Technology in Society 41 (2015) 54–64

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

Using mobile devices in a high risk context: The role of risk and trust in an exploratory study in Afghanistan

Kent Marett [a, *], Allison W. Pearson [a], Rodney A. Pearson [a], Erich Bergiel [b]

[a] Department of Management & Information Systems, College of Business, Mississippi State University, Box 9581, MS 39762, USA
[b] Department of Management, Richards College of Business, University of West Georgia, Carrollton, GA 30118, USA

ARTICLE INFO

Article history:
Received 6 May 2014
Received in revised form 19 November 2014
Accepted 26 November 2014
Available online 12 December 2014

Keywords:
Mobile use
Risk
Trust
Perceived benefits
Afghanistan

ABSTRACT

Mobile phone adoption and use are common-place in the western world, yet still are associated with risks of loss of privacy and information security. However, in high-risk cultures and countries, such as those at war or threatened by terrorism, mobile phone adoption and benefits of use may be perceived quite differently. In this study, we use e-commerce and adoption theories to build a model of trust and risk as predictors of mobile use benefits in a sample of current mobile users in southern Afghanistan. The responses collected from a survey of over seven thousand Afghani citizens were used to test the research model. The results suggest that despite the potential danger, the mobile device owners who were surveyed perceived the benefits derived from use as being worthwhile. The results are discussed with implications for managers and practitioners provided.

1. Introduction

The vast majority of research on business communication, including research investigating adoption and use of communicative technology, has been conducted within highly-developed, stable, capitalist societies. In fact, most research assumes that individuals have free speech rights, basic safety, and protection of their lives and business provided by the government. As other researchers have pointed out [1,2], we know little of the day-to-day communicative practices of individuals located in less developed, unstable, high-risk societies, even individuals in those regions who are members of multinational firms. The Fund for Peace identifies 67 countries around the globe that fall into a high-risk context based on groups of citizens who are vengeance – seeking, struggling economic development, poverty, deteriorating government, and violations of human rights. In this study, we explore the fundamental risks and dangers associated with mobile technology usage in a high-risk environment, fraught with war, terrorism, physical violence, and extreme poverty. Given that internal communication between members of multinational corporations come under the same strains of violence, terrorist attacks, and the inability of government to protect its infrastructure as the rest of the citizenry located in those areas, how does our current understanding of communicative technology usage apply to high risk environments?

Earlier work in mobile networking has called for increased attention toward cultural differences and perceptions of mobile services [3]. One of the areas in which cultural differences may manifest is with perceptions of privacy and safety. In many parts of the world, mobile users may take for granted that cell networks are secure and that providers will protect one's privacy, while in other regions a lapse in privacy may affect one's personal safety. For example, during focus group interviews

* Corresponding author. +1 662 325 7001.
E-mail addresses: kmarett@business.msstate.edu (K. Marett), apearson@business.msstate.edu (A.W. Pearson), rpearson@business.msstate.edu (R.A. Pearson), ebergiel@westga.edu (E. Bergiel).

http://dx.doi.org/10.1016/j.techsoc.2014.11.002
0160-791X/

conducted with a wide range of mobile users in Scandanavia, North America, and Eastern Asia, vulnerabilities were described as one's losing a phone and losing touch with others, and privacy issues took the form of discussing sensitive topics in public places around random bystanders [4]. As past events have shown, mobile users in the Western world may have a false sense of security, and that in more unstable countries and contexts, risks of mobile use may greatly differ.

In this study, we focus on mobile users who have reason to believe their cellular service provider makes their personal information and privacy vulnerable. To our knowledge, the literature on security and privacy in a mobile environment primarily focuses on the endpoints of the communication. However, there is every reason to believe that the vulnerabilities to a user may lie within the network. Mobile users frequently roam through multiple cells during a connection to the network, making them susceptible to malicious or compromised cell domains with the potential of engaging in information theft and denial of service, among other threats [5]. Researchers have also documented the possibility of remotely draining the battery power of others' mobile devices through "ping-of-death" vulnerabilities in cellular networks [6]. Reports indicate that mobile users have been unknowingly monitored through the use of location-based services implemented on their devices [7]. However, a more likely threat to privacy lies within the network providers themselves. Social engineering attacks on service providers have exploited holes in security policies protecting mobile user accounts in North America and Europe [8,9]. The providers themselves may be intentionally responsible for security breaches, including those originating from employees within the company [10]. When trust in mobile service providers is breached, mobile use and benefits of mobile use may decline. These effects may be even more pronounced in high risk contexts.

2. Literature and theory review

The widespread adoption of mobile devices is said to be "volcanic" in developing countries [11]. However, in less affluent countries stricken with political instability, war, and terrorism, mobile technologies may have different implications toward usage. Conflicting pressures from countries who want to provide information access and external threats, such as terrorist groups, who seek to reduce or control information access, result in difficult initial decisions to adopt [12] for citizen mobile users. Nonetheless, the widespread adoption and use of mobile phones can be linked to societal change including economic growth, improved medical care, and reductions in poverty [13,14]. In developing nations and war-torn nations with limited communications infrastructure, there is a powerful need and desire for access to information by the citizenry, in spite of the risks (such as terrorism) associated with use. The perceived benefits of use of mobile technologies for access to people and information are likely strong drivers of user behavior. Yet, very little is known about the impact of external, violent threats with regard to information access on mobile usage, even though it is widely acknowledged that such violence hinders entire economies [12,15]. Indeed, the adoption of IT in emerging and dynamic domains is a relatively unexplored area of research [16]. The purpose of our study is to explore the benefits and risks of mobile phone use, in a high-risk context, based on a sample of mobile users in Southern Afghanistan – a region that is unstable and with ongoing terrorist threats and violence.

Afghanistan is one current example of a high risk context, as it is considered to have a government, the Taliban, that supports state-sponsored terrorist activities [17]. Under pressure and threats of violence from the Taliban, mobile service providers shut down mobile towers at night, often from 5:00pm – 8:00am, and in some rare cases, the signal may be available only 4 h per day [18]. The Taliban forces mobile providers to shut down towers by threatening physical violence and property destruction on both mobile employees and mobile providers who do not comply with their demands. A manager for one of the major mobile providers reported to the New York Times that unless the towers are shut down at night, the Taliban promises that "employees will be abducted, killed, and the towers will be burned," a threat that was realized when three cell towers in the Kapisa Province were bombed and destroyed [18]. The control of mobile signal access is reported to send a strong psychological message to Afghani citizens that the Taliban can have direct control over their future. Further, the mobile shut down also creates doubt about whether or not the Afghanistan government can protect citizens, further increasing the fear and anxiety of mobile users. In the next section, we build a theory base upon which to explore why, in spite of such high risk, mobile users in high risk contexts will still see benefits in use of mobile technologies.

2.1. Theory of risk and use of technology

Researchers in the technology adoption literature have pointed out, perceived risk of using a technology has often been overlooked or minimized in lieu of focusing on the benefits stemming from adoption e.g., [19,20]. These criticisms have led to the conclusion that the core model of adoption theory "has limited usefulness in the constantly evolving IT adoption context" [[21], p. 212]; however, they may be adapted to understand mobile use in high risk contexts. For consumers of mobile services, *perceived risk* is defined as the "uncertainty regarding possible negative consequences of using a product or service" [[19], p. 453]. Researchers have since theorized the integration of technology adoption models and risk theories to explain the likelihood of on-line adoption, mainly focusing on purchase intent of consumers. Perceived risk is most prevalent during the decision to adopt and use IT when feelings of uncertainty, discomfort, anxiety, and conflict exist within the user [19]. Risks perceived by technology users are often centered around possible task inefficiencies coupled with the risk of unsecured communication, potential loss of private information, and possible financial losses [22]. The basic assumption in the e-commerce literature is that system