Addressing the Credibility of Mobile Applications

Pankaj Kamthan
Concordia University, Canada

INTRODUCTION

Mobile access has opened new vistas for various sectors of society including businesses. The ability that anyone using (virtually) any device could be reached anytime and anywhere presents a tremendous commercial potential. Indeed, the number of mobile applications has seen a tremendous growth in the last few years.

In retrospect, the fact that almost *anyone* can set up a mobile application claiming to offer products and services raises the question of credibility from a consumer's viewpoint. The obligation of establishing credibility is essential for an organization's reputation (Gibson, 2002) and for building consumers' trust (Kamthan, 1999). If not addressed, there is a potential for lost consumer confidence, thus significantly reducing the advantages and opportunities the mobile Web as a medium offers. If a mobile application is not seen as credible, we face the inevitable consequence of a product, however functionally superior it might be, rendered socially isolated.

The rest of the article is organized as follows. We first provide the motivational background necessary for later discussion. This is followed by introduction of a framework within which different types of credibility in the context of mobile applications can be systematically addressed and thereby improved. Next, challenges and directions for future research are outlined. Finally, concluding remarks are given.

BACKGROUND

In this section, we present the fundamental concepts underlying credibility, and present the motivation and related work for addressing credibility within the context of mobile applications.

Basic Credibility Concepts

For the purposes of this article, we will consider credibility to be synonymous to (and therefore interchangeable with) believability (Hovland, Janis, & Kelley, 1953). We follow the terminology of Fogg and Tseng (1999), and view credibility and trust as being slightly different. Since trust indicates a *positive* belief about a person, object, or process, we do not consider credibility and trust to be synonymous.

It has been pointed out in various studies (Fogg, 2003; Metzger, 2005) that credibility consists of two primary dimensions, namely *trustworthiness* and *expertise* of the source of some information. Trustworthiness is defined by the terms such as well-intentioned, truthful, unbiased, and so on. The trustworthiness dimension of credibility captures the *perceived* goodness or morality of the source. Expertise is defined by terms such as knowledgeable, experienced, competent, and so on. The expertise dimension of credibility captures the *perceived* knowledge and skill of the source. Together, they suggest that "highly credible" mobile applications will be perceived to have high levels of *both* trustworthiness and expertise.

We note that trustworthiness and expertise are at such a high level of abstraction that direct treatment of any of them is difficult. Therefore, in order to improve credibility, we need to find quantifiable attributes that can improve each of these dimensions.

A Classification of Credibility

The following taxonomy helps associating the concept of credibility with a specific user class in context of a mobile application. A user could consider a mobile application to be credible based upon direct interaction with the application (*active credibility*), or consider it to be credible in absence of any direct interaction but based on certain pre-determined notions (*passive credibility*). Based on the classification of credibility in computer use (Fogg & Tseng, 1999) and adapting them to the domain of mobile applications, we can decompose these further.

There can be two types of *active credibility:* (1) *surface credibility,* which describes how much the user believes the mobile application is based on simple inspection; and (2) *experienced credibility,* which describes how much the user believes the mobile application is based on first-hand experience in the past.

There can be two types of *passive credibility:* (1) *presumed credibility,* which describes how much the user believes the mobile application because of general assumptions that the user holds; and (2) *reputed credibility,* which describes how much the user believes the mobile application because of a reference from a third party.

Finally, credibility is not absolute with respect to users and with respect to the application itself (Metzger, Flanagin, Eyal, Lemus, & McCann, 2003). Also, credibility can be associated with a whole mobile application or a part of a mobile application. For example, a user may question the credibility of information on a specific product displayed in a mobile application. We contend that for a mobile application to be labeled non-credible, there must exist at least a part of it that is labeled non-credible based on the above classification by at least one user.

The Origins and Significance of the Problem of Mobile Credibility

The credibility of mobile applications deserves special attention for the following reasons:

- **Delivery Context:** Mobile applications are different from the desktop or Web environments (Paavilainen, 2002) where context-awareness (Sadeh, Chan, Van, Kwon, & Takizawa, 2003) is a unique challenge. The delivery context in a changing environment of mobile markup languages, variations in user agents, and constrained capabilities of mobile devices presents unique challenges towards active credibility.
- **Legal Context:** Since the stakeholders of a mobile application need not be co-located (different jurisdictions in the same country or in different countries), the laws that govern the provider and the user may be different. Also, the possibilities of fraud such as computer domain name impersonation (commonly known as "pharming") or user identity theft (commonly known as "phishing") with little legal repercussions for the perpetrators is relatively high in a networked environment. These possibilities can impact negatively on presumed credibility.
- **User Context:** Users may deploy mobile devices with varying configurations, and in the event of problems with a mobile service, may first question the provider rather than the device that they own. In order for providers of mobile portals to deliver user-specific information and services, they need to know details about the user (such as profile information, location, and so on). This creates the classical dichotomy between personalization and privacy, and striking a balance between the two is a constant struggle for businesses (Kasanoff, 2002). The benefits of respecting one can adversely affect the other, thereby impacting their credibility in the view of their customers. Furthermore, the absence of a human component from non-proximity or "facelessness" of the provider can shake customer confidence and create negative perceptions in a time of crisis such as denial of service or user agent crash. These instances can lead to a negative passive credibility.

Initiatives for Improving Mobile Credibility

There have been initiatives to address the credibility of Web applications such as a user survey to identify the characteristics that users consider necessary for a Web application to be credible (Fogg et al., 2001) and a set of guidelines (Fogg, 2003) for addressing *surface, experienced, presumed,* and *reputed credibility* of Web applications.

However, these efforts are limited by one or more of the following issues. The approach towards ensuring and/or evaluating credibility is not systematic, the proposed means for ensuring credibility is singular (only guidelines), and the issue of feasibility of the means is not addressed. Moreover, these guidelines are not specific to mobility, are not prioritized and the possibility that they can contradict each other is not considered, can be open to broad interpretation, and are stated at such a high level that they may be difficult to realize by a novice user.

ADDRESSING THE CREDIBILITY OF MOBILE APPLICATIONS

In this section, we consider approaches for understanding and improving active credibility of mobile applications.

A Framework for Addressing Active Credibility of Mobile Applications

To systematically address the active credibility of mobile applications, we take the following steps:

1. View credibility as a qualitative aspect and address it indirectly via quantitative means.
2. Select a theoretical basis for communication of information (semiotics), and place credibility in its setting.
3. Address semiotic quality in a practical manner.

Based on this and using the primary dimensions that affect credibility, we propose a framework for active credibility of mobile applications (see Table 1). The external attributes (denoted by E) are extrinsic to the software product and are directly a user's concern, while internal attributes (denoted by I) are intrinsic to the software product and are directly an engineer's concern. Since not all attributes corresponding to a semiotic level are at the same echelon, the different tiers are denoted by "Tn."