSION

I introduced the outbreak context in the experiments because health emergency tended to reveal situations where individual interests conflicted with public interests. In the MERS and Ebola outbreaks, people made different decisions regarding their health for various reasons. Those who were not infected and did not need to report their personal information insisted that public-health safety was more important than individual privacy. Some infected patients reported their symptoms and information to get the benefits of symptom treatments, or to prevent further outbreak. But some did not report their symptoms because of concerns about social blame for contagion. Thus, the outbreak context showed the different dimensions of the situations individuals could encounter.

I wanted to learn what value was more important to individuals, and in what situations they were more willing to provide their information when facing different benefits and risks in terms of information disclosure. First, trust and privacy concern to the system were very important factors for individuals to decide the amount of information disclosure. There was a negative relationship between trust and privacy concern and the relationship effected information disclosure.

Second, having permission on information distribution was a negative effect on information disclosure. It was interesting because individuals were willing to disclose less information when they had high control over their information distribution. It would be because high control over information release was not related to trust or privacy concern, both of which had statistically significant effects on information disclosure. Also, individuals might have more responsibility on their privacy when they had more options to control their personal information. Individuals have fears about privacy risk, and when they have control over their personal

information, they are more apprehensive to disclose their personal information.

Third, individuals were more responsive to privacy risk rather than benefit from information disclosure when it was directly related to themselves. When privacy risk was not directly related to them, they tended to disclose more information. However, regarding benefit from information disclosure, they were willing to disclose more information when their behaviors implied a benefit for more people even they had privacy risk.

5.1 Privacy Paradox Exists?

The privacy paradox is a principle issue among privacy literatures. Researchers have argued of the prevalence of the privacy paradox, however, there are empirical shortcomings among privacy paradox studies. For example, studies focusing on Facebook measured information disclosure with the amount of information present on a user's profile, and measured privacy concern of general Facebook use. It is also important to measure privacy concern regarding specific information disclosure behavior, in which the experiments presented in this dissertation were designed to set a controlled environment to measure the relationship between information disclosure and privacy concern. Specifically, I used a new website that participants did not have previous experience with. Information disclosure was first measured during the sign-up process, and privacy concern was also measured for the information disclosure that participants had during the sign-up process.

The results showed a negative relationship between information disclosure and privacy concern. Individuals who disclosed more information reported less privacy concern, which did not support the privacy paradox. Based on the result, I concluded that individuals did not make paradoxical decision.

5.2 Low Psychological Barrier of Information Disclosure

I understand that individuals made their privacy decisions rationally based on the context they were presented, but one thing I was surprised by was throughout the experiments participants were highly likely to disclose their personal information. The mean values of information disclosure in both Study 1 and Study 2 were 24 and 26, respectively, out of 30 questions each. This was a higher value than I expected considering I included questions from different sensitivity levels from the pre-test.

The high-value of information disclosure can be explained by a few reasons. First, participants trust to the system was high enough to offset their privacy concern. While trust may explain high-information disclosure, the measures of the studies were not designed to explain why individuals had such low barriers to providing their personal information. Second, it is possible that the questions included in these experiments were not sensitive enough to discourage information disclosures. I included questions with different levels of sensitivity, which were determined by the pre-test, but participants answered most questions aside from a few highly sensitive questions, such as phone number or emergency contact information. Although, they were free not to respond to all questions, they provided a large amount of their identifiable information in the registration form. Third, it is also possible that the health benefit was critical to them because a virus outbreak has potential to directly relate to one's health. Another possibility I am considering is that participants disclosed a large amount of information because they are accustomed to doing so with online services. With the perception that privacy is a tradeoff, online service providers such as Google and Amazon want to pay less for users' information and the users want to get paid more for the information they provide. However, users disclose their information with a small reward because they have only two options: give all

and use the service or give nothing and do not use the service. This unbalanced structure makes online users value their personal information less and it may yield a privacy paradox in some situations.

5.3 "Control Paradox" Exists?

One of the contributions of this research was understanding the relationship between the degree of control and the amount of information disclosure. Study 1 looked at the effect of low versus high control over shared information on the degree of information disclosure. In this study, when individuals had high control over their information they disclosed less personal information. More control lead to more privacy. However, Brandimarte, Acquisti, and Loewenstein (2013) argued the opposite. In their study, when people had more control they disclosed more information. They named the behavior as the "control paradox" because more control lead to less privacy (more information disclosure) in their experiments.

Then, why are there inconsistent explanations from different studies? One possibility is when individuals have more control over their personal information, they have more responsibility for their privacy and may be more careful to share their information. Microsoft had received complaints from users regarding privacy policies because there was not enough transparency about how Windows collected and passed users' information to third parties. Recently, Microsoft launched Windows 10 and it gave users more control over their personal information.[1] Now, users can turn on or off privacy setting based on their needs. In this case, users can provide less personal information with more control. Social media like Facebook has also provided more control to their users. Initially, the Facebook profile was quite simple, but now it contains lots of functions that allow users to subcategorize their audiences and set

[1] https://www.digitaltrends.com/computing/microsoft-announces-changes-to-windows-10-privacy-policies/

different options for different audiences. With more control, users' can determine which group can access more personal information while other groups are censored from that information or provided different kinds of information. In this regard, people may be willing to provide more information with more control when the situation reduces uncertainty of information distribution. Further, people may provide less information with more control when the information is sensitive and the boundary of who receives the information is not clear.

In the studies reported here, although participants had permission before their information release, it did not decrease the uncertainty of information distribution. With or without the permission, participants had the same information regarding how their information would be used by the system. Having permission would give more responsibility to the participants and they were less willing to disclose their information with more control. When high control helps to reduce the uncertainty of information uses it would be helpful to increase information disclosure but when it gives just authority to decision on information distribution, individuals would be conservative to disclose their information.

5.4 Trust and Privacy Concern

Across Study 1 and Study 2, the effect of trust was clear. Trust to the Outbreak Alert System had a statistically significant positive effect on information disclosure. One interesting point was that participants distinguished trust to the system and general trust to U.S. government agencies although it was their first time visiting the Outbreak Alert System. I measured two types of trust; trust to the system and trust to governmental agencies. On average, participants reported their trust to the system higher than their trust to government agencies, and only trust to the system had a significant effect on information disclosure within the system. It was quite surprising that participants built trust to the system in a short time. Although participants never

experienced the system before, they built their trust to the system based on the information they learned from the system.

I used the privacy concern measure which included four sub-dimensions. Conceptually, the four dimensions had meaningful differences but there was no statistical difference among the four sub-dimensions in these studies. It would be because that privacy concern was an integrated concept to individuals including all the risk from information disclosure and they might not distinguish concern from different risk factors. Also, the experimental condition did not give enough information regarding sub-dimension of privacy concern. Another reason would be the placement of questions. I arranged the twelve items for privacy concern together in one page. Participants might not consider carefully different wordings from the sub-dimensions and treated as the same information.

5.5 Dynamics of Individual and Social Interests

In Study 1, it was not a statistically significant change but individuals tended to disclose more personal information when they thought their behavior would be helpful to public health than when it was only related to individual health benefit. Study 2 also showed that participants disclosed more information when their disclosures were related to a local community health benefit rather than an individual health benefit. Individuals were altruistic when they thought about benefits from their information disclosure as affecting others. However, when privacy risk mattered to themselves, they were more reluctant to disclose personal information compared to when privacy risk affected their local community.

When individuals do not have the same amount of information regarding benefit and privacy risk from their information disclosure, one of the factors could affect more their decisions. If there were the same level of information about risk and benefit, other factors would

affect information disclosure. In this study, I looked at participants' perception on local community because people would define differently what local community was. The result showed that participants who had broader boundary of what local community was considered more privacy risk of local community and disclosed less personal information in spite of getting individual health benefit.

It was interesting to see this interaction between individual and social level interests. It would useful to use social level benefits or risk such as community and public to encourage individuals to disclose more personal information. But, from individual's stand point, it is important to ask information about privacy risk as much as benefit from information disclosure to make a better decision.

5.6 Practical Implications

Public health agencies increasingly require individually identifiable health information to perform public health services and functions. This includes collecting information to quell outbreaks and terrorism, and public health services (Myers, Frieden, Bherwani, & Henning, 2008). On the health agencies' standpoint, it is important to collect more personal information from individual. This study suggests that when the health agencies collect personal information from individuals, it is more useful to emphasize local community benefit instead of individual benefit. Also, it is very important to increase users trust to the health agencies because trust is one of the most important factors that decreases privacy concern and increases the amount of information disclosure.

However, there is a privacy warning in sharing health information about patients across health organizations. Although many individuals are likely to provide their personal information in exchange for some benefits, the level of anxiety is increasing when the disclosure includes

especially sensitive information (Madden, 2015). Particularly, health information includes sensitive contents, such as identified information, medical records, treatments, and/or history of family health (Bansal et al., 2010; Santos, Pedrosa, Costa, & Oliveira, 2010). On the users' standpoints, it is important to understand privacy risk yielded by their information disclosure. The study suggests organizations which fight for privacy protection that it is more effective to give users warning for individual privacy risk rather than public privacy risk in general if they want to alarm users not to provide personal information just for a small reward.

5.7 Future Direction

The goal of this dissertation was not to say one decision should be better than the other, rather, it was to better understand the dynamics of privacy decisions. This dissertation contributes to the privacy discussion by demonstrating: 1) the strong negative relationship between trust and privacy concern; 2) the consistent positive relationship between trust and information disclosure; 3) the negative relationship between privacy concern and information disclosure; 4) the negative relationship between having permission over information distribution (high control) and information disclosure; 5) that individuals are more sensitive to privacy risk than benefit when they had the same level of risk and benefit information; 6) the individual's altruistic attitude on his or her information disclosure regarding social benefit; 7) the perception on boundary of local community can affect information disclosure when the benefit and risk was related to the community.

Regarding no 4, it was interesting to see that individuals disclosed less information with high control. I interpreted high control as giving individuals more responsibility for their privacy, and that they could reduce their privacy risk by disclosing less personal information. Although they had control over information distribution it was not helpful at reducing uncertainty of

information use after its distribution. I want to continue to study the effect of control on information with comparing different settings of controls such as different levels of uncertainty of information use after information distribution and different levels of control over information distribution. For example, I can give participants authority to select the audience of their information to reduce uncertainty of information distribution or I can give them control for selecting the types of information which need their permission for distribution.

We have social issues related to privacy such as health outbreak and criminal information gathering. It would be useful to know attitudes on social or individual interests regarding privacy risk because it gives us an idea regarding how to encourage individuals to participate in the social issues. In these studies, individuals were more cooperative to provide their personal information when their information would be helpful to community health security. When we have a situation such as an outbreak, it would be helpful to emphasize community-health security to encourage individuals to cooperate with Government action for patient tracking. The dynamics of individual and social interests would work in different fields as well such as reducing criminal and increasing education quality. I'd like to explore this dynamics in different fields as well.

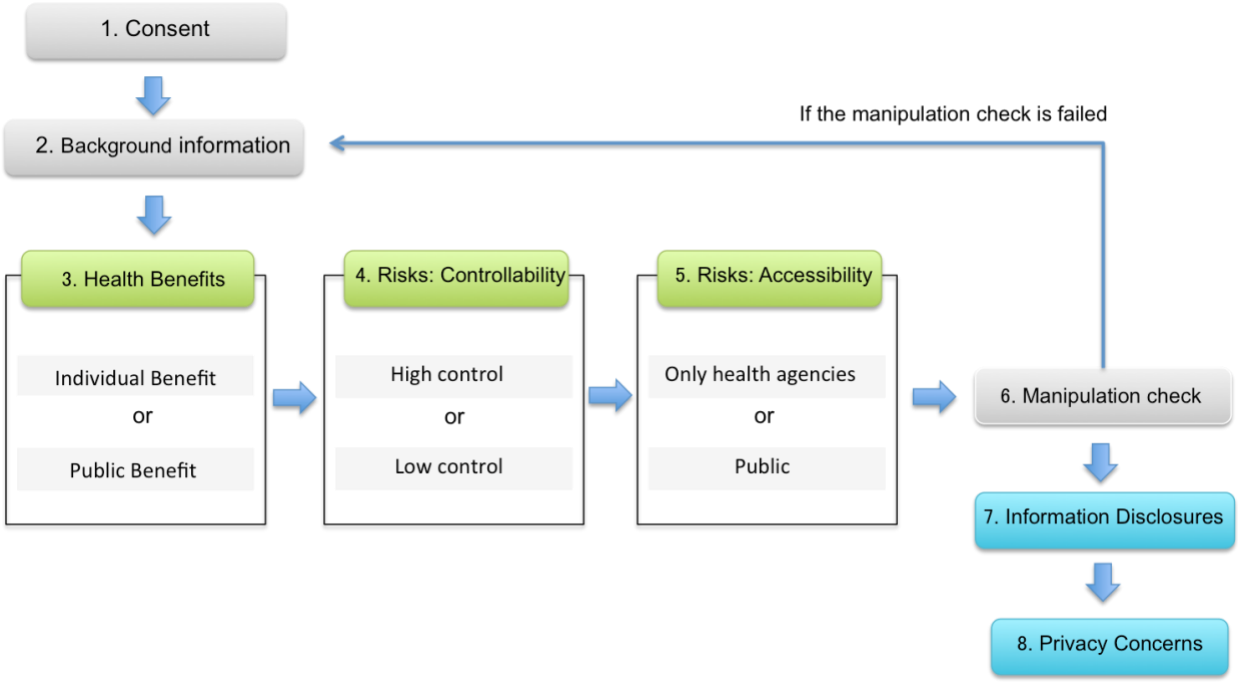
APPENDICES

APPENDIX A

Experiment Manipulations

A. Study 1 process

Figure 12 Study 1 process



1. Consent

2. Background information

The Zika virus is currently affecting to parts of the world including the U.S. Zika is transmitted through sexual intercourse as well as bites from infected mosquitos. And this type of viral outbreak is becoming more common. For example, last year, the Ebola virus killed nearly 7,500 people in West Africa. This epidemic was not contained to the African continent, but found its way to the U.S. as well. Similarly, MERS virus has killed more than 400 people in Saudi Arabia and traveled to South Korea and infected 172 people. These instances demonstrate we are all at risk when viruses get out of hand, and outbreaks can happen anytime and anyplace. One of ways to decrease risk is for governments to share information about growing epidemics. Therefore, it is critical for governments to establish an efficient disease-control system to deal with viral outbreaks.

3. Health benefits

a. Individual benefit:
The Department of Health and Human Services (HHS) and Michigan State University have developed a new health recording system, "Outbreak Health Portal," to deal with viral outbreaks that have no current cure, like Zika and Ebola. For this system to have the most benefit, it is important that people sign up and share their information. We need your participation to build up the system. By signing up:

> You will gain direct, certified alerts and information from the HHS when outbreaks occur. If you are in a high-risk group for exposure then HHS will contact you directly and monitor your symptoms.

b. Public benefit:
The Department of Health and Human Services (HHS) and Michigan State University have developed a new health recording system, "Outbreak Health Portal," to deal with viral outbreaks that have no current cure, like Zika and Ebola. For this system to have the most benefit, it is important that people sign up and share their information. We need your participation to build up the system. By signing up:

> The public will gain direct, certified alerts and information from the HHS when outbreaks occur. If anyone is in a high-risk group for exposure, HHS will provide them directly and monitor their symptoms.

4. Risk: control

a. High control:
Here is how your health record will be used:
If you are in a high-risk group for exposure, we may release your information to control disease with your permission.

b. Low control:
Here is how your health record will be used:
If you are in a high-risk group for exposure, we may release your information to control disease without your permission.

5. Risk: access

a. Small access:
We share your personal information with only governmental health agencies in outbreak situations.

b. Large access:
We share your personal information with not only health agencies but also with public in outbreak situations.

6. Manipulation check

Please choose True or False (A participant will be asked to the three of the following items depending on their assigned conditions)

You will gain direct, certified alerts and information from the HHS when outbreaks occur.
- True
- False
- I don't remember

Anyone will gain direct, certified alerts and information from the HHS when outbreaks occur.
- True
- False
- I don't remember

My information can be released without my permission.
- True
- False
- I don't remember

My information can be released with my permission.
- True
- False
- I don't remember

My information can be shared with not only health agencies but also with public.
- True
- False
- I don't remember

My information can be shared with only health agencies.
- True
- False
- I don't remember

7. Sign-up questions (information disclosure)

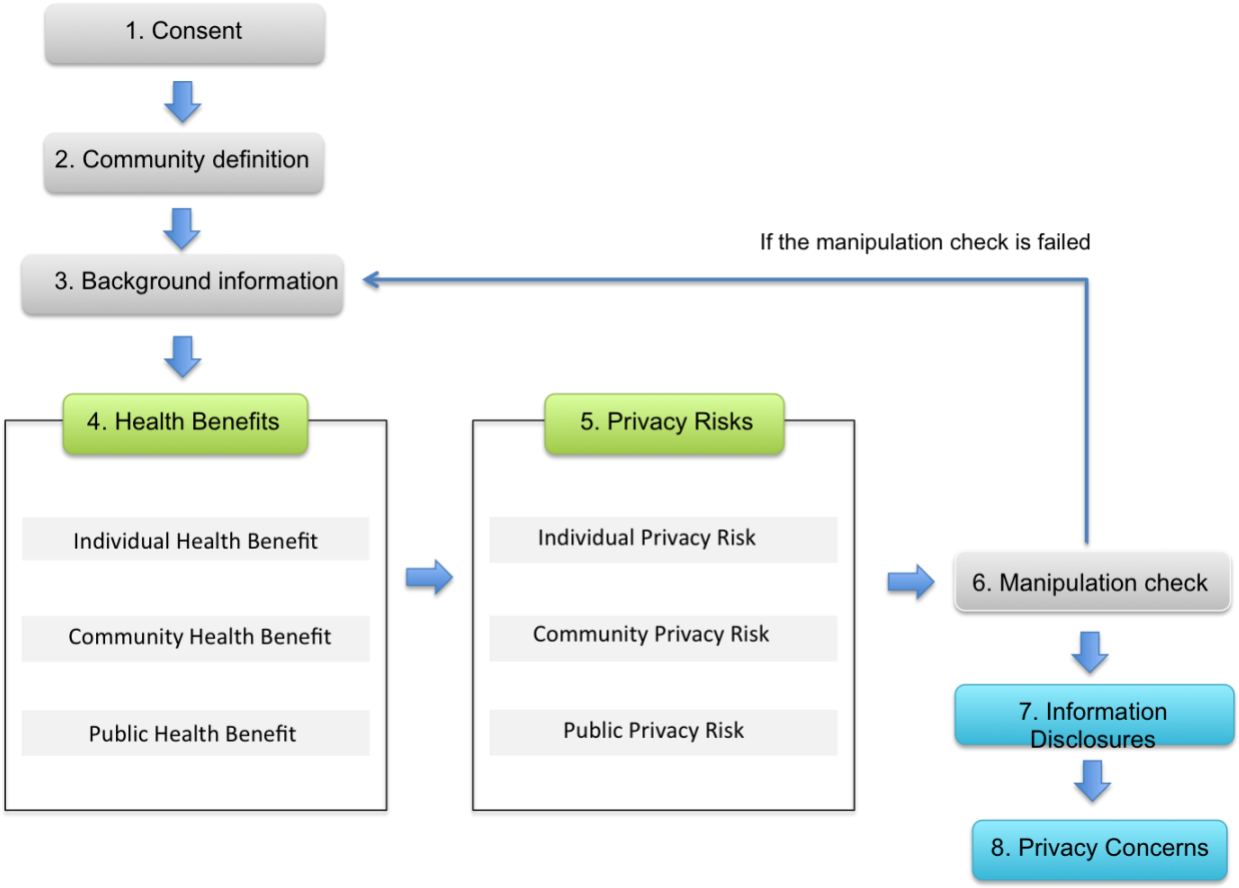
    - Have you traveled to South America or Africa in the last two months?
    - Do you have household members who traveled to South America or Africa in the last two months?
    - In the last 2 weeks, did you feel sick to your stomach?
    - Have you experienced a fever during the last 2 weeks?
    - Have you experienced brain fog (confusion, forgetfulness, or trouble concentrating) in the past 4 weeks?
    - Did you experience an unusual/new rash during the last 2 weeks?
    - What is your Blood type?
    - Have you had sex in the past 2 weeks?

- Do you use birth control?
- Are you currently in a relationship?
- Do you find yourself 'eating emotionally': eating unhealthy foods when you're not hungry, as a response to stress?
- How often do you drink alcohol?
- Have you gained more than 5 pounds in weight in the last two months?
- Are you disabled?
- Have you ever had a blood test taken?
- Are you pregnant?
- What is your current weight?
- What is your insurance company?
- What is your first name?
- What is your last name?
- What is your address?
- What is your zip code?
- What is your phone number?
- What is your email address?
- What city do you live in?
- What state do you live in?
- Where do you work? (Name of the place)
- What is your emergency contact information (name, relationship, phone number)

8. Post-surveys (Measures are listed in Appendix 2)

B. Study 2 process

Figure 13 Study 2 process



1. Consent

2. Background information

The Zika virus is currently affecting to parts of the world including the U.S. Zika is transmitted through sexual intercourse as well as bites from infected mosquitos. And this type of viral outbreak is becoming more common. For example, last year, the Ebola virus killed nearly 7,500 people in West Africa. This epidemic was not contained to the African continent, but found its way to the U.S. as well. Similarly, MERS virus has killed more than 400 people in Saudi Arabia and traveled to South Korea and infected 172 people. These instances demonstrate we are all at risk when viruses get out of hand, and outbreaks can happen anytime and anyplace. One of ways to decrease risk is for governments to share information about growing epidemics. Therefore, it is critical for governments to establish an efficient disease-control system to deal with viral outbreaks.

3. Health benefit

a. Individual benefit:
The Department of Health and Human Services (HHS) and Michigan State University have developed a new health recording system, "Outbreak Health Portal," to deal with viral outbreaks that have no current cure, like Zika and Ebola. For this system to have the most benefit, it is important that people sign up and share their information. We need your participation to build up the system. By signing up:

> You will gain direct, certified alerts and information from the HHS when outbreaks occur. If you are in a high-risk group for exposure then HHS will contact you directly and monitor your symptoms.

b. Community benefit:
The Department of Health and Human Services (HHS) and Michigan State University have developed a new health recording system, "Outbreak Health Portal," to deal with viral outbreaks that have no current cure, like Zika and Ebola. For this system to have the most benefit, it is important that people sign up and share their information. We need your participation to build up the system. By signing up:

> Your community will gain direct, certified alerts and information from the HHS when outbreaks occur. If your neighbors are in a high-risk group for exposure then HHS will contact your neighbors directly and monitor their symptoms.

c. Public benefit:
The Department of Health and Human Services (HHS) and Michigan State University have developed a new health recording system, "Outbreak Health Portal," to deal with viral outbreaks that have no current cure, like Zika and Ebola. For this system to have the most benefit, it is important that people sign up and share their information. We need your participation to build up the system. By signing up:

> The public will gain direct, certified alerts and information from the HHS when outbreaks occur. HHS will provide direct contact and symptom monitoring for those who are in a high-risk group exposure.

4. Privacy risk

a. Individual risk:
Here is how your health record will be used:

> If you are infected, your personal information can be shared with others in outbreak situations. Others are able to see who you are and where you live.

Community risk:
Here is how your health record will be used:

If someone in your local community is infected, the infected people's personal information can be shared with your local community in outbreak situations. Your local community is able to check who the infected people are and where they live.

Public risk:
Here is how your health record will be used:

If anyone is infected, their personal information can be shared with the public in outbreak situations. Anyone can check who is infected and where he or she lives.

5. Manipulation check

Please choose True or False (A participant will be asked to the two of the following items based on their assigned conditions)

You will gain direct, certified alerts and information from the HHS when outbreaks occur.
- True
- False
- I don't remember

Your community will gain direct, certified alerts and information from the HHS when outbreaks occur.
- True
- False
- I don't remember

The public will gain direct, certified alerts and information from the HHS when outbreaks occur.
- True
- False
- I don't remember

If you are infected, your personal information can be shared with others in outbreak situations.
- True
- False
- I don't remember

If someone in your local community is infected, the infected people's personal information can be shared with your local community in outbreak situations.
- True
- False
- I don't remember

If anyone is infected, their personal information can be shared with the public in outbreak situations.
- True
- False

- I don’t remember

6. Sign-up questions (information disclosure)

- Have you traveled to South America or Africa in the last two months?
- Do you have household members who traveled to South America or Africa in the last two months?
- In the last 2 weeks, did you feel sick to your stomach?
- Have you experienced a fever during the last 2 weeks?
- Have you experienced brain fog (confusion, forgetfulness, or trouble concentrating) in the past 4 weeks?
- Did you experience an unusual/new rash during the last 2 weeks?
- What is your Blood type?
- Have you had sex in the past 2 weeks?
- Do you use birth control?
- Are you currently in a relationship?
- Do you find yourself 'eating emotionally': eating unhealthy foods when you’re not hungry, as a response to stress?
- How often do you drink alcohol?
- Have you gained more than 5 pounds in weight in the last two months?
- Are you disabled?
- Have you ever had a blood test taken?
- Are you pregnant?
- What is your current weight?
- What is your insurance company?
- What is your first name?
- What is your last name?
- What is your address?
- What is your zip code?
- What is your phone number?
- What is your email address?
- What city do you live in?
- What state do you live in?
- Where do you work? (Name of the place)
- What is your emergency contact information (name, relationship, phone number)

7. Post surveys (Measures are listed in Appendix 2)

APPENDIX B

Post-Survey Measurements

1. Privacy concern

You signed up for the health portal website. Please rate your level of agreement with each statement below from Strongly Agree to Strongly Disagree (7 Likert Scale)

(Collection)

- It bothered me when the Outbreak Alert System asked me for personal information.
- When the Outbreak Alert System asked me for personal information, I thought twice before providing it.
- I was concerned that the Outbreak Alert System was collecting too much personal information about me.

(Secondary Usage)

- I'm concerned that when the Outbreak Alert System would use the information for other reasons.
- I'm concerned that the Outbreak Alert System would sell my personal information in their computer databases to other organizations.
- I'm concerned that the Outbreak Alert System would share my personal information with other organizations without my authorization.

(Improper Access)

- I'm concerned that the Outbreak Alert System database that contains my personal information is not protected from unauthorized access.
- I'm concerned that the Outbreak Alert System does not devote enough time and effort to preventing unauthorized access to my personal information.
- I'm concerned that the Outbreak Alert System does not take enough steps to make sure that unauthorized people could not access my personal information in their database.

(Control)

- It bothers me that I do not have control of personal information that I provided to the Outbreak Alert System.
- It bothers me that I do not have control or autonomy over decisions about how my personal information was collected, used, and shared by the Outbreak Alert System.
- I'm concerned when control is lost or unwillingly reduced as a result of information sharing with the Outbreak Alert System.

2. Trust

Please rate your level of agreement with each statement below from Strongly Agree to Strongly Disagree.

- The Outbreak Alert System is a trustworthy system
- I can count on the Outbreak Alert System to protect my privacy
- The Outbreak Alert System can be relied on to keep its promises

General trust

- I trust Government agencies
- (I trust government agencies keep my best interests in mind.)

3. Internet general privacy concern scale (Seven-point ascending Likert-type scale):

- When I provide data over the Internet, I am not sure who might collect it.
- My data is not safe on the Internet because it may be collected by unauthorized organizations.
- Websites would share with other firms the information they collect about my surfing process, without my permission.
- Websites would hand over the information they collect on me to other departments in the organization, without my permission.
- Websites would use the information they collect on me for purposes different to that initially authorized.

4. Altruism: Please rate your level of agreement with each statement below from Strongly Agree to Strongly Disagree. (Seven-point ascending Likert-type scale)
- My personal actions can greatly improve the well-being of people I don't know.
- It is my duty to help other people when they are unable to help themselves.
- Many of society's problems result from selfish behavior.
- Contributions to community organizations greatly improve the lives of others.
- My responsibility is to take care only of my family and myself.
- The individual alone is responsible for his or her own well-being in life.

5. Privacy violation experience (Not at all – Very often)
- How often have you personally been the victim of what you felt was an improper invasion of privacy?
- How much have you heard or read during the last year about the use and potential misuse of consumer's personal information without consumer's authorization by some service provider?

6. Community definition: What "community" means to you?
- Those who live in the same state with me
- Those who live in the same county with me
- Those who live in the same city with me
- Those who live in my neighborhood
- None of them (specify)

REFERENCES

REFERENCES

Accardo, J., & Chaudhry, M. A. (2014). Radiation exposure and privacy concerns surrounding full-body scanners in airports. *Journal of Radiation Research and Applied Sciences*, *7*(2), 198-200.

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM Conference on Electronic Commerce* (pp. 21–29). New York, NY, USA: ACM. http://doi.org/10.1145/988772.988777

Adey, P. (2002). Secured and sorted mobilities: Examples from the airport. *Surveillance & Society*, *1*(4). Retrieved from http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3333

Ancker, J. S., Edwards, A. M., Miller, M. C., & Kaushal, R. (2012). Consumer perceptions of electronic health information exchange. *American Journal of Preventive Medicine*, *43*(1), 76–80. http://doi.org/10.1016/j.amepre.2012.02.027

Andrade, E. B., Kaltcheva, V., & Weitz, B. (2002). Self-disclosure on the web: The impact of privacy policy, reward, and company reputation. *Advances in Consumer Research*, *29*(1), 350–353.

Awad, N. F., & 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*, 13-28.

Bansal, G., Zahedi, F. "Mariam," & 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), 138–150. http://doi.org/10.1016/j.dss.2010.01.010

Bellotti, V., & Sellen, A. (1993). Design for privacy in ubiquitous computing environments. In G. de Michelis, C. Simone, & K. Schmidt (Eds.), *Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW '93* (pp. 77–92). Springer Netherlands. Retrieved from http://link.springer.com/chapter/10.1007/978-94-011-2094-4_6

Berthon, P. R., Pitt, L. F., Plangger, K., & Shapiro, D. (2012). Marketing meets Web 2.0, social media, and creative consumers: Implications for international marketing strategy. *Business Horizons*, *55*(3), 261–271. http://doi.org/10.1016/j.bushor.2012.01.007

Bowyer, K. W. (2004). Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine*, *23*(1), 9–19. http://doi.org/10.1109/MTAS.2004.1273467

Bozsak, E., Ehrig, M., Handschuh, S., Hotho, A., Maedche, A., Motik, B., … Zacharias, V. (2002). KAON — Towards a large scale semantic web. In K. Bauknecht, A. M. Tjoa, & G. Quirchmayr (Eds.), *E-Commerce and Web Technologies* (pp. 304–313). Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/3-540-45705-4_32

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. http://doi.org/10.1177/1948550612455931

Calo, R. (2015). *Can Americans Resist Surveillance?* (SSRN Scholarly Paper No. ID 2635181). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=2635181

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, *6*(2-3), 181–202. http://doi.org/10.1007/s10799-005-5879-y

Choe, S. H. (2015, JUNE 14). South Korea's Response to MERS Cases Is Faulted. *The New York Times.* Page A11. Retrieved from https://www.nytimes.com/2015/06/14/world/asia/experts-fault-south-korean-response-to-mers-outbreak.html

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior*, *12*(3), 341–345. http://doi.org/10.1089/cpb.2008.0226

Dai, B., Forsythe, S., & Kwon, W.-S. (2014). The impact of online shopping experience on risk perceptions and online purchase intentions: Does product category matter. *Journal of Electronic Commerce Research*, *15*(1), 13–24.

Diallo, D. D, & Frew, P. M. (2014). Community engagement in public health research. In G. Guest & E. E. Namey (Eds.), *Public Health Research Methods* (pp. 101–121). SAGE Publications.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce - a study of Italy and the United States. *European Journal of Information Systems*, *15*(4), 389–402. http://doi.org/http://dx.doi.org.proxy2.cl.msu.edu/10.1057/palgrave.ejis.3000590

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado August 09-12 2007*. Retrieved from http://ci.nii.ac.jp/naid/10024984538/

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, *59*(8), 877–886. http://doi.org/10.1016/j.jbusres.2006.02.006

Fan, M., Lin, N.-P., & Sheu, C. (2008). Choosing a project risk-handling strategy: An analytical model. *International Journal of Production Economics*, *112*(2), 700–713. http://doi.org/10.1016/j.ijpe.2007.06.006

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies*, *59*(4), 451–474. http://doi.org/10.1016/S1071-5819(03)00111-3

Fehr, E., & Fischbacher, U. (2003). The nature of human altruism. *Nature,425*(6960), 785-791.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541–562. http://doi.org/10.1016/j.jbi.2012.12.003

Fine, P. E. M., & Clarkson, J. A. (1986). Individual versus public priorities in the determination of optimal vaccination policies. *American Journal of Epidemiology*, *124*(6), 1012–1020.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*, *9*(2), 127–152. http://doi.org/10.1007/BF00143739

Florance, C., Caravan, J., & Kaniewski, D. (2015). The Ebola Outbreak of 2013–2014: An Assessment of U.S. Actions. Retrieved from research on the Heritage Foundation website: http://www.heritage.org/homeland-security/report/the-ebola-outbreak-2013-2014-assessment-us-actions

Hann, I.-H., Hui, K.-L., Lee, T., & Png, I. (2002). Online information privacy: Measuring the cost-benefit trade-off. *ICIS 2002 Proceedings*, 1.

Heen, M. S., Lieberman, J. D., & Miethe, T. D. (2014). A comparison of different online sampling approaches for generating national samples. Retrieved from http://www.unlv.edu/sites/default/files/page_files/27/ComparisonDifferentOnlineSampling.pdf

Hoadley, C. M., Xu, H., Lee, J. J., & 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), 50–60. http://doi.org/10.1016/j.elerap.2009.05.001

Hong, W., & Thong, J. Y. L. (2013). *Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies* (SSRN Scholarly Paper No. ID 2229627).

Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=2229627

Im, I., Kim, Y., & Han, H.-J. (2008). The effects of perceived risk and technology type on users' acceptance of technologies. *Information & Management*, *45*(1), 1–9. http://doi.org/10.1016/j.im.2007.03.005

Kaelber, D. C., & Bates, D. W. (2007). Health information exchange and patient safety. *Journal of Biomedical Informatics*, *40*(6, Supplement), S40–S45. http://doi.org/10.1016/j.jbi.2007.08.011

Kandias, M., Mitrou, L., Stavrou, V., & Gritzalis, D. (2013). Which side are you on? A new Panopticon vs. privacy. In *2013 International Conference on Security and Cryptography (SECRYPT)* (pp. 1–13).

Kankanhalli, A., Tan, B. C. Y., & Wei, K.-K. (2005). Contributing knowledge to electronic knowledge repositories: An empirical investigation. *MIS Quarterly*, *29*(1), 113–143.

Khalfan, A. M. (2004). Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *International Journal of Information Management*, *24*(1), 29–42. http://doi.org/10.1016/j.ijinfomgt.2003.12.001

Kim, J., & Lennon, S. J. (2013). Effects of reputation and website quality on online consumers' emotion, perceived risk and purchase intention: Based on the stimulus-organism-response model. *Journal of Research in Interactive Marketing*, *7*(1), 33-56.

Klein, W. M., & Kunda, Z. (1994). Exaggerated self-assessments and the preference for controllable risks. *Organizational Behavior and Human Decision Processes*, *59*(3), 410–427. http://doi.org/10.1006/obhd.1994.1067

Knijnenburg, B. P., & Kobsa, A. (2013). Making decisions about privacy: Information disclosure in context-aware recommender systems. *ACM Trans. Interact. Intell. Syst.*, *3*(3), 20:1–20:23. http://doi.org/10.1145/2499670

Kusar, B. (2015). The right to liberty and security: A precondition for establishing and guaranteeing the human security. *European Scientific Journal, ESJ*, *11*(11). Retrieved from http://www.eujournal.org/index.php/esj/article/view/5445

Lichtblau, K. B. Eric, & Wingfield, N. (2016, February 25). Apple Goes to Court, and F.B.I. Presses Congress to Settle iPhone Privacy Fight. *The New York Times*. Retrieved from http://www.nytimes.com/2016/02/26/technology/apple-unlock-iphone-fbi-san-bernardino-brief.html

Liu, C., Ang, R. P., & Lwin, M. O. (2013). Cognitive, personality, and social factors associated with adolescents' online personal information disclosure. *Journal of Adolescence*, *36*(4), 629–638. http://doi.org/10.1016/j.adolescence.2013.03.016

Im, I., Kim, Y., & Han, H. J. (2008). The effects of perceived risk and technology type on users' acceptance of technologies. *Information & Management*, *45*(1), 1-9.

MacQueen, K. M., McLellan, E., Metzger, D. S., Kegeles, S., & al, et. (2001). What is community? An evidence-based definition for participatory public health. *American Journal of Public Health*, *91*(12), 1929–38.

Madden, M. (2015). *Privacy and Cybersecurity: Key findings from Pew Research*. Retrieved from http://www.pewresearch.org/key-data-points/privacy/

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Mauricio S. Featherman, Anthony D. Miyazaki, & David E. Sprott. (2010). Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. *Journal of Services Marketing*, *24*(3), 219–229. http://doi.org/10.1108/08876041011040622

McGraw, D., Dempsey, J. X., Harris, L., & Goldman, J. (2009). Privacy as an enabler, not an impediment: Building trust into health information exchange. *Health Affairs*, *28*(2), 416–427. http://doi.org/10.1377/hlthaff.28.2.416

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, *9*(4), 00–00. http://doi.org/10.1111/j.1083-6101.2004.tb00292.x

Miller, D. L., Alderslade, R., & Ross, E. M. (1982). Whooping cough and whooping cough vaccine: the risks and benefits debate. *Epidemiologic Reviews*, *4*, 1–24.

Miller, R., & Lessard, D. (2001). Understanding and managing risks in large engineering projects. *International Journal of Project Management*, *19*(8), 437–443. http://doi.org/10.1016/S0263-7863(01)00045-X

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs*, *38*(2), 217–232. http://doi.org/10.1111/j.1745-6606.2004.tb00865.x

Mironenko, O. (2011). Body scanners versus privacy and data protection. *Computer Law & Security Review*, *27*(3), 232-244.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *The Journal of Consumer Affairs*, *35*(1), 27–44.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2011). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research*, 1094670511424924. http://doi.org/10.1177/1094670511424924

Myers, J., Frieden, T. R., Bherwani, K. M., & Henning, K. J. (2008). Ethics in public health research. *American Journal of Public Health*, *98*(5), 793–801. http://doi.org/10.2105/AJPH.2006.107706

Nakashima, E. (2016, February 16). Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, *79*, 119.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. http://doi.org/10.1111/j.1745-6606.2006.00070.x

Norris, C., McCahill, M., & Wood, D. (2002). The growth of CCTV: A global perspective on the international diffusion of video surveillance in publicly accessible space. *Surveillance & Society*, *2*(2/3). Retrieved from http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3369

Nowak, G. J., & 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), 46–60. http://doi.org/10.1002/dir.4000090307

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, *25*(2), 243–262. http://doi.org/10.1016/S0167-4870(02)00172-1

Ornstein, C. (2015, March 2). Ebola-infected Nurse Contends Dallas Hospital Violated Her Privacy. ProPublica. Retrieved from https://www.propublica.org/article/ebola-infected-nurse-contends-dallas-hospital-violated-her-privacy

Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 129–136). New York, NY, USA: ACM. http://doi.org/10.1145/642611.642635

Patil, S., & Kobsa, A. (2009). Privacy considerations in awareness systems: designing with privacy in mind. In *Awareness Systems* (pp. 187-206). Springer London.

Pavone, V., & Esposti, S. D. (2010). Public assessment of new surveillance-oriented security technologies: beyond the trade-off between privacy and security. *Public Understanding of Science*. http://doi.org/10.1177/0963662510376886

Pearson, T. A., Palaniappan, L. P., Artinian, N. T., Carnethon, M. R., Criqui, M. H., Daniels, S. R., … on behalf of the American Heart Association Council on Epidemiology and Prevention. (2013). American Heart Association Guide for Improving Cardiovascular Health at the Community Level, 2013 Update: A Scientific Statement for Public Health Practitioners, Healthcare Providers, and Health Policy Makers. *Circulation*, *127*(16), 1730–1753. http://doi.org/10.1161/CIR.0b013e31828f8a94

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27–41. http://doi.org/10.1509/jppm.19.1.27.16941

Proenca, E. J. (1998). Community orientation in health services organizations: The concept and Its implementation: *Health Care Management Review*, *23*(2), 28–38. http://doi.org/10.1097/00004010-199804000-00004

Rainie, L., & Madden, M. (2015). *Americans' privacy strategies post-snowden*. Pew Research Centers Internet American Life Project RSS. Retrieved from http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/

Santos, J., Pedrosa, T., Costa, C. M., & Oliveira, J. L. (2010). Modelling a portable personal health record. *Health INF 2010, Third International Conference on Health Informatics*, 465–468.

Shapiro, J. S., Kannry, J., Lipton, M., Goldberg, E., Conocenti, P., Stuard, S., & Kuperman, G. (2006). Approaches to patient health information exchange and their impact on emergency medicine. *Annals of Emergency Medicine*, *48*(4), 426–432. http://doi.org/10.1016/j.annemergmed.2006.03.032

Simon, S. R., Evans, J. S., Benjamin, A., Delano, D., & Bates, D. W. (2009). Patients' attitudes toward electronic health information exchange: Qualitative Study. *Journal of Medical Internet Research*, *11*(3), e30. http://doi.org/10.2196/jmir.1164

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Q.*, *35*(4), 989–1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196. http://doi.org/10.2307/249477

Special, W. P., & Li-Barber, K. T. (2012). Self-disclosure and student satisfaction with Facebook. *Computers in Human Behavior*, *28*(2), 624–630. http://doi.org/10.1016/j.chb.2011.11.008

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826. http://doi.org/10.1016/j.chb.2012.11.022

Thorn, B. K., & Connolly, T. (1987). Discretionary data bases A theory and some experimental findings. *Communication Research*, *14*(5), 512–528. http://doi.org/10.1177/009365087014005004

Ursin, L. O. (2010, September). Privacy and property in the biobank context. In *HEC forum* (Vol. 22, No. 3, pp. 211-224). Springer Netherlands.

Vest, J. R., & Gamm, L. D. (2010). Health information exchange: persistent challenges and new strategies. *Journal of the American Medical Informatics Association*, *17*(3), 288–294. http://doi.org/10.1136/jamia.2010.003673

Viscusi, W. K., & Zeckhauser, R. J. (2003). Sacrificing civil liberties to reduce terrorism risks. In W. K. Viscusi (Ed.), *The Risks of Terrorism* (pp. 1–22). Springer US. Retrieved from http://link.springer.com/chapter/10.1007/978-1-4757-6787-2_1

Wang, H., Lee, M. K. O., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communication of the ACM*, *41*(3), 63–70. http://doi.org/10.1145/272287.272299

Wen, K.Y., Kreps, G., Zhu, F., & Miller, S. (2010). Consumers' perceptions about and use of the Internet for personal health records and health information exchange: Analysis of the 2007 Health Information National Trends Survey. *Journal of Medical Internet Research*, *12*(4). http://doi.org/10.2196/jmir.1668

Westin, A. F. (1970). *Privacy and Freedom*. 1967. *Atheneum, New York*.

Wilson, D., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus.

Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: an integrated mode. *Electronic Commerce Research*, *13*(2), 151–168. http://doi.org/10.1007/s10660-013-9111-6

Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. In *Proceedings of 28th Annual International Conference on Information Systems (ICIS 2007*.

Xu, H., Teo, H.-H., Tan, B. C. Y., & 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), 135–174. http://doi.org/10.2753/MIS0742-1222260305

Yang, H. (2014). Prior Negative Experience, Online Privacy Concerns and Intent to Disclose Personal Information in Chinese Social Media. *International Journal of E-Business Research (IJEBR), 10*(2), 23-44

Zureik, E., & Salter, M. (2013). *Global Surveillance and Policing*. Routledge.