Dec 14th, 12:00 AM

Privacy Awareness under Scrutiny: Field Experimental Evidence on Health Data Protection in Underserved Communities

Marie Gabel
WWU University Muenster, marie.gabel@wiwi.uni-muenster.de

J. Nils Foege
Leibniz University Hannover, nils.foege@wa.uni-hannover.de

Stephan Nüesch
University of Muenster, nueesch@wwu.de

Privacy Awareness under Scrutiny: Field Experimental Evidence on Health Data Protection in Underserved Communities

Completed Research Paper

Marie Gabel
University of Muenster
Business Management Group
Georgskommende 26
D-48143 Muenster
marie.gabel@wiwi.uni-muenster.de

J. Nils Foege
University of Hannover
Innovation Management Group
Schloßwender Str. 7
D-30159 Hannover
nils.foege@wa.uni-hannover.de

Stephan Nüesch
University of Muenster
Business Management Group
Georgskommende 26
D-48143 Muenster
stephan.nueesch@wiwi.uni-muenster.de

Abstract

Health information systems in developing countries support the political vision of promoting equity in access to health services. However, these data-driven advancements raise severe privacy issues in most developing countries due to the lack of awareness of privacy risks and of measures to counteract those risks. Drawing on social cognitive theory and the Antecedents-Privacy Concerns-Outcomes model, we combine two complementary theoretical lenses to argue that solution-focused and risk-focused privacy awareness-raising measures influence individuals' data protection behavior through the two channels of privacy self-efficacy and privacy concerns. To test our theorizing, we conducted a randomized, controlled field experiment in collaboration with a non-governmental organization working on health information systems in West Africa. Our results provide in-depth and context-sensitive insights into how privacy awareness influences privacy behavior. We show that even simple awareness-raising measures increase individuals' privacy protection behavior when framed in a solution-focused instead of a risk-focused way.

Keywords: Social cognitive theory; privacy awareness; privacy concerns; privacy self-efficacy; developing countries; data privacy; privacy protection

Introduction

With broad availability of smartphones and internet connections even in the most remote and rural areas, information systems have made their way into developing countries (Avgerou et al. 2016; Venkatesh et al. 2019). Although their manifold applications are useful in many aspects of life, they yield exceptional potential to improve the healthcare sector in developing countries, which often suffers from a lack of human resources and infrastructure (Braa et al. 2004; Fichman et al. 2011). To improve this situation, researchers and international agencies such as the World Health Organization are focusing on health information systems (Braa et al. 2004; Fichman et al. 2011; Källander et al. 2013). Health information systems promote the political vision of equity in healthcare services (World Health Organization 2005). They help to deliver healthcare to the most remote and deprived areas (Braa et al. 2004) and help to deal with epidemic outbreaks such as Ebola and COVID-19 in an effective way (Chen et al. 2015; Fichman et al. 2011).

Despite the immense benefits that information technology can provide for healthcare, the information that is stored about individuals' health can fall victim to data misuse. This is a delicate matter as individual-level health data are among the most sensitive data (Bansal et al. 2010; Fichman et al. 2011) and misuse of health data can have severe consequences for the individual as e.g. social exclusion or job loss (Acquisti et al. 2015). Nevertheless, the growing use of health information technology has not led to appropriate adjustments of data privacy and security legislation in developing countries (Harris et al. 2013). Moreover, the high unfamiliarity with the overall topic of data privacy increases individuals' vulnerability (Pötzsch 2009).

In line with the Antecedents-Privacy Concerns-Outcomes (APCO) model (Smith et al. 2011), prior research identifies privacy awareness as a core measure to support individuals' information privacy (Correia and Compeau 2017; Malandrino et al. 2013). Privacy awareness draws attention to the threats of data misuse as well as possible countermeasures for responding to these threats (Deuker 2010). We argue that privacy awareness includes both risk-focused aspects, i.e. potential negative consequences of data privacy violations, and solution-focused aspects, i.e. ways to protect individuals' data privacy, both of which are necessary for informed decision-making in data-driven environments (Deuker 2010). While prior research pointed out the importance of privacy awareness (Pötzsch 2009; Correia and Compeau 2017), there is little evidence indicating how privacy awareness has to be framed to efficiently affect privacy-related attitudes and behavior. Therefore, we pose the following research question: *How do risk and solution-focused awareness-raising measures affect the way people think and act in relation to their data privacy in developing countries?*

To understand the cognitive mechanisms behind privacy awareness and privacy protection, we examine the roles of privacy concerns and privacy self-efficacy. In their APCO model, Smith et al. (2011) argue that privacy concerns are the main predictor of privacy-related behavior. We argue that the explanatory power of the APCO model can be enhanced by including privacy self-efficacy, i.e. "individuals' level of confidence in protecting their privacy" (Lee and Hill 2013, p. 331) as another important antecedent of privacy protection (Chen 2018). While privacy concerns may be associated with a feeling of helplessness, privacy self-efficacy addresses the opposite, dealing with the self-confidence of individuals to be able to protect their personal data successfully. Following Chen and Zahedi (2016), levels of privacy self-efficacy differ greatly between cultures and contexts of rural and urbanized economies. We argue that privacy self-efficacy is both in short supply and greatly needed for privacy protection behavior in developing countries, as low levels of privacy education and high corruption rates tend to lower individuals' confidence levels.

We conducted a randomized, controlled field experiment in collaboration with eHealth Africa, a non-governmental organization working on data-driven health solutions in West Africa. The healthcare context is underrepresented in prior research and is subject to significant context specifics that are worth examining (Fichman et al. 2011). First, particularly in developing countries, improvements in the healthcare situation are greatly needed. Health information systems provide immense benefits that can influence individuals' decision-making regarding the protection of their data. Second, personal health information is among the most sensitive data (Anderson et al. 2017; Bansal et al. 2016), so understanding privacy-related risks and protective countermeasures is particularly important in the healthcare context. Our findings broadly support our theorizing, suggesting that even simple awareness-raising measures significantly influence privacy concerns and privacy self-efficacy. Solution-focused awareness-raising, which provided individuals with information on how to protect their privacy, increased privacy protection. In contrast, risk-focused awareness-raising did not affect individuals' behavior. In line with our theorizing, we find that privacy

protection is context-dependent, as the underlying cognitive mechanisms differ between developed and developing countries. Whereas prior studies conducted in developed countries show that privacy concerns are the main driver for privacy protection (e.g., Anderson and Agarwal 2011; Cichy et al. 2014), our findings suggest that, in developing countries, privacy self-efficacy is the critical factor in that regard.

We contribute to the literature on health information privacy in three major ways. First, our experimental approach makes it possible to examine the causal effects of solution-focused and risk-focused awareness-raising measures on individuals' privacy behavior. These two sides of privacy awareness-raising and their consequences to individuals' privacy protection have not received much attention from prior research (Smith et al. 2011). Insight is desperately needed, as individuals in developing countries are often under-informed and lack the capacity to protect their privacy. Second, we extend the APCO model (Smith et al. 2011) by linking it to social cognitive theory (Bandura 2001) and to the concept of privacy self-efficacy - an underlying mechanism that influences individuals' privacy behavior. Finally, while prior research mainly examined US samples (Belanger and Crossler 2011; Chen 2018; Chen and Zahedi 2016), we conduct context-sensitive research in Nigeria. The context of a developing country is particularly important as contextual differences like educational levels, corruption rates, information technology dissemination, and cultural traits influence individuals' decision-making and thereby significantly affect privacy-related attitudes and behaviors (Belanger and Crossler 2011; Gebre-Mariam and Bygstad 2019). Indeed, our results confirm that privacy awareness and privacy protection in healthcare are context-dependent.

Conceptual Background

Privacy in Information Systems. Privacy is a complex and multifaceted issue. In information systems, privacy can be defined as the ability of individuals to control the conditions under which their personal information is collected and used (Culnan and Bies 2003; Xu et al. 2009). Information asymmetry and uncertainty often restrict individuals in their data privacy and put them at risk of having that privacy violated (Youn 2009). As personal health data is particularly sensitive, data privacy violation can have serious consequences. Risk perceptions lead to privacy concerns, which in turn strongly influence the adoption of information technology in healthcare (Angst and Agarwal 2009; Bansal et al. 2010). In recent years, studies on privacy in information systems have gained traction, leading to many theories and conceptual frameworks. To establish a more robust approach, Smith et al. (2011) conducted an interdisciplinary review of over 400 privacy-related articles and books. Their analysis led to the development of an overarching macro model, the APCO model, which illustrates the relationship between antecedents, privacy concerns, and actual outcomes.

Privacy awareness. Smith et al. (2011) argue that culture, demographics, personality, privacy experiences, and privacy awareness are key antecedents of privacy concerns and privacy-related behavior. Privacy awareness is especially needed to get closer to the overriding goal of informed decision-making in data-driven environments (Harris et al. 2013; Malandrino et al. 2013). According to Pötzsch (2009), privacy awareness is the cognition and knowledge of (1) whether others have received personal data, (2) the type of data that is collected and shared, (3) how the data is processed and used, (4) the amount of data, and (5) how the data could jeopardize the individual by violating their personal privacy.

In general, individuals with poor data privacy knowledge are more likely to place themselves at risk. Individuals in developing countries are often unaware of privacy threats and of ways to reduce their vulnerability (Harris et al. 2013). Due to their high numbers of individuals unversed in data privacy, developing countries are particularly vulnerable to data privacy threats. Notwithstanding the importance of privacy awareness, especially in developing countries, the conceptualization and theoretical understanding of privacy awareness are still limited (Correia and Compeau 2017).

Privacy awareness is a crucial step to motivate individuals to take care of their data privacy. Privacy awareness can help to overcome irrational decision making caused by information asymmetry (Deuker 2010). Presenting individuals with privacy-related messages activates consciousness of data privacy. These messages can be framed in different ways. Scholarly research, governmental policy, and business practice have mainly applied awareness-raising in a risk-focused way, in terms of privacy warnings (LaRose and Rifon 2007). However, awareness of positive countermeasures that one can take to protect one's personal data is another important part of the equation (Crossler and Bélanger 2019). Thus, we argue that privacy

awareness comprises both awareness of potential privacy problems and awareness of ways to prevent those problems from happening (Deuker 2010).

These two sides are also reflected in protection motivation theory (Rogers 1975). Protection motivation theory argues that individuals adopt a protective behavior based on two underlying cognitive processes: the threat appraisal process, which refers to the severity and vulnerability of the respective situation and the coping-appraisal process, which refers to the effectiveness of counteracting potential harm. We argue that this two-sided phenomenon can be applied to the privacy context and advocate in favor of viewing privacy awareness as a two-sided construct. First, privacy awareness can be solution-focused, by educating individuals about ways to protect their data privacy. Second, it can be risk-focused, by educating individuals about potential negative consequences of data privacy violations (Deuker 2010).

Privacy concerns. In the center of the APCO model are privacy concerns (Smith et al. 2011). Privacy concerns are beliefs about risks and costs that come with the disclosure of personal information (Dinev and Hart 2006). Privacy concerns increase when individuals experience a loss of control over their personal data. Individuals who are concerned about online privacy exhibit lower trust and are thus less likely to engage in behavior that exposes them to risks of privacy violation. However, prior literature challenges the common assumption of rational decision making, arguing that actual privacy protection does not correspond to individuals' articulated behavioral intentions and attitudes (Acquisti 2004; Acquisti and Grossklags 2005). Norberg et al. (2007) call this phenomenon the privacy paradox. Given irrational decision making, real behavior does not necessarily reflect privacy concerns and behavioral intentions (Acquisti 2004; Acquisti and Grossklags 2005). To draw conclusions about individuals' behavior, it is necessary to focus on actual behavior instead of on attitudes or intentions (Belanger and Xu 2015).

Privacy self-efficacy. Privacy self-efficacy refers to the confidence of individuals to be successful in protecting their privacy (Lee and Hill 2013). Self-efficacy constitutes a critical element of social cognitive theory (Bandura 2001). According to social cognitive theory, individuals who believe in their power to master a certain situation will show higher effort toward this behavior which leads to a higher probability of being successful. Individuals' confidence levels are thus directly associated with their behavioral responses (Keith et al. 2015).

Applied to the privacy context, the theoretical notions of social cognitive theory suggest that individuals who believe in their ability to protect their privacy - i.e., who have higher privacy self-efficacy (Crossler and Bélanger 2019) - are more motivated and show higher effort to protect their privacy (Cho et al. 2009). Privacy self-efficacy can be particularly decisive for individuals' privacy-related decision making in developing countries, as low levels of privacy education and high corruption rates influence individuals' confidence levels (Harris et al. 2013). To understand the underlying cognitive mechanisms behind privacy protection in developing countries and the role of privacy awareness, we, therefore, combine social cognitive theory with the APCO model. We argue that privacy awareness affects privacy protection not only through privacy concerns but also through privacy self-efficacy.

Hypotheses

Privacy Awareness

Privacy awareness and privacy protection

A pre-requisite for individuals to assume ownership of their data is privacy awareness (Harris et al. 2013). Even though privacy awareness is a key antecedent of the APCO model, studies on privacy awareness are severely underrepresented in the information systems literature (Deuker 2010; Pötzsch 2009; Smith et al. 2011). Prior research shows that lack of awareness about privacy protection is still a major issue (Belanger and Crossler 2011). In developing countries, there are little to no official data privacy regulations, leaving individuals to protect their data themselves (Harris et al. 2013). Ironically, privacy awareness is particularly low in developing countries. Limited access to information technologies restricts individuals' experience, which leads to a general unawareness of internet threats (Harris et al. 2013; Kumaraguru and Cranor 2005).

Individuals who are unaware of privacy threats and potential countermeasures will be more likely to place themselves at risk or misunderstand information practices of requesting organizations (Crossler and Bélanger 2019; Dommeyer and Gross 2003; Harris et al. 2013). This issue is particularly delicate in the

healthcare sector due to the highly sensitive nature of personal health information (Angst and Agarwal 2009; Bansal et al. 2010, 2016). Increasing privacy awareness is, therefore, a crucial step to move individuals toward taking care of their personal health information in an adequate and reflected manner (Deuker 2010). Distinguishing between solution-focused and risk-focused awareness-raising measures, our study extends the APCO model by hypothesizing:

Hypothesis 1. Solution-focused awareness-raising increases privacy protection.

Hypothesis 2. Risk-focused awareness-raising increases privacy protection.

Solution-focused awareness-raising

Protection motivation theory (Rogers 1975) argues that individuals' protective behaviors are driven by the threat appraisal process, which refers to the severity and vulnerability of the respective situation and the coping-appraisal process, which refers to the effectiveness of counteracting potential harm. Applying this two-sided consideration to the topic of privacy awareness, we argue that privacy awareness consists of both, risk-focused and solution-focused privacy awareness. As prior studies mainly focused on the awareness of privacy-risks, we follow Deuker (2010) and argue that expanding privacy awareness from a risk-based toward a solution-based conceptualization is a key success factor to support informed privacy decisions.

Bandura (2008) states that feelings and emotions are critical influences on individuals' levels of self-efficacy concerning a certain behavior. Social persuasion shapes these feelings and emotions. When social persuasion decreases the negative misinterpretations of individuals' abilities and focuses instead on positive emotions, individuals' levels of self-efficacy increase (Bandura 2008). In turn, self-efficacy leads to greater effort and motivation even when individuals are confronted with obstacles. Educating individuals about how to master a certain task and thereby raising their awareness in a solution-focused way can persuade them of their efficacy. We expect that individuals in developing countries are insufficiently educated about ways to counteract potential privacy threats. Following our line of argumentation, privacy self-efficacy is also comparably low as individuals lack positive experiences or social persuasion that convince them of their ability to protect their privacy effectively.

Drawing on the theoretical mechanisms of social cognitive theory (Bandura 2001), we argue that expanding privacy awareness from a risk-focused approach toward a solution-focused approach will increase individuals' feeling of being able to master privacy issues (Deuker 2010). We argue that solution-focused educational support increases positive emotions, reduces negative feelings of being vulnerable to data misuse, and motivates individuals to proactively guard themselves against data privacy problems. Therefore, we propose the following hypothesis:

Hypothesis 3. Solution-focused awareness-raising increases privacy self-efficacy.

Prior literature on the so-called "control paradox" suggests that if individuals level of perceived control over the disclosure of personal information increases (e.g. by being presented with solution-focused awareness-raising measures) individuals will exhibit lower levels of privacy concerns and will be more likely to share information even though the absolute level of privacy risks does not change (Acquisti et al. 2015). However, we argue that solution-focused awareness-raising measures draw individuals' attention to the topic of data privacy. Presenting individuals with ways to protect their privacy will get them thinking about privacy issues (Baek 2014). The more knowledge individuals gain about data privacy, the more conscious they become of the associated privacy risks and threats. In turn, increased awareness triggers the feeling of loss of control over the personal data. Following Acquisti et al. (2015), the perceived loss of control triggers privacy concerns. The cognitive activation through solution-focused awareness-raising measures will, therefore, increase privacy concerns, as individuals become more aware of data privacy issues (Ozdemir et al. 2017).

Prior literature supports our line of argumentation. Cespedes and Smith (1993) suggest that privacy concerns are triggered when individuals are confronted with the overall topic of data privacy, as their general awareness increases. Culnan (1995) finds that consumers who are unaware of procedures for removing their names from mailing lists have fewer concerns about their privacy than consumers who are aware of such procedures. An experiment by Baek (2014) suggests that presenting individuals with privacy-related messages encourages reflection on privacy issues. An online survey by Ozdemir et al. (2017), shows that privacy awareness increases privacy concerns significantly.

Drawing on literature about the context-dependency of privacy-related attitudes and behaviors (see Acquisti et al. 2015), we argue that the context of our study amplifies this cause-effect relationship in two major ways. First, we expect that individuals in developing countries have limited knowledge about data privacy and will spend less time thinking about privacy issues. Thus, even though the solution-framed educational measures provide information about how to protect privacy, they will, in the context of our study, primarily trigger awareness about the presence of privacy issues and thus a feeling of low control over the data. Second, personal health information is among the most sensitive information (Angst and Agarwal 2009; Bansal et al. 2010, 2016), thus individuals might be more concerned about losing health-related information than about losing other types of personal data.

Therefore, we argue that solution-focused awareness-raising increases privacy concerns as recipients become more aware of data privacy issues. We propose the following hypothesis:

Hypothesis 4. Solution-focused awareness-raising increases privacy concerns.

Risk-focused awareness-raising

Whereas privacy success stories are rare, negative privacy messages have dominated the media. Headlines about personal data misuse and large-scale cyber-attacks have raised individuals' privacy awareness in a risk-focused way (Deuker 2010). Particularly in healthcare, data misuse scandals lead to great media attention due to the sensitive nature of health data (Bansal et al. 2010). The data scandal in 2019 in which Google collected and analyzed the health data of millions of US patients is only one of many examples in recent years (Singer and Wakabayashi 2019). Risk-focused awareness-raising measures, such as information about data scandals and general education about the dangers of data sharing, increase individuals' privacy awareness in a negatively-framed way (Deuker 2010).

Social cognitive theory (Bandura 2001) addresses the underlying cognitive mechanisms between risk-focused awareness-raising and privacy-related behavior. Following Bandura's (2001) theoretical notions, negative emotions regarding a certain activity decrease individuals' self-efficacy, their belief that they can be successful, which in turn decreases effort and motivation toward this activity. We transfer this theoretical mechanism to the context of privacy, arguing that awareness-raising measures that focus on potential privacy problems reduce individuals' belief that they can be successful in data protection. Negative emotions dominate and privacy self-efficacy decreases. In this regard, we expect that individuals in developing countries might feel particularly helpless due to the typically high corruption rates and limited transparency of media, business practice, and politics. We therefore hypothesize:

Hypothesis 5. Risk-focused awareness-raising decreases privacy self-efficacy.

Even if individuals consider health information as particularly sensitive (Angst and Agarwal 2009; Bansal et al. 2010, 2016), awareness of risks and threats is a core requirement for adequately dealing with privacy issues. Individuals who are unaware of problems that come with data sharing will not be able to identify the associated risks or employ appropriate data protection measures (Deuker 2010). Misuse of personal health information can have serious financial and social consequences (Acquisti et al. 2015). Supporting individuals in becoming aware of these consequences helps them to make good decisions in data-driven environments (Pötzsch 2009). Individuals who are presented with privacy-related content are more likely to think about privacy issues. Through cognitive activation, individuals familiarize themselves with risks of data sharing (Baek 2014). They become more aware of the negative consequences associated with their privacy-related behavior and feel vulnerable. Increased awareness of potential privacy problems is in turn positively associated with individuals' privacy concerns (Cespedes and Smith 1993). Following the notions of the APCO model, risk-focused awareness-raising measures increase privacy concerns as individuals become more familiar with the potential negative consequences of their behavior (Smith et al. 2011).

When researchers have applied this type of theorizing to experimental situations, the results have been mixed. LaRose and Rifon (2007) examine the effects of privacy warnings on the expectations of negative outcomes. The results were not significant. However, Culnan (1995) found that consumers who were unaware of procedures for removing their names from mailing lists had fewer concerns about their privacy than consumers who were aware of such procedures. Following Cespedes and Smith (1993), the awareness of data collection and the use of personal data without explicit permission trigger privacy concerns. We expect that the results of Culnan (1995) and Cespedes and Smith (1993) not only hold in the context of our

study but are even strengthened due to the sensitive nature of personal health information (Bansal et al. 2010).

Drawing on the APCO model (Smith et al. 2011), we argue that risk-focused privacy awareness-raising measures increase privacy concerns as individuals become more conscious of potential privacy threats and their negative consequences. Thus, we propose the following hypothesis:

Hypothesis 6. Risk-focused awareness-raising increases privacy concerns.

Privacy Self-Efficacy

Self-efficacy leads individuals to judge themselves competent to perform a certain task (Akhter 2014; Menard et al. 2017). High levels of self-efficacy positively influence behavioral intentions and the motivation to mobilize resources to be successful (Akhter 2014; Milne et al. 2009; Rippetoe and Rogers 1987). When confronted with obstacles, individuals with high self-efficacy will be more likely to search for alternative ways to reach their goals (Locke and Latham 2002). By contrast, low levels of self-efficacy lead to avoidance of certain behaviors, since individuals lack the confidence that they can be successful. Individuals with low self-efficacy will stay with the status quo even when presented with better alternatives (Seltzer 1983).

The concept of self-efficacy can be applied to different situations (Bandura 2001). For instance, self-efficacy can support individuals' beliefs that they can manage risks and threats in risky situations (Rippetoe and Rogers 1987). Prior research identifies self-efficacy as a decisive factor in the behavior that individuals adopt when coping with risks (Rimal 2000). As the disclosure of personal health information is an inherently risky situation that can have profound social and economic consequences for the individual (Acquisti et al. 2015), privacy self-efficacy affects data protection behavior (Crossler and Bélanger 2019).

Following the notions of social cognitive theory (Bandura 2001), an increase in individuals' confidence in their ability to protect their personal health information from data misuse leads to an increase in their effort to protect their data privacy (Menard et al. 2017; Milne et al. 2009). Thus, privacy self-efficacy increases success rates in protecting data privacy. The success triggers positive emotions, which in turn, increases privacy self-efficacy. This cause-effect relationship results in a self-fulfilling prophecy.

As the APCO model of Smith et al. (2011) does not account for privacy self-efficacy, we combine the APCO model with social cognitive theory (Bandura 2001) by adding privacy self-efficacy to the level of privacy concerns. Hence, we propose:

Hypothesis 7. Privacy self-efficacy increases privacy protection.

Privacy Concerns

Privacy concerns are instances of anxiety about data privacy violations (Dinev and Hart 2006; Malhotra et al. 2004; Stewart and Segars 2002). Thus, privacy concerns are directly related to risk perceptions regarding the sharing of personal data. In line with prior research (e.g., Sheehan and Hoy 2000; Wirtz et al. 2007; Youn 2009), the APCO model suggests that privacy concerns increase privacy protection, as negative feelings of being at risk of data misuse motivate individuals to protect their personal data (Smith et al. 2011). Since individuals avoid risky situations by nature, privacy concerns trigger risk-reducing behaviors (Anderson and Agarwal 2011).

We draw on the APCO model to examine the relationship between privacy concerns and privacy protection in developing countries. Contextual differences significantly influence privacy-related behavior (Belanger and Crossler 2011; Belanger and Xu 2015; Gebre-Mariam and Bygstad 2019). In particular, low privacy education and late information technology dissemination affect privacy protection behavior in less-developed countries (Harris et al. 2013; Kumaraguru and Cranor 2005). Moreover, we expect that the sensitive nature of personal health information attenuates the relationship between privacy concerns and privacy protection. Acknowledging these context specifics, we propose the following hypothesis:

Hypothesis 8. Privacy concerns increase privacy protection.

Figure 1 depicts our conceptual model with the derived hypotheses.

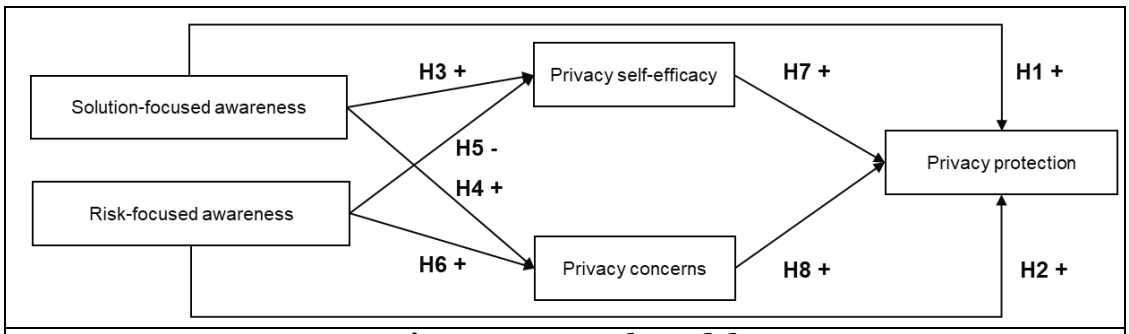


Figure 1. Research Model

Method

Experimental Design

In collaboration with eHealth Africa, a non-governmental organization working on data-driven health solutions in West Africa, we conducted a randomized, controlled field experiment. eHealth Africa's mission is "to build stronger health systems through the design and implementation of data-driven solutions that respond to local needs and provide underserved communities with tools to lead healthier lives" (eHealth Africa 2019). As the implementation of their data-driven healthcare solutions requires the input of sensitive personal data, eHealth Africa seeks to gain insights into individuals' privacy-related behavior. Based in Northern Nigeria, eHealth Africa provided us with insights into local conditions and on-site support so that we were able to successfully create, implement, and conduct the field experiment.

The experiment consists of three connected components: An educating treatment, a paper-based questionnaire, and an explanation of the experimental setting. All documents and interactions were in English, the official language in Nigeria. As an introduction, we told participants that we were working on improvements in the healthcare situation based on data-driven solutions. We further claimed that the presented questionnaire aimed at creating a dataset of personal health information supporting the development of artificial intelligence solutions.

To draw causal inferences about the effects of awareness-raising measures, we implemented three different scenarios: (1) Solution-focused awareness-raising, (2) risk-focused awareness-raising, and (3) no awareness-raising, for a control group. We implemented the treatment conditions in the form of informational brochures educating respondents either on how to protect data (i.e., solution-focused awareness-raising) or on the detrimental consequences of data misuse (i.e., risk-focused awareness-raising). We chose to use brochures for two major reasons. First, the distribution of informational brochures constitutes a situation that could occur in reality; verisimilitude helps conceal the inner dynamics of the experiment. Second, brochures are easy-to-understand, clear, and compact. This is important, as participants tend not to read information presented to them if it will take too much time and energy (Malandrino et al. 2013).

The solution-focused awareness-raising brochure contained information on ways to protect personal information in data-driven environments. It provided participants with a five-step guide on how to increase their data privacy. This brochure further informed participants about the newly-implemented (2019) Nigeria Data Protection Regulation and the data privacy rights that it is intended to uphold. The second brochure, the risk-focused one, educated participants about how data can be misused and about the negative consequences that data misuse could have for the individuals' data privacy. It discussed a recent data fraud scandal in Nigeria in which large amounts of personal data have been misused by a private company. The control group did not receive a brochure. Even very basic definitions of privacy such as "privacy is the ability of the individual to control the terms under which personal information is acquired and used" (Culnan and Armstrong 1999, p. 105) are not neutrally framed but emphasize aspects of protecting privacy or the associated risks when disclosing personal information. As privacy can hardly be defined as a neutral construct free from any solution-focused or risk-focused aspects, we argue that a general brochure for the control group could have led to blurring boundaries between the effects of our treatments. We developed the brochures' content based on Pötzsch's (2009) privacy awareness definition.

We enhanced both treatment conditions with pictures and kept the designs as similar as possible to avoid any biases. Participants received the brochures along with the questionnaires. We distributed the brochures randomly across the participants, places, and dates of data collection to avoid sampling bias among the treatment conditions.

The questionnaire comprised two parts. In the first part, we asked participants to indicate their personal health information, including questions regarding their general state of health, health-related behavior, chronic diseases, sexual diseases, and information on their mental health. Furthermore, at the end of the first part, participants had to rate the five health categories by perceived data sensitivity. In the second part of the questionnaire, we asked participants questions that assessed privacy concerns and privacy self-efficacy, as well as further covariates and demographics.

To conduct the experiment in an ethically correct manner, we gave participants a note explaining the true purpose of the experiment after they had returned to us the sealed envelopes with the questionnaires. Based on this, participants had the opportunity to have their data deleted. However, no participant chose this option. We refined both the scenarios and the questionnaire by pretesting. As an incentive to participate, individuals received 500 Naira, which equaled approximately USD 1.38 at the time of the experiment.

Operationalization of Variables

Dependent variable. We measured *privacy protection* through opt-out. The variable comprises the denial of the use of their provided data for further purposes. At the beginning of the questionnaire, we gave the participants the opportunity to tick a box saying: "I want my data only to be used for the purpose of this project and not for other purposes." We argue that this measure of privacy protection behavior is suitable as individuals had to answer sensitive information regarding their personal health in the questionnaire. Thus, opt-out means that individuals do not allow the use of their data for further purposes and thereby protect their personal data. The variable *opt-out* was measured on a binary scale with 0 indicating no opt-out and 1 indicating opt-out. The participants returned the questionnaire in a closed envelope, as a lack of anonymity could have biased the participants' data protection behavior.

Independent variables. We measured *solution-focused awareness-raising* and *risk-focused awareness-raising* as two dichotomous variables that derive from our experimental setting. They have a value of 1 if participants received a brochure with the respective treatment and 0 otherwise. Furthermore, we assessed the two mediating variables of *privacy concerns* and *privacy self-efficacy* in the questionnaire. We adapted the scale for privacy concerns from Dinev and Hart (2005). Three items asked participants if they were concerned that their disclosed information could be misused. We assessed privacy self-efficacy based on the scale of Cho et al. (2009). The six-item scale asked participants if they felt confident about protecting their information privacy. We assessed both privacy concerns and privacy self-efficacy on seven-point Likert scales ranging from 1, "strongly disagree," to 7, "strongly agree."

Control variables. The survey contained questions to assess further information on participants' personal backgrounds. Ethnically, Nigeria is one of the most diverse countries on earth. As culture is an antecedent of privacy protection behavior (Lowry et al. 2011; Smith et al. 2011), we asked participants to indicate their ethnic group. Moreover, following the APCO model, demographic factors play roles in individuals' privacy-related behavior. Therefore, we asked participants to indicate their age in years, their gender, and the number of years they had attended school.

Data Collection

The experiment was conducted in November 2019 in Nigeria. We chose Nigeria for three major reasons. First, Nigeria is a developing country, which is the prerequisite to answer our research question. Second, as English is the official language in Nigeria, we could keep the scales close to the original wording. Third, even though Nigeria has no principal data protection law, the country launched the Nigeria Data Protection Regulation in January 2019. This act has introduced initial compliance obligations on Nigerian companies to safeguard individuals' rights to data privacy (NIDTA 2019). We conducted our randomized controlled field experiment at several public places in Nigeria. Our target group was the Nigerian adult population. Our final sample comprises information from 382 individuals.

Analysis and Model Robustness

As *opt-out* is a binary variable, we applied logistic regression. We bootstrapped the regression analyses with 5,000 replications (Hayes 2015). We applied heteroscedasticity robust standard errors. To ensure the robustness of our research design and methodology, we took several conceptual and methodological steps.

First, our field experimental design provides a real-world setting that gives insights into actual privacy protection behavior of the relevant target group. By manipulating risk- and solution-focused awareness-raising, we were able to observe causal effects between our independent and dependent variables. Second, the rating of the five health categories by perceived data sensitivity showed that individuals actually perceived the data they provided in the questionnaire as sensitive. If they would not perceive the data as sensitive at all, our measure of privacy protection would be questionable. Third, we conducted the experiment using small groups. Thereby, we were able to ensure that participants received and read the brochures carefully before filling out the form. This is a prerequisite for our manipulations to work. Fourth, we included several demographic variables such as age, gender, ethnic group, and education as controls to avoid potential omitted variable bias. However, additional analyses revealed that the effects of solution-focused awareness and risk-focused awareness on privacy protection would remain virtually the same without the controls.

Results

Descriptive Results

Our dataset includes individuals between the age of 18 and 48 years. The gender distribution is approximately 2/3 men. Our sample comprises data of individuals from over 12 different ethnic groups. The demographic statistics among the two treatment conditions and the control group are comparable, indicating that the randomization procedure worked well. Of the total sample, 176 (46 %) participants chose to opt-out while 206 (54 %) participants allowed the use of their data for further purposes and thus did not opt-out. On average individuals rated the data they provided in the questionnaire as moderately sensitive with 4.1 on a scale from 1 to 7. The scales for privacy self-efficacy and privacy concerns performed well with Cronbach's alpha values of 0.86 and 0.72, respectively.

Results from Regression Analysis

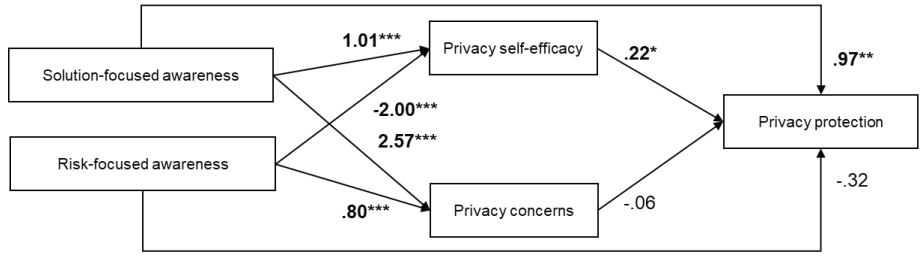
In Hypotheses 1 and 2, we examine the direct effects of solution-focused and risk-focused awareness-raising on privacy protection behavior. Our results show that solution-focused awareness-raising measures increase opt-out rates significantly at the one percent level (coefficient .97; p = .0033). Therefore, Hypothesis 1 is supported. The regression results do not support Hypothesis 2, as we could not find a significant effect of risk-focused awareness-raising on privacy protection behavior. Hypothesis 3 suggests that solution-focused awareness-raising increases privacy self-efficacy. Our results support this hypothesis, revealing a significant positive effect (coefficient = 1.01; p = .0000). In Hypothesis 4, we argue that solution-focused awareness-raising increases privacy concerns. Our conceptual model supports Hypothesis 4 at the 0.1 percent significance level (coefficient = 2.57; p = .0000).

Hypotheses 5 and 6 suggest that risk-focused awareness-raising decreases privacy self-efficacy and increases privacy concerns. Our analyses support both hypotheses, with significant regression coefficients of -2.00 (p = .0000) and 0.80 (p = .0005), respectively. Hypotheses 7 and 8 derive the effects of privacy self-efficacy and privacy concerns on individuals' privacy protection. Hypothesis 7 suggests that privacy self-efficacy increases privacy protection in terms of opt-out rates. The results support Hypothesis 7 at the five percent level (coefficient = .22; p = .0169). Hypothesis 8 suggests that privacy concerns increase privacy protection. Our findings do not support the proposed effect on opt-out rates (coefficient -.06; p = .4070).

Table 1 and Figure 2 depict the results of the conceptual model.

Table 1. Regression Analysis			
	Privacy protection	Privacy self-efficacy	Privacy concerns
Solution-focused awareness	**.97 (.33)****	**1.01 (.13)*****	**2.57 (.17)*****
Risk-focused awareness	-.32 (.34)	**-2.00 (.16)*****	**.80 (.23)*****
Privacy self-efficacy	**.22 (.09)***		
Privacy concerns	-.06 (.07)		
Age	.04 (.03)	-.03 (.03)	-.01 (.02)
Gender	.00 (.24)	.31 (.13)*	.19 (.18)
Ethnic group	.02 (.02)	-.03 (.01)*	.02 (.02)
Education	-.02 (.06)	.09 (.04)*	.06 (.05)
R^2	McFadden R^2 .09	.47	.34
Subjects	382	382	382

Note. Heteroscedasticity-robust standard errors are reported in parentheses. The results of the logistic regression on opt-out rates are reported in the log-odds metric. Results are bootstrapped with 5,000 replications. * p < .05, two-tailed test, ** p < .01, two-tailed test, *** p < .001, two-tailed test.



Note. Significant effects in the hypothesized direction are written in bold. Results are bootstrapped with 5,000 replications. Results are controlling for age, sex, ethnic group, and education. * p < .05, two-tailed test, ** p < .01, two-tailed test, *** p < .001, two-tailed test.

Figure 2. Results of the Conceptual Model

Post-hoc Analysis

To enhance our understanding of the mechanisms behind the effects of solution-focused and risk-focused awareness-raising on opt-out, we conduct binary mediation analysis. Following the APCO model of Smith et al. (2011), privacy awareness affects privacy protection through privacy concerns, as individuals become more aware of potential risks and threats regarding their information privacy and are thus more likely to protect their data. Distinguishing between solution-focused and risk-focused awareness-raising measures, we contribute to the theoretical underpinnings of the APCO model by arguing that privacy awareness affects privacy protection through privacy self-efficacy as well.

Applying 95% confidence intervals, the results of the binary mediation analyses reveal a significant positive indirect effect of solution-focused awareness-raising on opt-out through privacy self-efficacy (coefficient = .22; CI = .04|.45). The indirect effect of solution-focused awareness-raising on opt-out through privacy concerns is not significant. For the mediation analysis of risk-focused awareness-raising on opt-out, our results show a significant negative indirect effect through privacy self-efficacy (coefficient = -.43.; CI = -.96|-.07). However, we did not find a significant mediation of risk-focused awareness-raising on opt-out through privacy concerns. Table 2 depicts the results of the binary mediation analyses with the respective confidence intervals and bootstrapped standard errors.

Table 2. Binary-Mediation Analyses								
IV	Solution-focused awareness		Solution-focused awareness		Risk-focused awareness		Risk-focused awareness	
Mediator	Privacy self-efficacy		Privacy concerns		Privacy self-efficacy		Privacy concerns	
	Obs. Coeff.	*95% CI*	Obs. Coeff.	*95% CI*	Obs. Coeff.	*95% CI*	Obs. Coeff.	*95% CI*
Indirect	.22 (.11)	[.04|.45]	-.15 (.20)	[-.58|.22]	-.43 (.23)	[-.96|-.07]	-.05 (.07)	[-.20|.07]
Direct	.97 (.33)	[.32|1.61]	.97 (.33)	[.32|1.61]	-.32 (.34)	[-.99|.34]	-.32 (.34)	[-.99|.34]

Note. The dependent variable is opt-out. Standardized bootstrap results with 5,000 replications are reported. Bootstrap standard errors are reported in parentheses. The abbreviation CI stands for the confidence interval.

Discussion

Privacy awareness. In line with the APCO model (Smith et al. 2011), our results show that privacy awareness is a key antecedent of individuals' privacy-related attitudes and behaviors. Our results show that solution-focused awareness-raising measures increase opt-out rates significantly. Our solution-focused awareness-raising treatment educated individuals about ways to protect their personal information. The increased awareness of countermeasures resulted in individuals actively refusing to allow their data to be used for further purposes. In contrast to solution-focused awareness-raising, our results do not indicate significant direct effects of risk-focused awareness-raising on privacy behavior. Educating individuals about the negative consequences of data disclosure seems to trigger a feeling of helplessness and discourages individuals from protecting their data privacy. Social cognitive theory holds explanatory approaches for this mechanism. While verbally persuading people that they can master a task increases their self-efficacy, verbally persuading people that dangers are present can decrease their self-efficacy (Bandura 2001).

Moreover, we show that solution-focused awareness-raising increases privacy self-efficacy. When individuals learn how they can protect their data, they gain confidence in counteracting potential privacy risks. Particularly in developing countries, individuals lack basic privacy-related education (Harris et al. 2013). Therefore, we argue that even simple educational measures can make a difference in individuals' privacy protection. In addition to the positive effect on privacy self-efficacy, solution-focused awareness-raising increases privacy concerns. We argue that even though solution-focused awareness-raising increases knowledge about data protection, it also raises awareness about privacy issues, leading to an increase in privacy concerns.

In line with the APCO model (Smith et al. 2011), our results further show that the risk-focused educational measure makes individuals more aware of risks and threats when sharing their data, leading to an increase in privacy concerns. The mediation analysis reveals that risk-focused awareness-raising does not increase privacy protection through privacy concerns. However, we found a negative indirect effect of risk-focused privacy awareness on privacy protection through privacy-self efficacy. Applying Bandura's (2001) social cognitive theory to the privacy context, negative emotions regarding data privacy decrease individuals' beliefs that they can be successful in protecting their privacy, which in turn decreases their effort and motivation to protect their data. We argue that risk-focused privacy awareness triggers these negative emotions, as it reduces individuals' beliefs that they can successfully protect their privacy. Thus, even though we did not find a direct effect of risk-focused awareness-raising on privacy protection, there is a significant indirect effect showing that risk-focused awareness-raising decreases privacy protection because privacy-self efficacy decreases.

Privacy concerns. Our experiment yields a counter-intuitive result for privacy concerns. The effects of privacy concerns on opt-out do not support our theorizing. This result contradicts a large body of literature suggesting a positive relationship between privacy concerns and privacy protection behavior (e.g., Akhter 2014; Anderson and Agarwal 2011; Bansal et al. 2010; Chellappa and Sin 2005; Dinev and Hart 2005, 2006; Youn 2009). Two lines of reasoning help explain the contradiction. First, we argue that the counterintuitive result can be attributed to the context of healthcare in developing countries. The privacy calculus suggests that individuals conduct a risk-benefit assessment. If the benefits exceed the risks of data sharing, individuals disclose their personal information (Culnan and Armstrong 1999; Dinev and Hart 2006). Developing countries like Nigeria face a clear need for healthcare improvements. Thus, even though the participants of our study exhibit privacy concerns, the high benefits that go along with improvements in the overall healthcare situation outweigh these concerns (Chen 2018; Dienlin and Metzger 2016). Second, most prior studies apply survey designs and examine behavioral intention or stated attitude as outcome variables. However, the privacy paradox notes discrepancies between privacy concerns and actual behavior. Literature examining actual behavior shows that individuals often act against their intentions and disclose data even in the presence of privacy concerns (Kokolakis 2017; Norberg et al. 2007).

Privacy self-efficacy. In line with recent literature (e.g., Crossler and Bélanger 2019), we show a significant positive effect of privacy self-efficacy on privacy protection. Our results reveal that an increase in privacy self-efficacy leads to an increase in opt-out rates. Privacy self-efficacious individuals have the feeling that they can manage their personal data. Following social cognitive theory, individuals with high self-efficacy show higher motivation and effort toward the respective behavior (Bandura 2001). The positive significant effect of privacy self-efficacy on opt-out reflects this cognitive mechanism.

Theoretical Implications

Our study contributes to privacy-related information systems research in several ways. First, we examine the role of privacy awareness. Developing countries suffer from a widespread lack of privacy-related education, leading to misconceptions about risks and costs of data sharing (Cho et al. 2009; Dommeyer and Gross 2003; Kumaraguru and Cranor 2005). To understand how privacy awareness influences data protection, we assess the effects of solution-focused and risk-focused awareness-raising measures on privacy-related attitudes and behavior. Deuker (2010) suggests that viewing privacy awareness only in a risk-focused way is not conducive to success. Rather, it is necessary to extend the conceptualization of privacy awareness from a risk-focused toward a solution-based view (Deuker 2010). We argue that the basic idea behind this dual perspective is also reflected in the distinction between coping and threat appraisal process suggested by the protection motivation theory (Rogers 1975). Our results support recent comments on the high relevance of privacy awareness (e.g. Correia and Compeau), however, we show that the effects of privacy awareness-raising measures strongly depend on the conceptualization and implementation in practice. Privacy awareness has not received much attention from prior information systems scholars, which is particularly surprising given its high relevance for research and practice (Smith et al. 2011). We extend the theoretical understanding by showing that positive awareness-raising measures are effective in shaping individuals' privacy-related behavior.

Second, we take an integrational theoretical perspective by combining social cognitive theory (Bandura 2001) with the APCO model (Smith et al. 2011). Social cognitive theory assumes that individuals who believe in their ability to be successful in a certain situation show higher effort toward the respective behavior (Bandura 2001). We show that privacy self-efficacy is a decisive factor for individuals' privacy behavior. Individuals' confidence levels in privacy protection are directly associated with privacy protection responses. Our integrational approach enhances the explanatory power of the APCO model by integrating two largely contrasting psychological constructs: While privacy concerns refer to a feeling of helplessness, privacy self-efficacy addresses the opposite, dealing with the self-confidence of individuals to be able to protect their personal data efficiently. A key insight from our study for the interpretation of past and future research is therefore that privacy concerns matter, but not in all contexts and not exclusively because other psychological constructs such as privacy self-efficacy play a major role in individuals' privacy-related decision-making.

Third, we examine privacy protection against the background of a developing country. As prior information systems research mainly used US samples, developing countries have received limited attention (Belanger and Crossler 2011; Chen 2018; Chen and Zahedi 2016; Gebre-Mariam and Bygstad 2019). However, contextual and cultural differences are central to understanding privacy-related behavior (Bansal et al. 2016; Kokolakis 2017; Lowry et al. 2011; Smith et al. 2011). Prior research from developed countries identified privacy concerns as the core antecedent of privacy protection (Smith et al. 2011). Our results show that existing findings do not necessarily hold for developing countries. Following our extended APCO model, we find that privacy self-efficacy plays a major role in privacy protection behavior in developing countries like Nigeria.

Managerial Implications

Our findings yield valuable implications for governments and organizations to support awareness-based implementation of data-driven health solutions in developing countries. The dissemination of health information systems in developing countries contributes to the political vision of promoting equity in access to health services. However, these advancements involve significant amounts of sensitive personal health information. A profound understanding of individuals' risk-coping behaviors concerning the protection of personal health information is thus central to align the interests of users and providers. Our paper shows that findings cannot be transferred directly between different contexts. Therefore, we encourage policymakers and practitioners to consider contextual characteristics when managing data privacy.

If general privacy awareness is lacking, individuals have no opportunity to make sound decisions regarding their data privacy (Harris et al. 2013). Our experiment shows that increasing privacy awareness does not necessarily require sophisticated training. Even simple brochures can provide effective educational content. This measure is particularly conductive to success in fields where there is no mass of flyers and other information material, as it was the case in our experimental setting and is often the case in developed

countries. With comparably little financial resources, awareness-raising measures can support individuals in an educated decision-making process.

Having said that, our study shows that governments and organizations should pay attention to the specific type and tone of message implementation, as solution-focused and risk-focused awareness-raising measures trigger different cognitive mechanisms and behavioral responses. While risk-focused awareness-raising measures reduce privacy self-efficacy and do not directly affect privacy protection, solution-focused measures increase privacy self-efficacy and support privacy protection. As risk-focused awareness-raising has been more prominent so far, we argue that the media, organizations, and governments should rather emphasize solution-focused awareness-raising measures that convince individuals of their abilities to counteract privacy threats. These educational measures, however, require constant updates, given the rapid technological advancements and ever-increasing privacy threats (Milne et al. 2009).

Even though our results do not show significant effects of privacy concerns on privacy protection, we point out that the importance of privacy concerns should not be underestimated. The existence and clear communication of privacy concerns among the general population is critical to move policymakers toward implementing adequate data protection regulations (Correia and Compeau 2017). This applies particularly to developing countries, where sound privacy policies are often lacking and data protection rates are low.

Limitations and Future Research

This study has some limitations that offer opportunities for future research. First, using a Nigerian sample, our results show that even simple awareness-raising measures can make a difference for privacy-related attitudes and behaviors. These effects, however, could have been influenced by contextual and cultural specifics of our experimental setting. We call for future research examining the effectiveness of solution-focused and risk-focused awareness-raising measures in countries where privacy education is more prevalent. Second, country-level differences could explain our counter-intuitive finding of the insignificant effect of privacy concerns on opt-out (Acquisti et al. 2015). We suggest that the high need for healthcare improvements in countries like Nigeria outweighs privacy concerns. As our study does not provide empirical evidence for this line of argumentation, future research should investigate whether country-level differences or other situational factors influence the relationship between privacy concerns and opt-out. Third, healthcare professionals, research organizations, governments, and insurers are all potential providers of data-driven healthcare solutions. Our experimental setting told participants that their health information was requested by a university. Prior literature has found that privacy-related behavior changes when the requesting stakeholder changes (Anderson and Agarwal 2011). The different attitudes toward the various stakeholders are likely due to varying levels of trust and perceptions of corruption in each country about each stakeholder. As prior findings are not directly transferable between countries, we call for future studies to shed light on the role of the requesting stakeholder for privacy-related behavior in developing countries. Fourth, different types of information lead to differences in data protection. Health data is among the most sensitive type of data (Bansal et al. 2010). Therefore, our results are comparably conservative and should hold for settings that involve less-sensitive data. In line with recent studies (Chen 2018; Dienlin and Metzger 2016), we argue that perceptions of benefits are critical for individuals' privacy protection decisions. The question remains if the proposed cognitive mechanisms also hold for other settings that imply different benefits for the individuals.

Conclusion

The rapid progress and high potential of health information technology collide with poor privacy awareness in developing countries. Despite its high relevance, the topic of data protection in developing countries has been widely neglected by prior research. To support educated decision-making in data-driven environments, our experiment addressed the question of how privacy awareness affects privacy protection. In cooperation with eHealth Africa, a non-governmental organization working on data-driven health solutions, we conducted a randomized controlled field experiment in Nigeria. Our study extends the theoretical understanding of privacy protection and challenges the findings of related studies against the background of developing countries.

We combine the APCO model (Smith et al. 2011) with Bandura's (2001) social cognitive theory to examine the cognitive mechanisms behind the effects of solution-focused and risk-focused awareness-raising on

privacy protection. Our results provide evidence that even simple awareness-raising measures significantly influence privacy-related attitudes. However, they make a difference for individuals' privacy protection only when the educational measures are framed in a way that focusses on solutions instead of privacy risks. We identify contextual and conceptual boundary conditions for the theoretical mechanisms predicted by our extended APCO model. We hope our findings motivate future researchers to conduct further in-depth and context-sensitive analyses of privacy awareness and associated behavioral responses.

References

Acquisti, A. 2004. "Privacy in electronic commerce and the economics of immediate gratification," in *Proceedings of the 5th ACM conference on Electronic Commerce – EC '04*, J. Breese, J. Feigenbaum and M. Seltzer (eds.), New York, NY, USA. 17.05.2004 - 20.05.2004, New York, New York, USA: ACM Press, pp. 21-29.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, (347:6221), pp. 509-514.

Acquisti, A., and Grossklags, J. 2005. "Economics of information security – Privacy and rationality in individual decision making," *IEEE Security & Privacy* (January/February), pp. 24-30.

Akhter, S. H. 2014. "Privacy concern and online transactions: The impact of internet self-efficacy and internet involvement," *Journal of Consumer Marketing* (31:2), pp. 118-125 (doi: 10.1108/JCM-06-2013-0606).

Anderson, C., Baskerville, R. L., and Kaul, M. 2017. "Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information," *Journal of Management Information Systems* (34:4), pp. 1082-1112 (doi: 10.1080/07421222.2017.1394063).

Anderson, C. L., and Agarwal, R. 2011. "The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information," *Information Systems Research* (22:3), pp. 469-490 (doi: 10.1287/isre.1100.0335).

Angst, C. M., and Agarwal, R. 2009. "Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion," *MIS Quarterly* (33:2), pp. 339-370.

Avgerou, C., Hayes, N., and La Rovere, R. L. 2016. "Growth in ICT uptake in developing countries: New users, new uses, new challenges," *Journal of Information Technology* (31:4), pp. 329-333 (doi: 10.1057/s41265-016-0022-6).

Baek, Y. M. 2014. "Solving the privacy paradox: A counter-argument experimental approach," *Computers in Human Behavior* (38), pp. 33-42.

Bandura, A. 2001. "Social Cognitive Theory: An Agentic Perspective," *Annual Review of Psychology* (52:1), pp. 1-26.

Bandura, A. 2008. "An agentic perspective on positive psychology," *Positive Psychology* (1), pp. 167-196.

Bansal, G., Zahedi, F. M., and Gefen, D. 2010. "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems* (49:2), pp. 138-150 (doi: 10.1016/j.dss.2010.01.010).

Bansal, G., Zahedi, F. M., and Gefen, D. 2016. "Do context and personality matter? Trust and privacy concerns in disclosing private information online," *Information & Management* (53:1), pp. 1-21 (doi: 10.1016/j.im.2015.08.001).

Belanger, F., and Crossler, R. E. 2011. "Privacy in the digital age: A review of information privacy research in Information Systems," *MIS Quarterly* (35:4), pp. 1017-1041.

Belanger, F., and Xu, H. 2015. "The role of information systems research in shaping the future of information privacy," *Information Systems Journal* (25:6), pp. 573-578 (doi: 10.1111/isj.12092).

Braa, J., Monteiro, E., and Sahay, S. 2004. "Networks of action: Sustainable health information systems across developing countries," *MIS Quarterly* (28:3), pp. 337-362.

Cespedes, F. V., and Smith, H. J. 1993. "Database marketing: New rules for policy and practice," *MIT Sloan Management Review* (34:4), p. 7.

Chellappa, R. K., and Sin, R. G. 2005. "Personalization versus privacy: An empirical examination of the online consumer's dilemma," *Information Technology and Management* (6:2-3), pp. 181-202.

Chen, H.-T. 2018. "Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management," *American Behavioral Scientist* (62:10), pp. 1392-1412.

Chen, Y., and Zahedi, F. M. 2016. "Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China," *MIS Quarterly* (40:1), pp. 205-222 (doi: 10.25300/MISQ/2016/40.1.09).

Chen, Y. D., Brown, S. A., Hu, P. J. H., King, C. C., and Chen, H. 2015. "Managing emerging infectious diseases with information systems: reconceptualizing outbreak management through the lens of loose coupling," *Information Systems Research* (22), pp. 447-468.

Cho, H., Rivera-Sánchez, M., and Lim, S. S. 2009. "A multinational study on online privacy: Global concerns and local responses," *New Media & Society* (11:3), pp. 395-416 (doi: 10.1177/1461444808101618).

Cichy, P., Salge, T.-O., and Kohli, R. 2014. "Extending the privacy calculus: The role of psychological ownership," pp. 1-19. *International Conference on Information Systems* (ICIS), 2014.

Correia, J., and Compeau, D. 2017. "Information privacy awareness (IPA): A review of the use, definition and measurement of IPA," *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Crossler, R. E., and Bélanger, F. 2019. "Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap," *Information Systems Research* (30:3), pp. 995-1006 (doi: 10.1287/isre.2019.0846).

Culnan, M. J. 1995. "Consumer awareness of name removal procedures: Implication for direct marketing," *Journal of Interactive Marketing* (9), pp. 10-19.

Culnan, M. J., and Armstrong, P. K. 1999. "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science* (10:1), pp. 104-115.

Culnan, M. J., and Bies, R. J. 2003. "Consumer privacy: Balancing economic and justice considerations," *Journal of Social Issues* (59:2), pp. 323-342.

Deuker, A. 2010. "Addressing the privacy paradox by expanded privacy awareness – The example of context-aware services," in *Privacy and Identity Management for Life*, M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen and G. Zhang (eds.), Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 275-283.

Dienlin, T., and Metzger, M. J. 2016. "An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample," *Journal of Computer-Mediated Communication* (21), pp. 368-383.

Dinev, T., and Hart, P. 2005. "Internet privacy concerns and social awareness as determinants of intention to transact," *International Journal of Electronic Commerce* (10:2), pp. 7-29.

Dinev, T., and Hart, P. 2006. "An extended privacy calculus model for e-commerce transactions," *Information Systems Research* (17:1), pp. 61-80.

Dommeyer, C. J., and Gross, B. L. 2003. "What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies," *Journal of Interactive Marketing* (17:2), 34–51.

eHealth Africa 2019. *eHealth Africa*. https://www.ehealthafrica.org/our-mission-vision-values. Accessed 16 October 2019.

Fichman, R. G., Kohli, R., and Krishnan, R. 2011. "The role of Information Systems in healthcare: Current research and future trends," *Information Systems Research* (22:3), pp. 419-428.

Gebre-Mariam, M., and Bygstad, B. 2019. "Digitalization mechanisms of health management information systems in developing countries," *Information and Organization* (29:1), pp. 1-22.

Harris, A., Goodman, S., and Traynor, P. 2013. "Privacy and security concerns associated with mobile money applications in Africa," *Washington Journal of Law, Technology & Arts* (8:3), pp. 245-264.

Hayes, A. F. 2015. *Introduction to Mediation, Moderation, and Conditional Process Analysis*: *A Regression-Based Approach*, New York, NY: The Guilford Press.

Källander, K., Tibenderana, J. K., Akpogheneta, O. J., Strachan, D. L., Hill, Z., Asbroek, A. H. A. T., Conteh, L., Kirkwood, B. R., and Meek, S. R. 2013. "Mobile Health (mHealth) approaches and lessons for increased performance and retention of community health workers in low- and middle-income countries: A review," *Journal of Medical Internet Research* (15:1), e17 (doi: 10.2196/jmir.2130).

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., and Abdullat, A. 2015. "The role of mobile-computing self-efficacy in consumer information disclosure," *Information Systems Journal* (25:6), pp. 637-667.

Kokolakis, S. 2017. "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security* (64), pp. 122-134 (doi: 10.1016/j.cose.2015.07.002).

Kumaraguru, P., and Cranor, L. (eds.) 2005. *Pricing and Disseminating Customer Data With Privacy Awareness*, Berlin, Heidelberg: Springer.

LaRose, R., and Rifon, N. J. 2007. "Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior," *Journal of Consumer Affairs* (41:1), pp. 127-149.
Lee, H. H., and Hill, J. T. 2013. "Moderating effect of privacy self-efficacy on location-based mobile marketing," *International Journal of Mobile Communications* (11:4), p. 330.
Locke, E. A., and Latham, G. P. 2002. "Building a practically useful theory of goal setting and task motivation: A 35-year odyssey," *American Psychologist* (57:9), p. 705.
Lowry, P. B., Cao, J., and Everard, A. 2011. "Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures," *Journal of Management Information Systems* (27:4), pp. 163-200 (doi: 10.2753/MIS0742-1222270406).
Malandrino, D., Scarano, V., and Spinelli, R. 2013. "Impact of privacy awareness on attitudes and behaviors online," *Science Journal* (2), pp. 65-82.
Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information Systems Research* (15:4), pp. 336-355.
Menard, P., Bott, G. J., and Crossler, R. E. 2017. "User motivations in protecting information security: Protection motivation theory versus self-determination theory," *Journal of Management Information Systems* (34:4), pp. 1203-1230 (doi: 10.1080/07421222.2017.1394083).
Milne, G. R., Labrecque, L. I., and Cromer, C. 2009. "Toward an understanding of the online consumer's risky behavior and protection practices," *Journal of Consumer Affairs* (43:3), pp. 449-473.
NIDTA 2019. *Nigeria Data Protection Regulation*. https://nitda.gov.ng/wp-content/uploads/2019/01/Nigeria%20Data%20Protection%20Regulation.pdf. Accessed 1 October 2019.
Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs* (41:1), pp. 100-126.
Ozdemir, Z. D., Smith, J. H., and Benamati, J. H. 2017. "Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study," *European Journal of Information Systems* (26:6), pp. 642-660 (doi: 10.1057/s41303-017-0056-z).
Pötzsch, S. 2009. "Privacy awareness: A means to solve the privacy paradox?" in *The Future of Identity in the Information Society*, V. Matyáš, S. Fischer-Hübner, D. Cvrček and P. Švenda (eds.), Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 226-236.
Rimal, R. N. 2000. "Closing the knowledge-behavior gap in health promotion: the mediating role of self-efficacy," *Health Communication* (12:3), pp. 219-237.
Rippetoe, P. A., and Rogers, R. W. 1987. "Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat," *Journal of Personality and Social Psychology* (52:3), p. 596.
Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, (91:1), pp. 93-114.
Seltzer, L. F. 1983. "Influencing the" shape" of resistance: An experimental exploration of paradoxical directives and psychological reactance," *Basic and Applied Social Psychology* (4:1), pp. 47-71.
Sheehan, K. B., and Hoy, M. G. 2000. "Dimensions of privacy concern among online consumers," *Journal of Public Policy & Marketing* (19), pp. 62-72.
Singer, N., and Wakabayashi, D. 2019. "Google to store and analyze millions of health records," *The New York Times* (ed.), New York, NY.
Smith, H. J., Dinev, T., and Xu, H. 2011. "Information privacy research: An interdisciplinary review," *MIS Quarterly* (35:4), pp. 989-1015.
Stewart, K. A., and Segars, A. H. 2002. "An empirical examination of the concern for information privacy instrument," *Information Systems Research* (13:1), pp. 36-49.
Venkatesh, V., Sykes, T. A., Rai, A., and Setia, P. 2019. "Governance and ICT4D initiative success: A longitudinal field study of ten villages in rural India," *MIS Quarterly* (43:4), pp. 1-24.
Wirtz, J., Lwin, M. O., and Williams, J. D. 2007. "Causes and consequences of consumer online privacy concern," *International Journal of Service Industry Management* (18:4), pp. 326-348.
World Health Organization 2005. "58th World Health Assembly Report," WHO, Geneva.
Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. 2009. "The role of push-pull technology in privacy calculus: The case of location-based services," *Journal of Management Information Systems* (26:3), pp. 135-174 (doi: 10.2753/MIS0742-1222260305).
Youn, S. 2009. "Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents," *Journal of Consumer Affairs* (43:3), pp. 389-418.