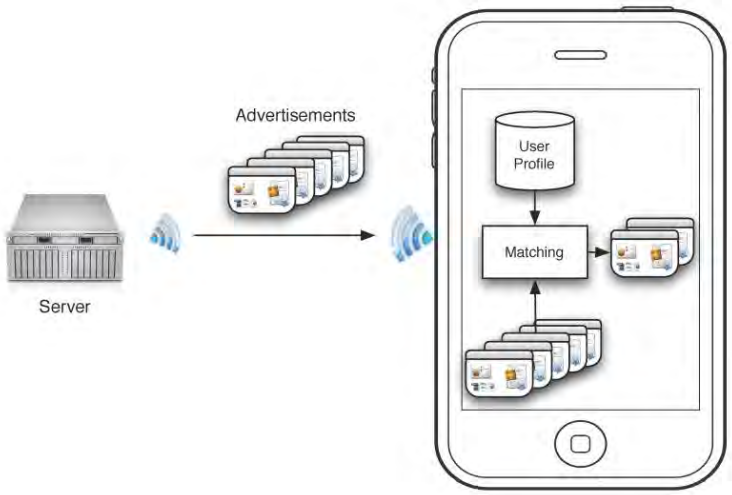
Project title: Designing Privacy-Safe Personalized Content Offering

Project summary:

IT-enabled personalization, while potentially making user-computing experience more gratifying, often relies heavily on user's personal information to deliver individualized services, so raises users' privacy concerns. We term the tension between personalization and privacy - which follows from marketers exploiting consumers' data to offer personalized product information - the personalization-privacy paradox.

To overcome the personalization-privacy paradox, we designed an IT solution - referred to as a personalized, privacy-safe application - that retains users' information locally on their IT devices while still providing them with personalized messages in an efficient manner. An important mechanism of the personalized, privacy-safe application is the short-lived agent, one of which is created for each message, containing details of the message (i.e., the content, the targeting rule, and the expiry date). Each agent is then cloned and broadcast to the IT devices of all consumers using the application - once delivered, the agent first retrieves the consumer's locally stored personal information and then matches the message' targeting rule to the consumer's profile, displaying the message only if the targeting rule matches the consumer's profile. Having completed this task, the agent expires and auto-deletes. The fact that the agent is 'short-lived' means marketers can only broadcast new messages to consumers, but cannot gain knowledge about their personal information.

Set in the context of personalized advertising applications for smartphones, we built and validated this technical solution through a field experiment. The architectural view of the personalized, privacy-safe application is shown in the figure below.



The personalized, privacy-safe application was benchmarked against two more conventional applications which we self-developed for the validation purpose: a base non-personalized application that broadcasts non-personalized product information to users; and a personalized, non-privacy safe application that transmits user information to a central marketer's server. The key performance indicators of such

advertising applications are the frequency of users launching the application, and the number of advertisements that users saved. The results showed that our proposed IT solution reduced users' perceptions of their information boundaries being intruded on, and significantly increased both key performance indicators, thus mitigating the personalization-privacy paradox.

This work clearly falls in the realm of design science, as it fits all three definitions provided in the appendix that emphasize the artifact's importance in organizational context. The supporting documents cover end-to-end design realization of the IT artifact, including the identification and statement of need, design principles of the artifact, real-life implementation of the artifact, and validation and evaluation of the feasibility and value of the artifact.

Verification:

The project is principally led and driven by university based faculty staffs for R&D purpose. The PhD. students involved in the artifact development have since graduated.

Supporting Documents

Journal Publication

Sutanto, Juliana; Palme, Elia; Tan, Chuan Hoo; Phang, Chee Wei. "Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users", *MIS Quarterly, forthcoming*

Patent

Palme, Elia; Gasimov, Anar; Sutanto, Juliana; Magagna, Fabio, "Method and Devices for Targeted Distribution of Data," *International Patent (PCT/EP2011/004190) pending, US Patent 20130212217 A1*

MIS Quarterly

RESEARCH ARTICLE

ADDRESSING THE PERSONALIZATION–PRIVACY PARADOX: AN EMPIRICAL ASSESSMENT FROM A FIELD EXPERIMENT ON SMARTPHONE USERS[1]

Juliana Sutanto
Department of Management, Technology, and Economics, ETH Zürich, Weinbergstrasse 56/58,
Zürich, SWITZERLAND {jsutanto@ethz.ch}

Elia Palme
Newscron Ltd., Via Maderno 24, Lugano, SWITZERLAND {elia.palme@newscron.com}

Chuan-Hoo Tan
Department of Information Systems, City University of Hong Kong, Tat Chee Avenue,
Kowloon, HONG KONG {ch.tan@cityu.edu.hk}

Chee Wei Phang
Department of Information Management and Information Systems, Fudan University, 670 Guoshun Road,
Shanghai, CHINA {phangcw@fudan.edu.cn}

Privacy has been an enduring concern associated with commercial information technology (IT) applications, in particular regarding the issue of personalization. IT-enabled personalization, while potentially making the user computing experience more gratifying, often relies heavily on the user's personal information to deliver individualized services, which raises the user's privacy concerns. We term the tension between personalization and privacy, which follows from marketers exploiting consumers' data to offer personalized product information, the ***personalization–privacy paradox****. To better understand this paradox, we build on the theoretical lens of uses and gratifications theory and information boundary theory to conceptualize the extent to which privacy impacts the process and content gratifications derived from personalization, and how an IT solution can be designed to alleviate privacy concerns.*

Set in the context of personalized advertising applications for smartphones, we propose and prototype an IT solution, referred to as a ***personalized, privacy-safe application****, that retains users' information locally on their smartphones while still providing them with personalized product messages. We validated this solution through a field experiment by benchmarking it against two more conventional applications: a base* ***non-personalized application*** *that broadcasts non-personalized product information to users, and a* ***personalized, non-privacy safe application*** *that transmits user information to a central marketer's server. The results show that (compared to the non-personalized application), while personalized, privacy-safe or not increased application usage (reflecting process gratification), it was only when it was privacy-safe that users saved product messages*

[1]Al Hevner was the accepting senior editor for this paper. Samir Chatterjee served as the associate editor.

The appendix for this paper is located in the "Online Supplements" section of the *MIS Quarterly*'s website (http://www.misq.org).

(reflecting content gratification) more frequently. Follow-up surveys corroborated these nuanced findings and further revealed the users' psychological states, which explained our field experiment results. We found that saving advertisements for content gratification led to a perceived intrusion of information boundary that made users reluctant to do so. Overall our proposed IT solution, which delivers a personalized service but avoids transmitting users' personal information to third parties, reduces users' perceptions that their information boundaries are being intruded upon, thus mitigating the personalization–privacy paradox and increasing both process and content gratification.

Keywords: Personalization–privacy paradox, mobile advertising applications, uses and gratifications, information boundary theory

Introduction

> *Although privacy often has been said to mean "the right to be left alone"….Consumers live in a world where information about their purchasing behavior, online browsing habits…is collected, analyzed, combined, used, and shared, often instantaneously and invisibly.* (Federal Trade Commission 2010, p. 1)

A December 2010 Federal Trade Commission (FTC) report highlighted a pertinent and ongoing issue confronting the information technology (IT) industry: the personalization–privacy paradox, the tension between how the developers and marketers of IT applications exploit users' information to offer them personalized services, and those users' growing concerns about the privacy of that information, which can restrain their use of such applications (Angst and Agarwal 2009; Dhar and Varshney 2011). Information privacy refers to users' rights "to keep information about themselves from being disclosed to others [marketers and other unknown people]" (Rognehaugh 1999, p. 125).

The personalization–privacy paradox can be prominently observed in the mobile application industry, especially since the emergence of smartphones[2] such as the iPhone (Kavassalis et al. 2003; Lee and Benbasat 2003; Watson et al. 2002). In addition to possessing typical mobile phone characteristics (being closely tied to their specific user, going where they go), the latest generations of smartphones are equipped with significantly improved processing capacity that approximates to that of a personal computer, and are therefore excellent tools via which marketers (i.e., merchants and advertising companies) can use mobile applications (widely known as "apps") to gather information about phone users, and then offer them personalized information and individually tailored services based on that information (Peppers and Rogers 1997; Stewart and Pavlou 2002; Xu et al. 2008). So it is not surprising that, despite their enhanced personalization features, these mobile applications have raised widespread concerns among users about the privacy of their personal information. A 2010 global survey by Accenture found that more than half of the 1,000 respondents (from more than 10 countries) surveyed were worried that smartphone-enabled mobile applications would erode their information privacy,[3] a concern reflected in a remark by Eswar Priyadarshan, the chief technology officer at Quattro Wireless:[4] "[Smartphone is] potentially a portable, personal spy." The recent news that iPhones and Android phones secretly track user information (Angwin and Valentino-DeVries 2011), and that half of all iPhone applications are capable of doing so (Hutchinson 2011), further confirms users' worries, and pressure has been mounting on mobile application developers to address information privacy issues in their application designs (Haselton 2012; Tode 2012).

However, addressing the information privacy issue is tricky, since phone personalization—a capability that users value—often involves the explicit utilization of information about them, which is at the root of their information privacy concerns, and about which the existing literature has offered conflicting views. While opinion polls, surveys, and experiments have repeatedly indicated privacy to be of the utmost concern to users (Culnan and Milne 2001; Fox 2000; Phelps et al. 2000), research has also suggested the impact of such con

[2]Ever since Apple introduced the iPhone in 2007, comparable smartphone products have fast become the norm for individual ownership, so that the smartphone user base is predicted to exceed USD 1.32 billion (Gartner 2009).

[3]Source: "Use of Smartphones by Bargain-Hunting Consumers is Changing the Customer-Retailer Relationship, Accenture Survey Finds," Accenture, December 6, 2012 (http://newsroom.accenture.com/article_display.cfm?article_id=5109; accessed May 5, 2011).

[4]Quattro Wireless was a mobile advertising agency that placed advertising for clients such as Sony on mobile sites (Clifford 2009). The company was acquired by Apple in January 2010 but was subsequently closed in favor of Apple's own iAd advertising platform.

cerns may be limited, in that people may be willing to forgo privacy in return for the advantages they enjoy from personalization (Hann et al. 2002). In addition, the measures currently proposed to address information privacy issues have not yet yielded satisfactory results. One such stream attempts to design security solutions, such as anonymizing techniques (e.g., Bulander et al. 2005; Gedik and Liu 2008) and peer-to-peer user agents (e.g., Brar and Kay 2004)—to ensure the transmission of user information over communication networks is properly handled, but these measures may appear strange or overly sophisticated to general computer users, so they are unwilling to adopt them, or unable to utilize them effectively (Jensen et al. 2005). Another group of measures provides written assurance regarding information collection and use, such as privacy policy statements (e.g., Andrade et al. 2002; Bargh et al. 2003; Xu et al. 2005; Youssef et al. 2005), but given the typical length and complexity of these assurances, these solutions have again been criticized as imposing unrealistic cognitive burdens on consumers, so that only very few of them consult such privacy policies (Jensen et al. 2005).[5] This discussion highlights the need for a better theoretical understanding about the personalization–privacy paradox, and the establishment of alternative measures to alleviate users' information privacy concerns effectively, while still allowing them to enjoy the benefits of personalization.

To understand this paradox better, we build on uses and gratifications theory (UGT) (McGuire 1974; Rubin 1985) and information boundary theory (IBT) (Petronio 1991). We anchor our considerations in UGT to underscore the need to consider two distinct types of gratification—process and content—that users derive from using a medium: the former relates to their enjoyment of the act of using the medium, while the latter reflects the pleasure they gain from using the content the medium offers (Lee 2001; Stafford et al. 2004). UGT suggests these types of gratification may be mediated by such social and psychological factors as users' desires and concerns, hence mediating how consumers' desires for personalization and concerns about information privacy influence their different gratifications. To specifically theorize about such relationships, we employ IBT to argue that individuals form informational spaces around themselves, which have defined boundaries (Petronio 1991; Stanton and Stam 2003), and attempts by external parties (e.g., marketers) to cross those boundaries may disturb them, making them feel anxious or uncomfortable (Solove 2006). We argue that personalization benefits will lead users to experience greater process gratification, but not greater content gratification, as the perceptions of information boundary penetration involved in the latter will raise significant privacy concerns.

Leading on from this argument, we propose and design an IT solution in a context which exemplifies the paradox: personalized mobile advertising applications.[6] The solution, which we refer to as *personalized, privacy-safe application*, stores and processes information locally (i.e., within a user's smartphone) but does not transmit it to the marketer, so that personalized product information (adverts) can be delivered to without compromising the privacy of personal information. We demonstrate empirically that such an IT solution can promote psychological comfort in users since their information boundaries are not violated, thus both enhancing the process gratification they can gain from mobile phone applications, and allowing them to enjoy the associated content gratification. We pilot-tested and then validated our proposed IT solution via a field experiment in which actual users received real advertising messages provided in collaboration with an advertising agency via the application. The experiment benchmarked our personalized, privacy-safe application against both a base mobile application (referred to as *non-personalized application*) that broadcast product information to users, and a personalized application (a *personalized, non-privacy safe application*) that transmitted user information to a central server (i.e., marketer) which then used it to deliver personalized adverts. We then conducted follow-up surveys that revealed users' privacy perceptions and psychological states that explained our field experiment observations.

The rest of the paper is organized thus: the next section reviews the prior studies on the personalization–privacy paradox. The subsequent section introduces the UGT and IBT. The following sections develop our hypotheses, document our field experiment, and report our hypothesis testing. We then present the post-experiment investigations that reveal more details about users' psychological states that explain our field experiment results more fully. The pentultimate section discusses our findings and draws some implications. Finally, we present our conclusions.

[5] Jensen et al.'s study found that only 26 percent of users read privacy policies during a laboratory experiment, and the readership in real situations is believed to be far lower.

[6] A mobile application is a software application that is developed to run on a mobile phone. The application is typically downloaded in a mobile application store (e.g., Apple App store). Mobile applications can serve many purposes such as social networking, location-based social marketing, and provision of information (e.g., news and weather forecast). A mobile advertising application is a specific type of mobile application that delivers advertisement information to users (e.g., adverts of a fashion brand, adverts from a particular store).

Prior Studies

The several prior studies which have examined the personalization–privacy paradox serve as the research foundation for this study. Table 1 summarizes the key extant studies and how they relate to our research. Our review highlights two issues. First, the theoretical interpretation of consumers' responses to information personalization and privacy issues is not entirely clear. As Table 1 shows, while most previous studies clearly highlight privacy as a pertinent issue that can prevent consumers from using and enjoying personalized applications, some studies argue otherwise. Thus, for instance, although Awad and Krishnan (2006) build on utilization maximization theory to argue that, while privacy may not significantly influence individuals' attitudes toward personalized services, consumers' concerns remain detrimental to their responses to personalized advertising. Xu et al.'s (2011) laboratory simulation (where subjects responded to given privacy scenarios but without interacting with real applications) found personalization could, to an extent, override subjects' privacy concerns. These inconsistent findings also confirm the need for more theory-grounded investigations to gain deeper understandings into how much privacy anxieties impact people's acceptance and enjoyment of personalized applications. Table 1 shows that most prior studies in this research area, with the exception of Awad and Krishnan who adopted the utility maximization theory, lack comprehensive theoretical foundations. While acknowledging the weakness of this theory (in that consumers do not compute exact cost–benefit analyses for each information exchange) they argue for the theory's appropriateness for their study as consumers do weigh the tradeoff involved (in this case, between a personalized offering and information privacy). Our study goes beyond examining this tradeoff to address specifically the personalization–privacy paradox through a validated IT solution. As noted above, this involves the adoption of two theories, UGT and IBT, the former yielding a more refined consideration of the enjoyment people derive from personalization, and the latter offering a complementary understanding of the limits on how privacy may impact the different gratifications derived.

Second, extant studies typically restrict their empirical research methodologies to surveys and controlled laboratory experiments, so that it is unclear whether their findings would be robust in actual commercial contexts. Previous research has cautioned that there could be significant differences between individuals' perceptual responses and their actual behaviors (Hui et al. 2007; Jensen et al. 2005; Norberg et al. 2007). For instance, Norberg et al. (2007) show that individuals' perceptions of trust may have no significant impact on their actual behaviors in terms of disclosing their personal information, so research needs to assess user responses to personalized applications more realistically, in actual commercial contexts. Our study proposes and designs a technological solution that satisfies users' desires for personalization but also alleviates their information privacy concerns, and then validates this solution via a multimethod approach. Specifically, we conducted a field experiment that provided users with our self-designed applications to assess their response in the actual commercial context, and corroborated our findings through surveys to gain more robust understandings that incorporate both the perceptual beliefs and the actual behaviors of users.

Theoretical Foundations

Uses and Gratifications Theory (UGT)

UGT originates from research on the use and impact of communication media (Klapper 1963; Lin 1999; McGuire 1974; Rubin 1985), and is often applied by scholars to understand why individuals become involved in particular types of media and what gratifications they receive from that involvement (Ruggiero 2000). Prior UGT research has suggested that consumers use a medium either for the experience of the process itself (e.g., playing with the technology), or for the content (information, etc.) it delivers (Stafford et al. 2004), and these two broad dimensions are categorized as *process gratification* and *content gratification* (Cutler and Danowski 1980; Stafford and Stafford 1996; Swanson 1992). "Content gratification includes use of the messages carried by the medium, and process gratification relates to enjoyment of the act of using the medium, as opposed to interest in its content" (Stafford and Stafford 2001, p. 96). Stafford et al. (2004) also note that the distinctions between process and content gratifications should be defined *in context*, with operational definitions and resulting measures that are specific to the medium.

In the context of visiting websites, Stafford and Stafford (2001, p. 97) illustrated that "aimless surfing is an apt Internet characterization of process gratification." Relating to our context of a pull-based mobile personalized application, when people enjoy the process of navigating a technology (e.g., a mobile application), they are more likely to use it, even when they have no clear interest in any particular content provided by the technology: in the web context, this corresponds to aimless surfing (Stafford and Stafford 2001). The argument is also consistent with previous literature on technology acceptance, which shows that peoples' enjoyment of a technology can lead to them using it more often, as measured by the number of times users log into a system (Venkatesh et al. 2002), the number of times they engage in a technology ses-

Table 1. Summary of Prior Work on the Personalization–Privacy Paradox and Comparison with Our Paper

Authors (Year)	Focus	Theory	Methodology	System Developed	Findings
Awad and Krishnan (2006)	Information transparency on collected personal data and consumer attitude regarding online profiling.	Utility maximization theory	Survey (400 online consumers)	None	In the case of personalized services, where the benefits are more apparent to consumers, previous privacy invasions are not significant, as the potential benefit of the service outweighs the potential risk of a privacy invasion. In the case of personalized advertising, where the benefit is less apparent and the risk is more apparent, previous privacy invasion is significant. Consumers who value information transparency are less likely to participate in personalized services and advertising.
Norberg et al. (2007)	Investigated the effects of risk and trust perceptions on personal information disclosure.	—	Exploratory study (Survey and interview involving 23 students)	None	Risk perception has a significant negative impact on individuals' stated intentions to disclose personal information. Trust perception has no significant impact on individuals' actual personal information disclosure.
Sheng et al. (2008)	Impact of personalization and privacy concerns in an ubiquitous environment.	—	Scenario-based survey (100 students)	None	Privacy concerns have a negative impact on intention to adopt personalized services. There is no significant relationship between privacy concerns and intention to adopt non-personalized services. The results also provide evidence for the personalization-privacy paradox, that is, personalization triggers privacy concerns, which can, in turn, influence users' intention to adopt u-commerce applications.
Treiblmaier and Pollach (2007)	Probes users' perspectives on benefit and cost of personalization.	—	Interview (25 experts in personalized communication) Survey (405 online consumers)	None	Users' general attitudes toward personal data (i.e., their perceived level of risk associated with data disclosure) determines their perceptions of personalized marketing communication. The finding that users expect personalization to lead to an increase in unsolicited commercial messages suggests that personalization may have varying consequences, depending on how responsibly companies use the data they collect.
Utz and Kramer (2009)	Investigated whether users of a social network are benefitting from the ability to set different privacy levels.	—	Multiple surveys (217 online user, 70 students, 147 students)	None	The vast majority of users had changed the default privacy settings into more restrictive settings.
Xu et al. (2011)	Investigated the dynamics of the personalization–privacy paradox when dealing with the disclosure of personal information in the location-awareness marketing context.	—	Laboratory Experiment (545 undergraduate and graduate students)	Scenario-based simulation	Personalization could somehow override privacy concerns for both covert-based and overt-based location-aware marketing. Consumers are more likely to regard location-aware marketing as valuable if advertising messages are perceived to be relevant and customized to their context.
This study	Argues that consumer response to personalization–privacy paradox could vary depending on whether he/she is engaging in process or content gratifications. Addresses the personalization–privacy paradox through a validated technological solution.	Uses and gratifications theory and information boundary theory	Field experiment (691 actual mobile phone users) and post-experiment surveys	3 mobile applications developed *(1 proposed application solution and 2 bench-marking applications)*	Personalization benefits are expected to lead to higher process gratifications, but not content gratifications, due to perceptions about the latter's penetration of information boundaries which raise significant privacy concern. Users of personalized, privacy-safe application not only engaged in higher application usage behavior (process gratification), but also saved adverts more frequently (content gratification) than those whose applications lacked this privacy-safe feature.

sion (Heerink et al. 2008), and their frequency of access (Yi and Hwang 2003). Leading from these, an appropriate proxy measurement for process gratification would be the frequency of launching the application. Such a choice of measurement, the individual's capacity and freedom to *initiate/discontinue use* of a medium, is also of great interest in practice. Despite intensive media competition, the act of running an application is a good indication of the user's affinity with the medium (Rubin 1993).[7]

Stafford and Stafford (2001) also note in the context of visiting websites that

> bookmarking a site might be more representative of motivations arising from content gratifications. When a user finds a site compelling enough to mark the return passage for a later visit, this is likely indicative of strong content interest (p. 97).

In relation to the context of a mobile application, when a user is interested in the content (advert) transmitted by a mobile personalized advertising application (i.e., content gratification), they are more likely to save it so it can be retrieved later, the equivalent of bookmarking a website in the web-surfing context. Thus, we measure content gratification in terms of the frequency of saving adverts.

Studies applying UGT have mainly treated process and content gratifications as antecedents of media selection, use, and addiction (e.g., Song et al. 2004; Stafford et al. 2004; Zeng 2011), but questions of what might promote or prevent people from obtaining process and content gratifications (i.e., the social and psychological factors highlighted in UGT) are given little attention. To gain a better understanding about these factors, which affect the process and content gratifications users may derive from mobile personalized advertising applications, given the personalization-privacy paradox, we consult IBT.

Information Boundary Theory (IBT)

IBT was formulated to explain the psychological processes individuals use to try to control the outflows of private and valued information to other parties (in our case, marketers) (Stanton 2003; Stanton and Stam 2003). The theory suggests that consumers form physical or virtual informational spaces around themselves which have defined boundaries, and that these boundaries play pivotal roles in their willingness to disclose information (or not) (Petronio 1991; Stanton and Stam 2003). An attempt by an external party to cross such a boundary (e.g., a marketer collecting information about the consumer) may be perceived as an invasive act that makes them feel uncomfortable (Solove 2006). Whether such a potential crossing of a personal information boundary is *actually* perceived as an intrusion—and so arouses anxiety—depends on the extent to which the individual concerned considers it to likely to be harmful, or if disclosing the information to the party concerned would be worthwhile to the user (Petronio 1991). An individual may engage in that calculation based on a risk-control assessment, that is, weighing their perceptions of the risk of disclosing the information (and the extent of their control over that disclosure) (Xu et al. 2008) against the benefits they can expect to receive from doing so. A consumer may deem such a disclosure as unacceptable and as raising uncomfortable privacy concerns if they see a high risk to disclosing the information, a lack of control over the information, the absence of worthwhile benefits, or a combination of these worries. The type and nature of the information that individuals contemplate disclosing is central to their considerations about this trade-off (Petronio 1991; Stanton and Stam 2003), so, for instance, given similar benefits (such as receiving personalized financial recommendations), information about an individual's poor health is likely to be seen as a higher risk and as requiring greater control than other information, such as their age.

IBT has been widely applied in assessing individuals' privacy concerns about IT applications. Previous research has used the theory to understand the effects of privacy issues on the implementation and acceptance of IT systems in healthcare contexts (Zakaria, Stam, and Stanton 2003), the cultural factors involved in individuals' reactions to communication applications in general (e.g., e-mail, bulletin boards) (Zakaria, Stam, and Sarker-Barney 2003), and the antecedents of privacy concerns in the context of e-commerce sites (Xu et al. 2008). Zakaria, Stam, and Sarker-Barney (2003) note that IBT can

> predict an individual's preferences and choices regarding the amount and type of personal information [he/she] would be willing to reveal in various e-commerce [i.e., IT application] scenarios (p. 57).

Stanton and Weiss (2000) suggest individuals frame their uses of IT applications to reveal information about themselves in similar terms to how they reveal it in human relationships (characterizing the revelations as, for example, "telling about me," or "becoming visible to others"), so they need to feel

[7]According to Sebastian Holst, chief marketing officer for preemptive solutions, developers are naturally keen to see how end users are invoking the applications they build (Vizard 2010).

comfortable in revealing personal information when the process is mediated by IT applications. Our study leverages this refined understanding about the different gratifications users may derive from a specific class of IT applications, personalized mobile advertising applications, and employs IBT to investigate where privacy concerns are significant enough to undermine those specific gratifications.

Hypotheses Development

This section develops our research hypotheses grounded on UGT and IBT, using the two types of gratification (process and content) UGT highlights as coming from using a medium (Rubin 1993; Stafford et al. 2004) as the bases for assessing the effects of personalization and of privacy concerns in the context of the use of mobile personalized advertising applications: whether and how these factors affect individuals' ability to derive these gratifications are then considered via the IBT lens (Petronio 1991; Stanton and Stam 2003).

Effects of Personalization on User Gratifications

Research on personalization, which arises from the emergence of Internet-based applications, has been best articulated by Abrahamson (1998) who envisioned that technological advancement could offer a "vehicle for the provision of very specific high-value information to very specific high-consumption audiences" (p. 15), an insight that was shared by Ha and James (1998) who concluded that the application medium would evolve from a mass-produced and mass-consumed commodity to an "endless feast of niches and specialties" (p. 2). The fact that each particular smartphone is closely tied to a specific consumer (Kavassalis et al. 2003; Lee and Benbasat 2003; Watson et al. 2002), gives marketers the opportunity to identify, differentiate, interact with, and send personalized adverts to each individual user (Stewart and Pavlou 2002), and this process—of using the individual's information to deliver specifically customized advertising messages—is known as "personalized advertising" (Peppers and Rogers 1997). The ability to personalize the advertising information specific users receive via mobile applications gives users a degree of flexibility and control in how they interact with the application (Brusilovsky and Tasso 2004). Annoying irrelevant adverts can be filtered out, and only those relevant to the user can be displayed in a personalized form, reducing the cognitive load involved in browsing through the adverts and also meeting individuals' personal needs more effectively, leading to more positive results for all concerned (West et al. 1999). From the UGT lens, customized communications should attract users' attention and induce positive responses in them, such as higher loyalty and lock-in (Ansari and Mela 2003), so mobile advertising applications that can filter and display adverts based on users' information when requested should enhance users' process gratification in browsing and navigating via the application.

> **H1a**: *The provision of a personalization feature in a mobile advertising application* ***will result in a higher level of users' process gratification*** *compared to an application without the personalization feature.*

Given the widespread recognition of the supposed benefits of technology-enabled personalization since the advent of the Internet (Peppers and Rogers 1997) and more recently of the smartphone (Brusilovsky and Tasso 2004), optimistic predictions have been made regarding users' receptiveness of applications that offer personalization. According to Reza Chady, head of global market research at Nokia Networks, "users are receptive to advertising that is personalized and relevant to their lifestyle" (DeZoysa 2002). Previous research has suggested personalization as the key to overcoming consumers' negative attitudes about mobile advertising (Xu 2007), even if it requires them to reveal their personal information to some extent (Chellappa and Sin 2005; Xu et al. 2008), which may be reflected by "consented personal information and habit gathering to receive special offers and coupons" (Xu et al. 2008, p. 4).

However, there could be a boundary beyond which consumers interacting with mobile personalized advertising applications consider revealing their information would be unacceptable. We argue that the provision of personalization can only enhance users' process gratification, not their content gratification. We follow IBT in suggesting the nature of user information involved in deriving that these two different types of gratification may play a determining role. To derive process gratification (i.e., a more enjoyable experience of navigating and using applications), users may be willing to provide some level of personal information (such as age, gender, dietary preferences etc.) so that irrelevant adverts can be filtered out (e.g., poultry product adverts are not sent to vegans), leaving only relevant material to be displayed on the users application interface. In contrast, for users to derive content gratification from adverts implies that they actually acting on their contents (Stafford and Stafford 2000), in the mobile personalized advertising application context, this typically involves them saving adverts for the convenience of retrieving them later, an action (similar to bookmarking a website) which indicates their attention to and interest in the content (Lee 2001).

In practice, however, saving an advert to the application usually demands the user reveal a far deeper level of personal information than the broader, everyday elements (e.g., age, gender, dietary preferences) noted earlier. Saving an advert is analogous to the user confirming their genuine interest in a specific product. And, importantly, the act of saving it also typically leaves footprints on the application, showing which adverts the user has browsed and which they have marked as favorites. This information is then likely to become a permanent part of some digital profile of the user which is held without their knowledge by an organization and in a location they know nothing about, and which they are unlikely to be given the option to challenge or change in the future. Thus, compared to revealing "simple" personal information to gain process gratification, saving a mobile personalized advert may deliver content gratification, but is also likely to cause users to worry the advertising application may be breaching their personal information boundary (Stanton and Stam 2003). This information privacy concern may cause users to hesitate to save such messages to their mobile applications, so that

> **H1b**: *The provision of a personalization feature in a mobile advertising application* ***will not result in a higher level of users' content gratification*** *when compared to an application without the personalization feature.*

Effects of the Proposed Privacy-Safe Feature on User Gratifications

To address the issue that users' concerns about the privacy of their information may undermine their achievement of content gratification, we propose a design for mobile personalized advertising applications that stores and processes user information locally (on their phone, as opposed to sending it out to a marketer's central server), which we refer to as the *privacy-safe feature*. As it remains held within their own information space, such a design gives users control over their personal information, as well as over the adverts they choose to save. The fact that marketers can no longer insist on having information transmitted to their central servers before they offer personalized services alleviates users' concerns about the risk that it may be abused (e.g., exploited for unintended, secondary usage) or intercepted during the transmission (Smith et al. 1996).

This privacy-safe feature may thus resolve users' concerns that their information boundary may be intruded upon, allowing them to make a more favorable risk-control assessment about using mobile personalized advertising applications (Stanton 2003; Stanton and Stam 2003; Xu et al. 2008). We argue that the ensuing sense of greater psychological comfort that this feature could promote may lead users to receive enhanced gratification from using the application, making browsing adverts through the application (i.e., process gratification), as well as saving adverts of interest for later retrieval (i.e., content gratification), more enjoyable. Hence, we hypothesize

> **H2a**: *The provision of a privacy-safe feature (which stores and processes user information locally) in a personalized mobile advertising application* ***will result in a higher level of users' process gratification*** *compared to an application without the privacy-safe feature (which transmits user information to a marketer's central server).*

> **H2b**: *The provision of a privacy-safe feature (which stores and processes user information locally) in a personalized mobile advertising application* ***will result in a higher level of users' content gratification*** *compared to an application without the privacy-safe feature (which transmits user information to a marketer's central server).*

Research Methodology

This study primarily uses a field experiment methodology to collect real usage data in a natural, unobtrusive environment with manipulation of the independent variables (i.e., the type of mobile advertising applications). The dependent variables employed were the frequency of launching/using the mobile advertising applications (reflecting users' *process gratification* with the application) and the number of adverts saved (reflecting users' *content gratification* with the application).

Mobile Application Design

Three mobile advertising applications were developed specifically for the purpose of this study: (1) an application that broadcasts adverts generally (i.e., a *non-personalized application*), (2) an application that filters and displays adverts based on a user's profile information stored in a central server (i.e., a *personalized, non-privacy-safe application*), and (3) an application that filters and displays adverts based on a user's profile information stored on their own smartphone (i.e., a *personalized, privacy-safe application*). All applications allow consumers to save adverts for later scrutiny; unsaved adverts are deleted the next time the application is run. The proposed *personalized, privacy-safe* solution, incorporated in the third application, was developed to offer personalized adverts while preserving the user's sense of psychological comfort that their information space was not invaded. Figure 1

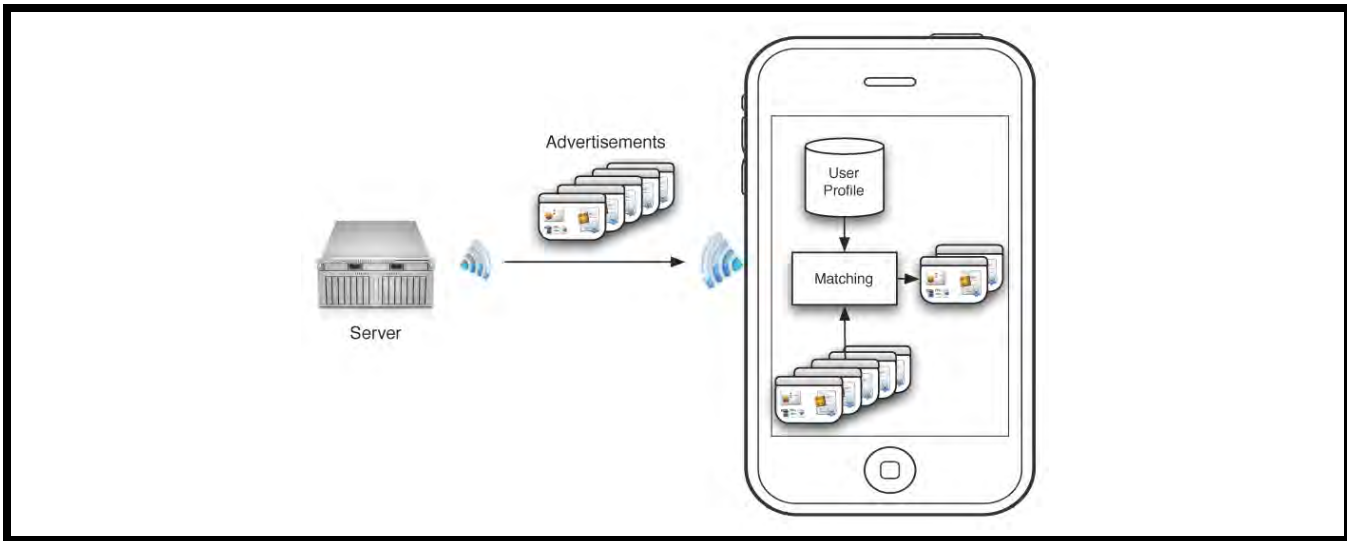


Figure 1. Architectural View of the Designed Personalized, Privacy-Safe Application

gives an overall architectural view of this application, which personalizes advertising messages on the smartphone rather than at the marketer's central server. The marketer simply broadcasts new adverts to consumers, but without knowing their personal information; the *personalized, privacy-safe application* then filters out irrelevant adverts before displaying them based on the personal information the user has previously stored on their smartphone.

Figure 2 shows the overall mobile advertising process and our three experimental versions of the mobile applications. The internal mechanism of the *personalized, privacy-safe application* is shown in section 3c at the bottom of the figure. The other two benchmarked applications (discussed later) are presented in the upper sections. The process starts with the marketers uploading new advertising messages to the application's central server (point 1), after which the adverts and their targeting rules are added to the advert database (point 2). An important mechanism of the *personalized, privacy-safe application* is the short-lived mobile advertising-agent, one of which is created for each advert (Figure 2, point 3c), containing details of the advert (i.e., the content, the targeting rule and the expiry date). Each agent is then cloned and broadcast to the phones of all consumers using the application. Once delivered, the agent first retrieves the consumer's locally stored personal information and then matches the adverts' targeting rules to the mobile phone owner's profile, selecting only the best matches (as specified in the targeting rules) to display on the consumer's phone (point 4c). Having completed this task, the mobile agent expires and auto-deletes. The fact that the agent is short-lived means marketers can only broadcast new adverts to consumers, but cannot gain knowledge about their personal information.

Given that the *personalized, privacy-safe application* is equipped with two features (i.e., personalization and local protection of consumer's information), assessing the effects of these two individual features on users' process and content gratifications requires us to have two benchmarked mobile applications: a base version that broadcasts non-personalized adverts (*non-personalized application*) and another version that sends users' profile information to a central server to perform personalization (*personalized, non-privacy safe application*). The first of these selects adverts at random to be sent to consumers, and ignores the adverts' targeting rules (see 3a in Figure 2). In the second (the *personalized, non-privacy-safe application)*, consumer data is transmitted to and centrally stored at the server, which filters the adverts according to that data before sending them to the consumers (Figure 2, point 3b).[8]

[8]The design of our mobile advertising application also considered performance issues, to ensure there were no systematic differences in processing and communication response times. We built on two main principles: web services for machine-to-machine interoperability interface over the network, and mobile agency for distributed computation and consumer privacy protection. Web services were designed around the representational state transfer (REST) idiom, mainly because of its efficiency. In fact, REST has a better relationship with the Web than simple object access protocol (SOAP) based Web services (Shi 2006). This approach differs from SOAP services that usually require specific libraries to be included in the client software. The mobile agency enables us to distribute the computational power. The match between the adverts and the users' profile is distributed in the users' mobile device. Consequently, the number of users that can be handled is highly scalable and the server-side infrastructure is very light. The task of the application's central server is to dispatch the mobile agents to the users; involving a workload comparable to a simple web server. Moving the matching computation to the client side is the key to protecting consumers' information privacy.

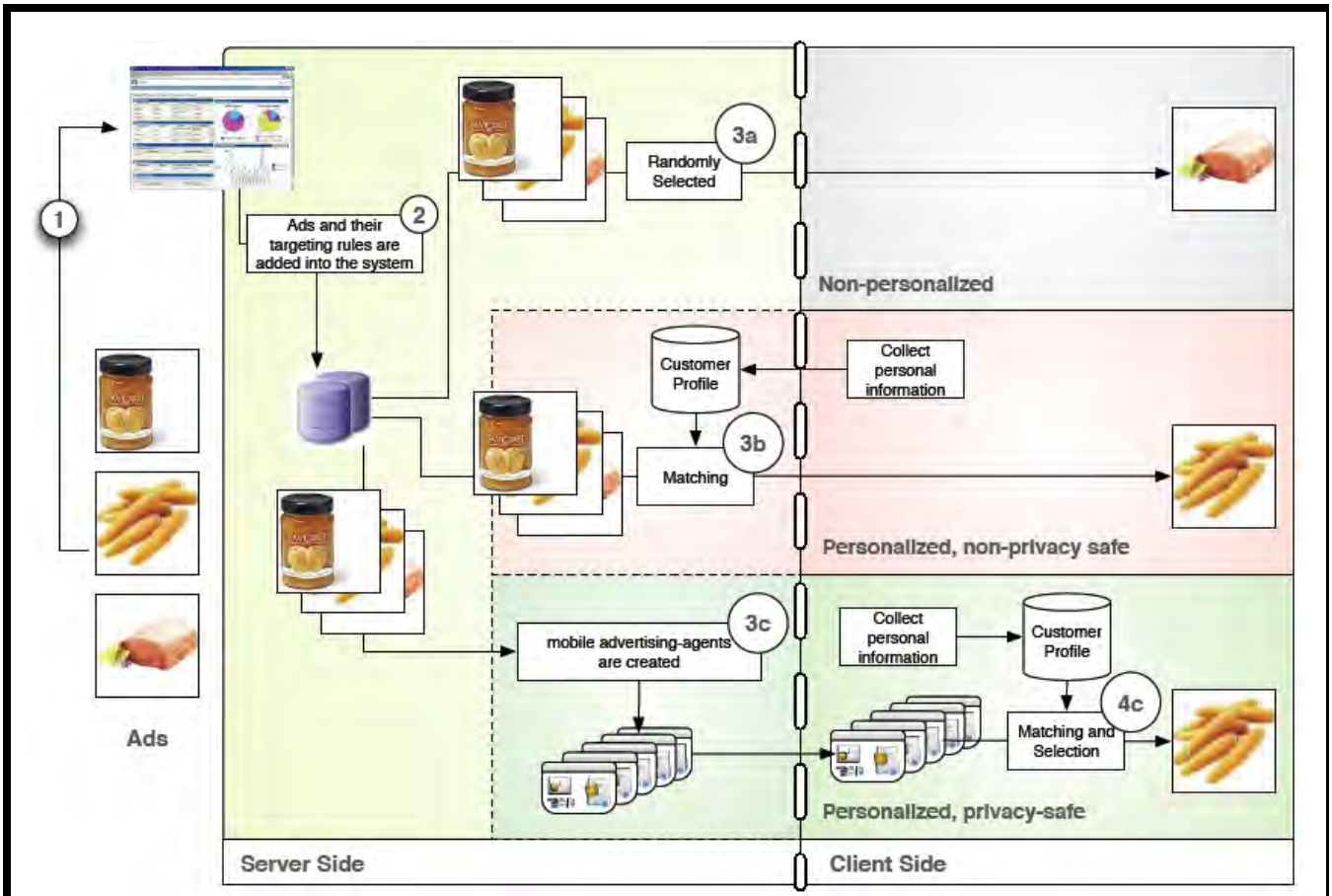


Figure 2. Overview of the Three Experimental Versions of Mobile Advertising Applications

In all three cases, the early part of the process is the same: the marketer enters new advertising messages and their targeting rules on the system server, which adds them to database. The difference between the three applications is how the adverts are selected and delivered to consumers. The second and third mobile advertising applications in Figure 2 both offer personalization, but differ with respect to whether they are equipped with the privacy-safe feature. Both applications question the user to gain personal information (Figure 3), but the personalized, privacy-safe advertising application saves the answers to the user's own mobile phone (as at 3c in Figure 2), along with a privacy-safe label (see Figure 3), whereas the personalized, non-privacy-safe version transmits consumers' answers to a central server (3b in Figure 2), so that users only sent adverts that match their updated profiles. The core differences in the process concern where (and thus by whom) the filtering decisions are taken: in the privacy-safe application, adverts are filtered locally (actually on the consumer's phone), while in the non-privacy-safe application, the adverts are filtered at the marketers' servers, a process that is under their control.

For the advertising messages delivered to the users in our study, we partnered with an advertising agency specializing in retail supermarkets, an ideal industry for this study, given its appeal to a wide consumer base and the tremendous opportunities to offer personalization over a broad range of products. The agency fed new adverts to our server on a daily basis for dissemination to the users of the three different mobile advertising applications. Our primary purpose in arranging an industrial collaboration for our advertising content was to ensure the practical relevance of our advertising messages to consumers at large. The personalization questions we used were also developed in consultation with the advertising agency, and based on advert categories they suggested (see Table 2), and were used in common by all three mobile advertising applications, which also accessed the advertising messages from the same database.

Personalized, Privacy-Safe Application

Personalized, Non-Privacy-Safe Application

Figure 3. Personal Information Request Pages of the Two Personalized Mobile Advertising Applications

Table 2. Product Categories and Subcategories (furnished by the collaborating advertising agency)

Categories	Subcategories
Food	Pork, beef, chicken, fish, mixed meat, diet, tobacco, ice cream, chocolate, biscuits, sweets, other desserts, snacks, dairy, lactose-free, processed food
Beverages	Energy drinks, alcohol, soda, coffee, tea, fruit juice
Household Products	Household cleaning products, laundry detergents
Pet and Animal-Related Products	Cat products, dog products
Personal Care	Male products, female products, baby products, kids' products, sports products, general personal care

Table 3. Examples of Personalized Questions Asked

Questions	Options
Do you have a lifestyle diet?	No; Vegetarian; Vegan
Do you consume alcoholic beverages?	Yes; No
Do you have pets?	No; Cat(s); Dog(s); Cat(s) and Dog(s)

Research has shown that effective marketing offers should be customized according to consumers' personal information rather than their indicated product preferences, as consumers' actually appear to have limited insights into their own product preferences, which are (to at least some significant degree) undeveloped and unstable (Simonson 2005), so we based the personalization for our study on personal information elicited from consumers. Table 3 shows examples of some of the personalization questions asked.

Measurements of Process and Content Gratifications

We follow previous literature (Lee 2001; Stafford et al. 2004) in measuring users' process gratification in terms of their frequency of launching the application and content gratification in terms of their frequency of saving adverts. The first measure is in line with UGT, which highlights individuals' ability to *initiate/discontinue* using a medium (Rubin

1993). Application use was pull-based, in that there was no notification sent to users regarding new adverts, and choosing to browse through adverts involved users launching the applications themselves. We also deliberately designed the applications so that they primarily supported browsing through adverts, with no functionality (such as search features) provided to let them access adverts directly to see their content. This minimized the possibility of users launching the applications because they were already interested in the content of a particular advert, which would have made it difficult for us to disentangle process and content gratification motivations. So if a user enjoys the process of using the application, this will be reflected by how often they launch it (Lee 2001; Rubin 1993). The second measure, using advert saving to indicate users' content gratification, is based on the rationale that users interested in the content of an advert will have to save it so that they can retrieve and use it later (e.g., opening the application in the store to retrieve the message and buy the relevant product). As previous literature notes (Lee 2001), this resembles browsers bookmarking an interesting website. Figure 4 depicts the steps consumer take when using a mobile application, and how these steps correspond to process and content gratifications.

Pilot Test

Before starting the actual field experiment, we conducted a pilot test with eight consumers—two males with IT backgrounds (M1, M2), two females with IT backgrounds (F1, F2), two males without IT backgrounds (M3, M4), and two females without IT backgrounds (F3, F4). The test had two main objectives: (1) to find out if consumers had less information privacy concerns with our privacy-safe mobile advertising application than with the non-privacy-safe application, and (2) to understand the diverse levels of process and content gratifications they gained from using the three different applications. It also allowed us to ensure the main experiment would be well planned and efficiently executed. All participants of the pilot test signed confidentiality agreements not to reveal information about the applications or the discussion to any third-party or to participate in the subsequent field experiment. Participants trialed all three mobile advertising applications over a nine-day period, first installing and using the application without the personalization feature for three days, then using the personalized, non-privacy-safe application for the next three days, and finally the personalized, privacy-safe application for the final three days. We asked them to record their experiences and share them in the subsequent 1.5-hour focus group discussion. Our server captured all installations and usage logs, which the authors reviewed and which showed that the participants had utilized all three mobile advertising applications diligently as requested. They each received US $40 for their efforts.

We began the focus group discussion by asking all eight participants which application they preferred and why. Six of the eight expressed higher process and content gratifications with the *personalized, privacy-safe* mobile advertising application: only F3 and M2 preferred the non-personalized advertising application, and their answers showed that they both habitually preferred browsing through adverts on their own.

> **F4**: "Why would you browse through 500 [adverts]?"
> **F1**: "I wanted to see products related to my taste...like I don't have any kids. I don't want to see any products for kids."
> **M2**: "Even if I have to browse through 500 [adverts] per week, I do not mind."
> **F3**: "Yes, I also prefer to browse through all [adverts]. Instead of having an application filter them for me."

Next we focused our discussion on comparing the privacy-safe and non-privacy-safe mobile advertising applications, to check if participants could identify the differences between the two.

> **M1**: "Yes, it is this one [pointing to the privacy-safe label.]"
> **F2** (*nodding her head, indicating agreement with M1*): "The only difference is the security part."

Participants were asked for their perceptions on the personalized, privacy-safe mobile advertising application.

> **M1**: "I would say that it is actually quite nice [referring to the privacy-safe application]. And even if the people who did the privacy-safe application lie to me and give away my...information, I could sue the company. So I think I am doubly secure...I have never heard about people hacking the mobile phone. But there are people hacking the server."
> **F2 and M3**: "Of course I prefer the one where the information does not leave the phone."

Next, we asked: *"Who thinks that a privacy-safe version would be better at controlling your information and thus would make you feel more comfortable about using it?"* The same six individuals noted above agreed, but, again, confirmed their dislike for personalized applications.

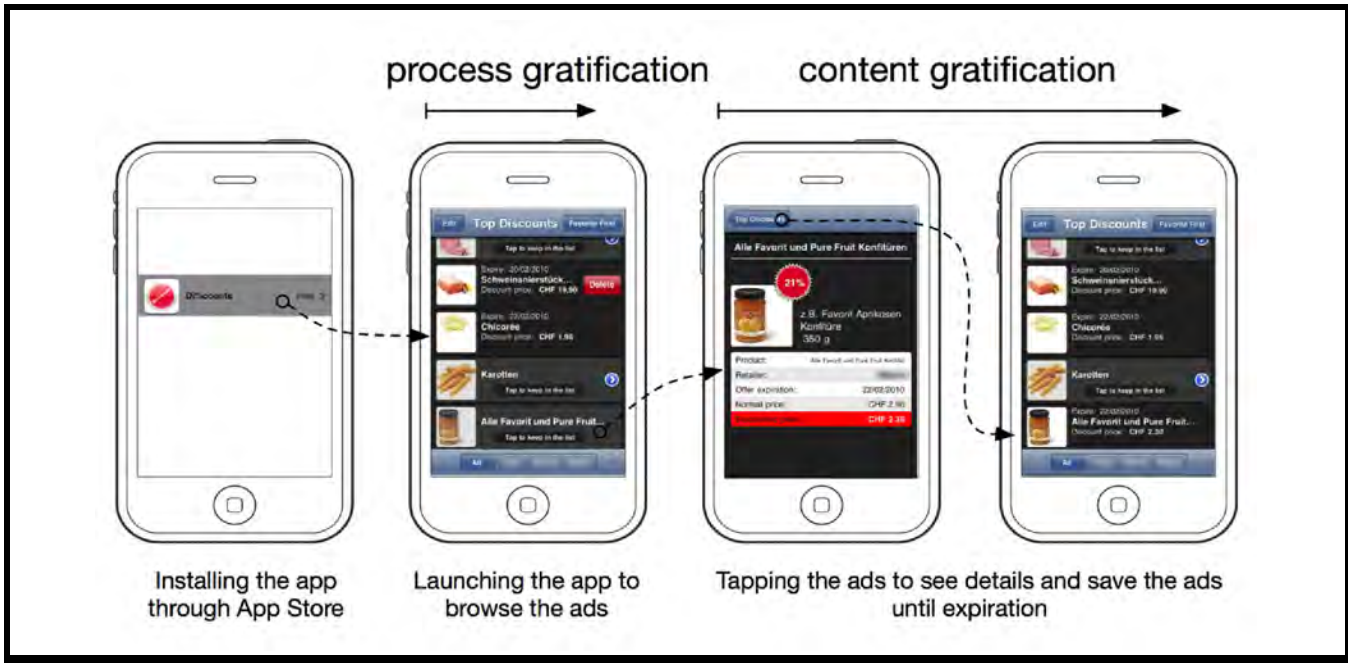


Figure 4. Uses and Gratifications of Mobile Advertising Application

M3: "Local storage on my mobile phone gives me more control!...I prefer local storage"
M4** agreed with **M3
F1: "I would prefer that my selections [referring to the personal information and adverts saved] are stored in my mobile phone. I would not trust my data to be sent to a server....Since I store my messages, contacts, and everything in my mobile phone, it means I trust my phone and I will trust the data stored in it."
M1: "Definitely more control, since no second/third person has access. On a server, people like the server administrator may have access to the information."
F4: "I think that sending my information out to a server is much less secure than storing everything on my mobile phone because...the company is able to... know what kind of person I am."
F2: "Yes, I do feel more secure with the local version. Knowing that everyone else could easily have access to my logs, makes me feel slightly uncomfortable when I am using the application."

Based on their answers, it seems that most participants had less information privacy concerns when using our privacy-safe mobile advertising application than they had with the non-privacy-safe application, and so felt more comfortable using it for browsing (process gratification) and for saving the individually personalized adverts to the application (content gratification). To validate these observations more comprehensively, we performed field experiment as described next.

Field Experiment

For our field experiment, we developed mobile advertising applications and made them available via Apple's App Store (www.apple.com/iphone/apps-for-iphone) to users in one European country, so anyone living there and owning an iPhone could download and install them. In practice, the three applications were randomly distributed to iPhone users: the App Store only listed one application title, and every time an iPhone user downloaded that item, our system randomly allocated one of the three versions to their phone. The field experiment ran for 3 months (mid-November 2009 to mid-February 2010) during which time 629 users downloaded one of our applications. The first application (the *non-personalized* version) was sent to 31 percent of the users, 30 percent were sent the second application (the *personalized, non-privacy-safe* version), and 39 percent were sent the third application (*personalized, privacy-safe* version). About 70 percent of the application users were male, and their ages ranged as follows: under 18 (4.5%), 18–25 (27%), 26–35 (36.4%), 36–45 (20%), 46–55 (7.5%), and over 55 (4.6%). Over the three-months, we transmitted a total of 73,077 adverts, which were updated daily, based on daily input from our collaborating advertising agency. Figure 5 shows how often each application was launched during the experiment period.

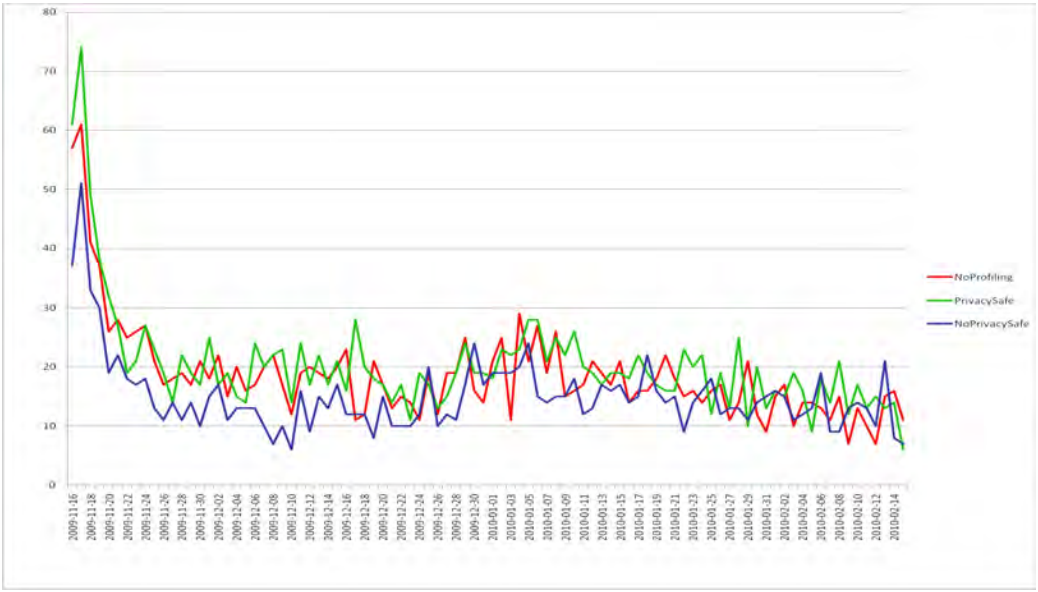


Figure 5. Daily Usage Graph of the Mobile Advertising Applications

Table 4. Count Data Descriptive Statistics

Variable	Non-personalized		Personalized, Privacy-Safe		Personalized, Non-Privacy-Safe	
	Count	***Std. Error***	***Count***	***Std. Error***	***Count***	***Std. Error***
Application Launch	956	69.594	1,707	163.416	1,469	119.273
Adverts Received	11,025	631.618	11,368	1,167.719	10,486	884.458
Adverts Saved	749	83.442	1,653	377.512	1,220	223.939
Personalization Questions Skipped	n.a.	n.a.	291	36.860	283	34.698

Data Analysis

Table 4 provides the descriptive statistics of the dependent variables—application launch/usage denoting process gratification and advert saving (indicating content gratification), and key control variables (number of adverts received and number of personalization questions skipped), which are count data. For data skewness reasons, log transformations were performed on the variables except for demographic variables (age and gender), which were also used as additional control variables.

As the two dependent variables (i.e., frequency of application launch and the number of adverts saved) are counts data, there are two possible regression models we could adopt: Poisson regression and negative binomial regression. The latter model builds on the former by adding a parameter α to reflect unobserved heterogeneity among the observations. Fitting our dataset to both models showed the negative binomial regression model was a better fit for our dataset (as illustrated in Figure 6), and we further confirmed its appropriateness for our analysis by testing for over-dispersion in outcome, as the negative binomial regression model is more appropriate for datasets with highly dispersed outcomes (Long and Freese 2006), which is particularly prevalent in field experiments like this case. To validate our testing, we computed the likelihood-ratio test of the null hypothesis where $\alpha = 0$. The test indicated the null hypothesis could be rejected ($G^2 = 985.78$, $p < .01$), as visually indicated in Figure 6, again confirming the suitability of the negative binomial regression model for analyzing this dataset.

Table 5 presents the results of the negative binomial regression comparing the impact of the personalization feature (H1a and H1b). H1a posits that providing a personalization feature as part of a mobile advertising application will lead users to launch it more often, and is supported by the results that show its presence significantly enhances the number of application launches (Z =

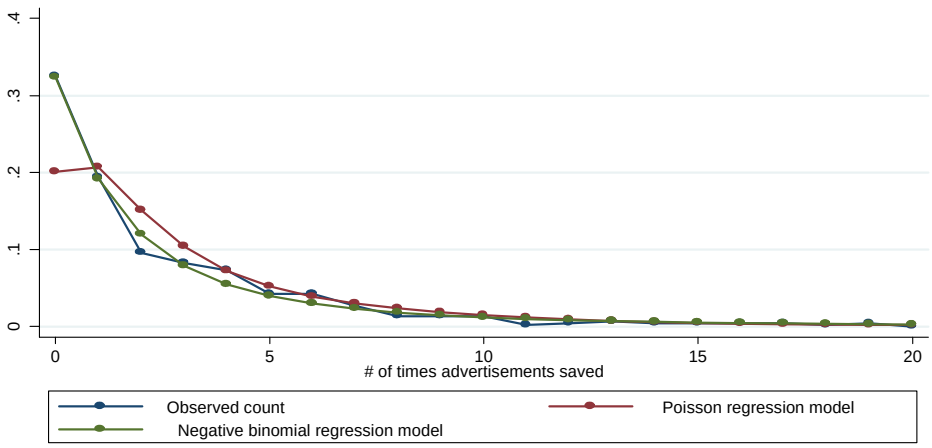


Figure 6. Fitting Poisson and Negative Binomial Regression Models to the Datasets

Table 5. Results on Personalization (versus Non-Personalization) Application

	Application Launch			Adverts Saved		
	Coefficient	*Std. Error*	*Z*	*Coefficient*	*Std. Error*	*Z*
Personalization *(0 – absence; 1 – present)*	0.49	0.05	10.44***	0.22	0.15	1.49
Application launch *(log)*	–	–	–	1.00	0.45	2.23
No. of adverts received *(log)*	1.99	0.06	34.30***	2.00	0.33	6.03
Age	-0.02	0.03	-0.69	-0.07	0.09	-0.79
Gender	0.05	0.10	0.49	-0.51	0.32	-1.62
Intercept	-1.86	0.17	-11.05***	-2.36	0.49	-4.86
Alpha (log)	-3.73	0.35		-0.06	0.11	
Log likelihood	-884.841			-948.59		
LR Chi²(4)	660.44, p < .01			281.62, p < .01		

*p < .10; **p < .05; ***p < .01

10.44, p < .01). H1b posits that the provision of the personalization feature will make no difference to how often users save adverts, the results (Z = 1.49, p > .10) indicate this hypothesis is also supported.

Table 6 presents the analyses of our tests of the effects of providing a privacy-safe feature (H2a and H2b). H2a suggests that the presence of such a feature will lead to the application being launched and used more often, and our analysis results—after controlling for the number of adverts received, the number of personalization questions users skipped, and the demographic information—suggest it did have a significant and positive influence on application launch figures (Z = 2.02, p < .01), thus supporting H2a. We also observed that the privacy-safe feature had a significant influence on the numbers of adverts saved (Z = 1.95, p = .05), so H2b is also supported. Table 7 summarizes the test results for our four hypotheses.

To check whether both process and content gratifications (manifested in application launch and advert saving) were greater when the personalized, privacy-safe mobile advertising application was used than the non-personalized version, we conducted two additional negative binomial regressions (see Table 8), the results confirm our predictions.

We also conducted further robustness tests. Specifically, we observed a surge in the intensity of usage when the applications were initially offered in Apple's App Store at the start of the experiment (as Figure 5 shows). To address this problem, we removed the data for the first six days of the experiment (i.e., be-

Table 6. Results on Privacy-Safe (Versus Non-Privacy-Safe) Application

	Application Launch (DV)			Adverts Saved (DV)		
	Coefficient	*Std. Error*	*Z*	*Coefficient*	*Std. Error*	*Z*
Privacy-safe *(0 = absence; 1 = presence)*	0.09	0.05	2.02***	0.22	0.11	1.95**
Application launch *(log)*	–	–	–	1.01	0.40	2.52**
Number of adverts received *(log)*	1.92	0.05	38.59***	1.74	0.29	6.00***
Number of personalized questions skipped *(log)*	0.27	0.07	3.63***	0.43	0.19	2.27**
Age	-0.10	0.03	-3.65***	-0.11	0.07	-1.59
Gender	0.08	0.08	1.03	-0.43	0.22	-1.95**
Intercept	-1.12	0.14	-8.07***	-1.83	0.36	-5.06***
Alpha (log)	-2.92	0.19		0.02	0.10	
Log likelihood	-1,033.04			-1,058.40		
LR Chi²(4)	818.56, p < .01			379.18, p < .01		

*p < .10; **p < .05; ***p < .01

Table 7. Summary of Results on Hypotheses Testing

H1a: *The provision of a personalization feature in a mobile advertising application **will result in** a higher level of users' process gratification when compared to an application without the personalization feature.*	Supported
H1b: *The provision of a personalization feature in a mobile advertising application **will not result in** a higher level of users' content gratification when compared to an application without the personalization feature.*	Supported
H2a: *The provision of a privacy-safe feature (which stores and processes user information locally) in a personalized mobile advertising application **will result in** a higher level of users' process gratification when compared to one without the privacy-safe feature (which transmits user information to a marketer's central server).*	Supported
H2b*: The provision of a privacy-safe feature (which stores and processes user information locally) in a personalized mobile advertising application **will result in** a higher level of users' content gratification when compared to one without the privacy-safe feature (which transmits user information to a marketer's central server)*	Supported

Table 8. Comparing Personalized, Privacy-Safe, and Non-Personalized Advertising Applications

	Application Launch (DV)			Adverts Saved (DV)		
	Coefficient	*Std. Error*	*Z*	*Coefficient*	*Std. Error*	*Z*
Non-personalized (0) vs. Privacy-safe (1)	0.58	0.05	12.16***	0.44	0.16	2.78***
Application launch *(log)*	–	–	–	0.73	0.47	1.56
No. of adverts received *(log)*	2.12	0.06	37.36***	1.95	0.37	5.22***
Age	-0.14	0.04	-3.67***	-0.08	0.10	-0.77
Gender	0.10	0.10	1.02	-0.43	0.32	-1.34
Intercept	-1.76	0.19	-9.26***	-2.13	0.58	-3.67***
Alpha (log)	-3.24	0.24		0.01	0.10	
Log likelihood	-882.52			-980.44		
LR Chi²(4)	745.92, p < .01			293.63, p < .01		

*p < .10; **p < .05; ***p < .01

fore November 22, 2009) and repeated our negative binomial regression analysis on the trimmed dataset, but this additional set of results confirmed our prior analyses. Specifically, the frequency of application launch of the non-personalized advertising application was significantly lower than that of the two versions offering personalization ($Z = 6.12$, $p < .01$). However, the numbers of advertising messages saved did not differ significantly between those delivered to users via the non-personalized and personalized applications ($Z = 1.45$, $p > .10$), two observations that confirmed the earlier test results for H1a and H1b. In the same way, further analysis on the results for the non-privacy-safe and privacy-safe personalized applications suggested that the inclusion of the privacy-safe feature leads both to applications being launched more often ($Z = 3.13$, $p < .01$) and to more advertising messages being saved ($Z = 3.09$, $p < .01$).

Post-Experiment Investigations

To further corroborate our field experiment observations and to uncover the underlying psychological reasons behind them, we approached the advertising agency about the possibility of conducting further studies with the users. Given the potential risk to the agency's reputation from annoying its users, it was thought more appropriate to start with a short survey to probe general user perceptions about the applications. In consultation with the agency, we designed a short survey consisting of four succinct questions, which was sent to the smartphones of 120 users (i.e., 40 users of each mobile advertising application), of whom 85 responded (a response rate of 70.83%). Table A1 in the Appendix shows the mean responses.

Question 1 asked users of all three applications the degree to which they perceived the number of advert messages to be excessive and (as expected) the users of the non-personalized advertising application reported the highest level of this perception. Answers to question 2 showed that users also seemed to perceive the adverts to be more annoying than did those who used the personalized applications, although it is interesting to note that users of the privacy-safe version perceived the adverts as being the least excessive. Questions 3 and 4 focused on the privacy feature. As expected, users of this application expressed fewer worries about personal data storage (Q3) and were more likely to provide answers to the personalization/profiling question (Q4). These findings further corroborated our field experiment observations, and suggested how we might gain deeper insights into the reasons behind users' perceptions. The fact that they proved generally receptive about sharing their feelings about the applications (as partly indicated by the fairly high response rate) allayed (at least to some extent) concerns that a further survey might be annoying, and the agency agreed it was worthwhile engaging in a more comprehensive survey to gain deeper understanding about the psychological reasons behind users' field experiment behaviors.

Given that the relative advantage of the personalized applications over the non-personalized version was more clearly indicated in the initial survey, our second survey focused on the users of the two applications with personalization features. The overarching aim was to understand why the proposed privacy-safe technological design worked—as users' perceptions indicated it did—in alleviating their privacy concerns, and so allowing them to derive greater process *and* content gratifications from interacting with it. We invited 189 users of the personalized, non-privacy-safe application and 245 users of the personalized, privacy-safe application to participate in the second survey; 80 and 113 of them responded, respectively, representing response rates of 42.33 percent and 46.12 percent. We designed the survey questions around four themes:

(1) Users' general perceptions about how commercial entities offering personalization deal with their personal information.

(2) Whether the types of information involved in users' deriving process and content gratifications from an application differed in terms of the privacy concerns raised.

(3) How users' information privacy concerns, in terms of perceived intrusion to their information boundaries, undermined the level of gratification (specifically of content) they gained from using the application.

(4) The extent to which the privacy-safe feature, by alleviating users' information privacy concerns, allowed them to gain greater content gratification from the application beyond that offered by personalization alone.

The first theme was dealt with by an open-ended question: *How do you think a marketer would use your information that was collected through the personalized application offered?* The other three themes revolved around the logic of our hypothesis based on IBT, and consisted of items measuring the following constructs: information privacy concerns (in using the application to perform different activities), perceived sensitivity (of disclosing different types of information), psychological comfort, perceived intrusion of information boundaries, benefits of personalization, perceived effectiveness of privacy-safe feature, and intention to save adverts to the application. We also included items measuring trust in the application software provider and in their reputation as a controlled variable. Table A2 in the Appendix lists the constructs, their corresponding items, and references, while Tables A3 and A4 document the satisfactory results of the convergent and discriminant validity tests.

Overall, the results from this second survey reveal four key insights, corresponding to the four themes above. First, users are strongly inclined to assume that marketers who provide personalized applications will employ users' personal information for secondary or unintended uses, as reflected in such comments as: *"I believe marketers would store my information for a prolonged period, so they can use it for other purposes later," "I wouldn't be surprised that marketers will sell my information to other third parties," "this [marketers' use of personal information for unintended purposes] is unethical, but I think it is common as personal information of consumers is valuable resource [to them],"* and *"marketers may use my information to send various messages to me, some of which may be inappropriate."*

Second, users are concerned that their privacy is compromised when saving adverts to their mobile phone applications, significantly more so than when providing basic personal information (gender, age, dietary preferences, alcohol consumption; see Table A5 in the Appendix). The mean differences between users' perceived sensitivity to saving adverts and to providing personal information are significant at the $p < 0.001$ levels, and this perception was further reflected in the greater information privacy concerns they expressed when saving adverts, compared to just browsing/viewing them[9] (see Table A6 in the Appendix. Together the results support our arguments that users' saving of adverts reveals deeper levels of information about themselves, increasing their privacy concerns.

Third, this heightened privacy concern related to saving adverts, which (IBT suggests) users are likely to perceive as intruding on their information boundaries, will undermine their psychological comfort in using the application (see the statistical test results in Figure A1 in the Appendix), in turn tending to prevent them from using it to save adverts. The negative effect of perceived privacy intrusion is significant even after controlling for the reputation of and users' trust in the agency providing the application.

Finally, users' favorable perceptions about the effectiveness of our privacy-safe feature imply they see it as serving to reduce their worries about information boundary intrusion, while at the same time enhancing their perceptions of the benefits of personalization (see Figure A1 for the statistical test results). So our proposed privacy-safe feature (which stores and processes the user information needed to personalize their adverts locally on their mobile phone) promoted the positive factor (perceived benefits of personalization) and alleviated the negative factor (perceived privacy intrusion) in users' psychological comfort with the application, thereby increasing the frequency with which they saved adverts to the application (reflecting their content gratification).

Overall these findings not only corroborate our field experiment observations, but also enrich our understanding about how privacy concerns undermine users' gratification when using mobile personalized advertising applications, and confirm how our proposed privacy-safe feature could address those concerns.

Discussion

Our objective in this study has been to contribute to previous research and provide useful guidance to practitioners on how to address the personalization–privacy paradox (Kavassalis et al. 2003; Lee and Benbasat 2003; Watson et al. 2002). Noting that consumers face an important dilemma between enjoying the benefits of personalization and being concerned about the privacy of their personal information, we argue that additional IT design considerations need to be addressed if the benefits offered by smartphone-enabled applications are to be more fully utilized. Indeed, our field experiment, conducted in a real commercial setting using actual mobile advertising applications, allowed us to observe that consumers demonstrated greater process gratification via the personalized mobile advertising application than from traditional broadcast-based advertising applications. Our *post hoc* analysis reveals that application usage increased by 62.4 percent ($p < .01$), all other variables remaining constant. However, we also found that there was *no significant difference* in consumers' content gratification between personalized (without privacy-safe) and non-personalized applications (i.e., the number of adverts saved was not significantly different). Through the IBT lens, we suggest this finding may be explained by understanding how consumers tend to form an information space around them with boundaries they use to control the flow of their personal information to other people/entities. Compared to broad-based, mundane personal information (age, gender, etc.), saving adverts explicitly indicates an individual's interest in specific products and, more importantly, requires the user to reveal deeper levels of information than their boundaries really allow, which is more likely to cause them uncomfortable feelings of being intruded upon, and to hesitate to save adverts to the application. Our post-experiment surveys confirmed our conjectures, revealing consumers' greater privacy concerns when saving adverts. Recognizing these issues, the question is: *How can we improve personalized mobile advertising applications to achieve a better result in terms of the number of adverts saved?*

[9]Except in the privacy-safe application, users' expressed privacy concerns with saving adverts was the same as that with viewing adverts, which is consistent with our expectation that the privacy-safe feature we propose can alleviate users' privacy concerns about saving adverts to the application. For the non-privacy-safe application, the test of mean difference between users' privacy concerns about saving and browsing adverts and between saving and viewing adverts are both significant (at $p < 0.001$ and $p < 0.01$ respectively).

Answering this question is important, because a consumer saving advertising messages is taking a significant step beyond merely using an application to browse adverts. While marketers who invest in developing and/or providing mobile advertising applications would certainly hope their applications would be launched more frequently (Vizard 2010), they may be more concerned with achieving further steps (i.e., consumers reacting to product messages by saving them to view later, indicating they are interested in the message and may be heading toward a purchase decision).

This study proposes a novel technological design solution to address the personalization–privacy paradox that can preserve users' information space by storing their information (including the adverts they choose to save) locally on their own smartphones. Our field experiment shows that our local privacy-safe personalization design not only increases consumers' process gratification (shown in using the application) but also enhances their content gratification (in that they save more adverts). In quantitative terms, application use increased by 9.6 percent ($p < 0.05$) compared to the personalized, non-privacy-safe application, and by a massive 79.1 percent ($p < .01$) compared to the non-personalized application. Furthermore, advert saving increased by 24.4 percent ($p = 0.05$) compared to the personalized, non-privacy-safe version, and by 55.1 percent ($p < 0.05$) compared to the non-personalized application. Post-experiment survey investigations show our design reduces users' perceptions about their information boundaries being breached when saving adverts, while also enhancing their perceptions of the benefits of personalization in mobile advertising applications. By alleviating the personalization/privacy tension, users' psychological comfort with the application improves, and the number of adverts they save increases.

Before discussing the study's implications, we need to note a caveat. We use the frequency of users' launching applications to indicate their process gratification, deeming this a reasonable measure for our self-developed application, which was deliberately designed to limit users' activity to browsing lists of adverts, in order to make it clear that how often users launch an application reflects how much they enjoy the process of using it. But future research that intends to replicate this study using off-the-shelf applications (rather than self-developed applications such as the ones we developed) may be confronted with more sophisticated issues in measuring process gratification. For instance, applications that incorporate a search function may allow users to access adverts of interest directly (e.g., where they are already considering purchasing it), making it more difficult to disentangle process gratification from content gratification.

Despite the care we took in designing our applications, the possibility that some users launched the applications because they were already interested in certain advertising content cannot be completely ruled out. We conducted a further assessment based on the variation in users' viewing of adverts (average per use session, i.e., from launching to closing the application), and the correlation of this measure with their frequency of launching the application. The rationale is that if many users launched the application to view advert contents they already have in mind, this should show up in systematic patterns in how users viewed advert contents in the data. Two observations were made. First, the variation in users' average viewing of adverts per session was low (i.e., standard deviation = 1.029, max. = 10.75), implying they viewed more or less the same number of adverts per session, that is, it did not appear that some users viewed significantly fewer adverts because they already had some content in mind that they wanted to view. This may have to do with our application design, which primarily encouraged browsing and saving of adverts, and provided users with no search function to allow them to access to adverts directly. Second, the correlation between the average number of adverts viewed per session and the frequency of launching the application was also quite low (0.183). This would suggest that there was no clear systematic pattern in users' frequency of launching the application and their interest in certain advert contents. In other words, it did not appear that users launched the application frequently because they were interested in certain advert contents rather than just browsing through the adverts. Despite this *post hoc* analysis, researchers may attempt to solve this problem by recording every instance of user-application interaction (e.g., so as to differentiate between aimless and purposive search by examining prior activity patterns), but they will need to be aware that obtaining such activity data may make users feel excessively monitored. Indeed, the trade-off between minimizing intervention and bias and ensuring data collection procedures are acceptable to subjects in a field experiment (Harrison and List 2004) is an intricate challenge to be addressed cautiously.

Notwithstanding this limitation, this study makes several significant contributions that we believe are worth highlighting.

Implications for Research

UGT suggests individuals obtain both process and content gratification when using media, but does not explain how the particular features of a given medium may alter the degree of these two gratifications. By integrating personalization and privacy research with the UGT, our study extends theory as well as raising several issues for future research. A first important implication of our study for UGT is that, while personalization enhances user gratification, it is only from the process angle: gratification in content terms may still be undermined by privacy concerns. By integrating UGT with IBT, we suggest the fol-

lowing reasoning, which was supported by our post-experiment survey investigations: saving adverts to the application may give users greater content gratification, but will also heighten their worries that their information boundaries may be being breached, undermining their psychological comfort and so inhibiting them from saving adverts. Such insights make non-trivial contributions to current discourses on the personalization–privacy paradox, some of which emphasize privacy as being of the utmost importance (e.g., Culnan and Milne 2001; Phelps et al. 2000), while others depict a bounded impact of privacy when personalization is desired (e.g., Hann et al. 2002). Our findings more clearly demarcate the extent to which personalization and privacy affect users' gratifications from mobile personalized advertising applications, and a similar approach could be employed in future research to conduct finer-grained investigation into the limits to which personalization and privacy influence process and content gratifications on different technological platforms (e.g., Web, mobile, and the emerging cloud computing) and for applications for purposes other from advertising (e.g., for checking bus or train schedules, or for social networking). This stream of research may aid commercial organizations in their efforts to ensure their technological applications give greater user gratification, resulting in more favorable user responses. Our findings also suggest that the type of information involved plays a determining role in whether privacy concerns affect the gratification users get from personalized applications: future research may follow this direction to pay more fine-grained attention to which information aspects users consider too private or sensitive, and most likely to violate their sense of privacy.

Second, our study shows that IT solutions can effectively overcome the personalization–privacy paradox that the technology itself effectively creates. Our empirical studies (entailing field experiment, focus group, and surveys) show consistently that our proposed technological design, which stores and processes users' information locally on their smartphones, promotes their sense of psychological comfort by preserving their information space. Such findings contribute to IBT by demonstrating how technological design can help preserve a user's information space, and to UGT by showing how a medium's design features can lead to fuller gratification for its users. Essentially, by giving users greater gratifications from personalization, technological design can increase their psychological comfort that their information space is secure. We hope this conclusion will stimulate an exciting direction of future mobile phone application research, in which—given the highly personal and private nature of the device—the notion of preserving users' information security is seen as paramount. We believe IS researchers are particularly qualified to explore a range of possible technological designs, beyond that proposed in this study, which can give users this increased sense of comfort, and that such a stream would be a good complement to the extant research focused on ensuring data transmission security (e.g., Brar and Kay 2004; Gedik and Liu 2008) and on providing users with the assurance that the information transmitted about them will not be abused (e.g., Andrade et al. 2002; Xu et al. 2005; Youssef et al. 2005). Such efforts may also draw the mobile application industry's attention to the importance, viability, and plausible ways of incorporating such features.

Implications for Practice

Jules Polonetsky, director and cochair of the Future of Privacy Forum, commented,

> The reality is that companies are getting a huge amount of data and the effort to getting privacy right is just as critical and getting an app to work.…Making sure that users feel mobile devices are becoming more useful to them and are not tracking them is important.…We cannot afford for consumers to have a nagging sense of lack of control for a device that is so personal (Tode 2012).

Our research responds to this call in terms of mobile applications, and alerts various stakeholders, including mobile application developers, mobile phone providers, merchants, advertising companies and their consumers, to important implications for their industry.

For mobile application developers who face mounting pressure to address information privacy issues (Tode 2012), our study provides practical guidance on designing an effective technological solution for the problem we identify, which builds on the notion that the provision of personalization through mobile applications can be achieved without gathering user information into a central server, but by storing and processing user information locally on individuals' own phones. Our approach to validating our design solution may also provide insights to application developers wanting to test the effectiveness of their applications. We developed three mobile advertising application prototypes for our field experiment and launched them simultaneously, with users downloading, installing, and using one of them at random, without being aware of the other two prototypes, using an application versioning approach that is a viable option for developers trying to assess consumers' gratification with an application. Many IT companies have recently attempted to test and market their applications to the user community simultaneously. For instance, at Google, the two phases are virtually indistinguishable from each other, which creates a unique relationship with consumers, who become integrated into the company's development efforts as new products take shape and grow (Iyer and Davenport 2008).

Our study suggests the need to develop mobile handsets, operating system architectures, and application market platforms that together afford stronger protection of users' information and more effective prevention against hacking and unauthorized access at the hardware and architectural levels. This way, mobile application developers can work within enhanced and agreed platforms and architectures to offer effective privacy-safe applications based on our proposed design principle. Our applications leveraged the WebKit sandboxed environment of Apple's iOS platform, which helps protect locally stored user information. Further efforts should be invested to continuously improve platforms and architectures to improve users' psychological comfort and the increase the satisfaction they gain from using applications.

This study contributes to the knowledge stock of mobile phone providers by presenting an architectural design that can be easily adapted to support various "context-aware" personalized services, a capability that builds on an important recent trend among phone providers competing to develop mobile handsets with the most sophisticated personalized features. Every new personalization, such as context-aware personalized services including ring tones customized according to users' moods, and customized speaker volumes based on the background noise levels at the user's location, - is likely to increase users' anxieties about their privacy. Mobile phone providers are not only competing to develop sophisticated personalized services, but at the same time are accusing each other of violating users' privacy in their attempts to win more buyers for their handsets. Our study suggests providers should focus on enhancing their handsets' platforms and operating system architectures by incorporating our proposed design feature for addressing the personalization–privacy paradox.

For marketers (merchants and advertising companies) engaged in mobile advertising campaigns, our study recommends they work closely with those application developers who incorporate privacy-safe features in their application designs. Specifically, given users' heightened concerns about privacy when using such applications, advertisers should delegate the personalization of their advertising messages to application developers, rather than attempting to solicit user information directly for centralized storage, as is typical in Web contexts. On their part, the advertisers must accept that they do not need to know their individual consumers to be able to deliver personalized advertising messages to achieve their desired results, but need to make efforts in raising the interest level of their advertising messages to be delivered via our proposed design, whose principles can be applied not just to smartphones and other mobile devices, but to computing devices generally.

Finally, for consumers, we hope to draw their attention to the option of technological solutions, such as the one demonstrated and validated in this study, which can alleviate their privacy concerns while still affording them the benefits of personalization. Such design solutions may both place less cognitive burdens on them than do existing measures (such as the usually lengthy privacy statements that take time and effort to comprehend fully) but also allow them to feel more secure that their personal information never actually leaves their handsets. Consumers have the right to preserve their own information space; we hope using mobile applications based around our proposed privacy-safe feature may make their mobile computing experiences more gratifying.

Conclusions

Building on the uses and gratifications theory and information boundary theory, this research seeks to exemplify how the fundamental thrust of the personalization–privacy paradox can be addressed effectively through technology. Results from the empirical validation indicate that our privacy-safe solution for delivering personalized advertising messages, which stores and processes consumers' information locally (on their own smartphones) significantly increases both the usage of the application (process gratification) and the saving of adverts (content gratification). Beyond demonstrating how IT solution could be developed to address the personalization–privacy paradox, this research addresses a broader, enduring challenge of how to better understanding consumers' concerns over information privacy in the digital age.

Acknowledgments

The work described in this paper was supported by a grant from the National Natural Science Foundation of China (Grant No. 71102018), a grant from the Research Grants Council of the Hong Kong Special Administrative Region, China (Project No. 149810 (City University of Hong Kong No. 9041612)), and a grant from the Sino-Swiss Science and Technology Cooperation (SSSTC), ETHZ Global (Project No. IP 14-092009).

References

Abrahamson, D. 1998. "The Visible Hand: Money, Markets, and Media Evolution," *Journalism and Mass Communication Quarterly* (75), pp. 14-18.

Andrade, E. B., Kaltcheva, V., and Weitz, B. 2002. "Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Company Reputation," *Advances in Consumer Research* (29), pp. 350-353.

Angst, C., 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.

Angwin, J., and Valentino-DeVries, J. 2011. "Apple, Google Collect User Data," *The Wall Street Journal*, U.S. Edition, April 22 (http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html; accessed July 4, 2011).

Ansari, A., and Mela, C. F. 2003. "E-Customization," *Journal of Marketing Research* (40:2), pp. 131-145.

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

Bargh, M. S., van Eijk, R., Ebben, P., and Salden, A. H. 2003. "Agent-Based Privacy Enforcement of Mobile Services," in *Proceedings of International Conference on Advances in Infrastructure for Electronic Business, Education, Science and Medicine and Mobile Technologies on the Internet*, L'Aquila, Italy.

Brar, A., and Kay, J. 2004. "Privacy and Security in Ubiquitous Personalized Applications," Technical Report No. 561, School of Information Technologies, University of Sydney.

Brusilovsky, P., and Tasso, C. 2004. "Preface to Special Issue on User Modeling for Web Information Retrieval," *User Modeling and User-Adapted Interaction* (14:2-3), pp. 147-157

Bulander, R., Decker, M., Kölmel, B., and Schiefer, G. 2005. "Enabling Personalized and Context Sensitive Mobile Advertising while Guaranteeing Data Protection," in *Proceedings of the EURO-mGOV 2005*, Mobile Government International LLC, Brighton, UK, pp. 445-454.

Chellappa, R. K., and Sin, R. 2005. "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management* (6:2-3), pp. 181-202.

Clifford, S. 2009. "Advertisers Get a Trove of Clues in Smartphones," *The New York Times*, Media & Advertising, March 11 (http://www.nytimes.com/2009/03/11/business/media/11target.html; accessed May 5, 2011).

Culnan, M. J., and Milne, G. R. 2001. "The Culnan-Milne Survey on Consumers and Online Privacy Notices: Summary of Responses," Interagency Public Workshop: Getting Noticed: Writing Effective Financial Privacy Notices, December 4 (http://www.ftc.gov/bcp/workshops/glb/supporting/culnan-milne.pdf).

Cutler, N. E., and Danowski, J. A. 1980. "Process Gratification in Aging Cohorts," *Journalism Quarterly* (57:Summer), pp. 269-277.

DeZoysa, S. 2002. "Mobile Advertising Needs to Get Personal," *Telecommunications: International Edition* (36:2), p. 8.

Dhar, S., and Varshney, U. 2011. "Challenges and Business Models for Mobile Location-Based Services and Advertising," *Communications of the ACM* (54:5), pp. 121-129.

Federal Trade Commission. 2010. "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," Preliminary FTC Staff Report, December (http://ftc.gov/os/2010/12/101201privacyreport.pdf).

Fox, S. 2000. "Trust and Privacy Online: Why Americans Want to Rewrite the Rules," The Pew Internet & American Life Project (available at http://www.pewinternet.org).

Gartner, Inc. 2009. "Gartner's Top Predictions for IT Organizations and Users, 2010 and Beyond: A New Balance," Gartner's Research ID Number: G00173482).

Gedik, B., and Liu, L. 2008. "Protecting Location Privacy with Personalized K-Anonymity: Architecture and Algorithms," *IEEE Transactions on Mobile Computing* (7:1), pp. 1-18.

Ha, L., and James, E. L. 1998. "Interactivity Reexamined: A Baseline Analysis of Early Business Web Sites," *Journal of Broadcasting & Electronic Media* (42), pp. 457-474.

Hann, I. H., Hui, K. L., Lee, T. S. Y., and Png, I. P. L. 2002. "Online Information Privacy: Measuring the Cost-Benefit Tradeoff," in *Proceedings of the 23rd International Conference on Information Systems*, Barcelona, Spain, December 15-18, pp. 1-10.

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

Haselton, T. 2012. "Congress Probes Apple Over Path Address Book Debacle, Apple to Require 'Explicit User Approval,'" TechnoBuffalo, February 15 (http://www.technobuffalo.com/news/congress-probes-apple-over-path-address-book-debacle-apple-to-require-explicit-user-approval; accessed March 23, 2012).

Heerink, M., Kröse, B., Wielinga, B., Evers, V. 2008. "Enjoyment, Intention to Use and Actual Use of a Conversational Robot by Elderly People," in *Proceedings of the 3rd ACM/IEEE International Conference on Human–Robot Interaction*, pp. 113-119.

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

Hutchinson, R. 2011. "50 Percent of iPhone Apps Can Track User Data," Applie News, January 26 (http://www.geeky-gadgets.com/50-percent-of-iphone-apps-can-track-user-data-26-01-2011; accessed July 4, 2011).

Iyer, B., and Davenport, T. H. 2008. "Reverse Engineering Google's Innovation Machine," *Harvard Business Review* (86:4), pp. 56-68.

Jensen, C., Potts, C., and Jensen, C. 2005. "Privacy Practices of Internet Users: Self-Report Versus Observed Behavior," *International Journal of Human Computer Studies* (63:1-2), pp. 203-227.

Kavassalis, P., Spyropoulou, N., Drossos, D., Mitrokostas, E., Gikas, G., and Hatzistamatiou, A. 2003. "Mobile Permission Marketing: Framing the Market Inquiry," *International Journal of Electronic Commerce* (8:1), pp. 55-79.

Klapper, J. T. 1963. "Mass Communication Research: An Old Road Resurveyed," *Public Opinion Quarterly* (27), pp. 515-527.

Lee, O. 2001. *Internet Marketing Research: Theory and Practice*, Hershey, PA: Idea Group Publishing.

Lee, Y. E., and Benbasat, I. 2003. "Interface Design for Mobile Commerce," *Communications of the ACM* (46:12), pp. 49-52.

Lin, C. 1999. "Online Service Adoption Likelihood," *Journal of Advertising Research* (39), pp. 79-89.

Long, J. S., and Freese, J. 2006. *Regression Models for Categorical Dependent Variables Using Stata* (2nd ed.), College Station, TX: Stata Press.

McGuire, W. J. 1974. "Psychological Motives and Communication Gratification," in *The Uses of Mass Communications: Current Perspectives on Gratifications Research*, J. Blumler and E. Kaatz (eds.), Beverly Hills, CA: Sage Publications, pp. 167-196.

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), pp. 100-126.

Peppers, D., and Rogers, M. 1997. *The One to One Future*, New York: Doubleday.

Petronio S. 1991. "Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information between Marital Couples," *Communication Theory* (1), pp. 311-335.

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing* (19:1), pp. 27-41.

Rognehaugh, R. 1999. *The Health Information Technology Dictionary*, Gaithersburg, MD: Aspen.

Rubin, A. M. 1985. "Uses and Gratifications: Quasi-Functional Analysis," in *Broadcasting Research Methods*, J. Dominick and J. Fletcher (eds.), Boston: Allyn and Bacon, pp. 202-220.

Rubin, A. M. 1993. "Audience Activity and Media Use," *Communication Monographs* (60:1), pp. 98-105.

Ruggiero, T. E. 2000. "Uses and Gratifications Theory in the 21st Century," *Mass Communication and Society* (3:1), pp. 3-37.

Sheng, H., Nah, F. F. H., and Siau, K. 2008. "An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns," *Journal of the Association for Information Systems* (9:6), Article 15.

Shi, X. 2006. "Sharing Service Semantics Using SOAP-Based and REST Web Services," *IT Professional* (8), pp. 18-24.

Simonson, I. 2005. "Determinants of Customers' Responses to Customized Offers: Conceptual Framework and Research Propositions," *Journal of Marketing* (69), pp. 32-45.

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

Solove, D. J. 2006. "A Raxonomy of Privacy," *University of Pennsylvania Law Review* (154:3) pp. 477-560.

Song I., LaRose R., Eastin M. S., and Lin C. A. 2004. "Internet Gratifications and Internet Addiction: On the Uses and Abuses of New Media," *Cyberpsychol. Behavior* (7:4), pp. 384-94.

Stafford, M. R., and Stafford, T. F. 1996. "Mechanical Commercial Avoidance: A Uses and Gratifications Perspective," *Journal of Current Issues and Research in Advertising* (18), pp. 27-38.

Stafford, T. F., and Stafford, M. R. 2000. "Consumer Motivations to Engage in Electronic Commerce: Uses and Gratifications of the World Wide Web," in *Electronic Commerce: Opportunities and Challenges*, S. Rahman and M. Raisinghani (eds.), Hershey, PA: Idea Group Publishing.

Stafford, T. F., and Stafford, M. R. 2001. "Investigating Social Motivations for Internet Use," in *Internet Marketing Research: Theory and Practice*, O. Lee (ed.), Hershey, PA: Idea Group Publishing, pp. 93-107.

Stafford, T. F., Stafford, M. R., and Schkade, L. L. 2004. "Determining Uses and Gratifications for the Internet," *Decision Sciences* (35:2), pp. 259-288.

Stanton, J. M. 2003. "Information Technology and Privacy: A Boundary Management Perspective," in *Socio-Technical and Human Cognition Elements of Information Systems*, S. Clarke, E. Coakes, M. Hunter, and A. Wenn (eds.), Hershey, PA: Idea Books, pp. XX-XX.

Stanton, J. M., and Stam K. 2003. "Information Technology, Privacy, and Power Within Organizations: A View from Boundary Theory and Social Exchange Perspectives," *Surveillance and Society* (1:2), pp. 152-190.

Stanton, J. M., and Weiss, E. M. 2000. "Electronic Monitoring in Their Own Words: An Exploratory Study of Employees' Experiences with New Types of Surveillance," *Computers in Human Behavior* (16), pp. 423-440.

Stewart, D. W., and Pavlou, P. A. 2002. "From Consumer Response to Active Consumer: Measuring the Effectiveness of Interactive Media," *Journal of the Academy of Marketing Science* (30:4), pp. 376-396.

Swanson, D. L 1992. "Understanding Audiences: Continuing Contributions of Gratifications Research," *Poetics* (21:4), pp. 305-28.

Tode, C. 2012. "App Developers Face Mounting Pressures on Privacy," Mobile Marketer (http://www.mobilemarketer.com/cms/news/legal-privacy/12143.html; accessed March 23, 2012).

Treiblmaier, H., and Pollach, I. 2007. "Users' Perceptions of Benefits and Costs of Personalization," in *Proceedings of the 28th International Conference on Information Systems*, December 9-12, Montreal, Canada.

Utz, S., and Kramer, N. 2009. "The Privacy Paradox on Social Network Sites Revisited: The Role of Individual Characteristics and Group Norms," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* (3:2).

Venkatesh, V., Speier, C., and Morris, M. G. 2003. "User Acceptance Enablers in Individual Decision Making about Technology: Toward an Integrated Model," *Decision Sciences* (33:2) pp. 297-316.

Vizard, M. 2010. "Personalization vs. Privacy in the Age of the Mobile Web," *IT Business Edge* (http://www.itbusinessedge.com/cm/blogs/vizard/personalization-vs-privacy-in-the-age-of-the-mobile-web/?cs=44892).

Watson, R. T., Pitt, L. L., Berthon, P., and Zinkhan, G. M. 2002. "U-Commerce: Expanding the Universe of Marketing," *Journal of the Academy of Marketing Science* (30:4), pp. 333-347.

West, P. M., Ariely, D., Bellman, S, Bradlow, E., Huber, J., Johnson, E., Kahn, B., Little, J., and Schkade, D. 1999. "Agents to the Rescue?," *Marketing Letters* (10:3), pp. 285-300.

Xu, H. 2007. "The Effects of Self-Construal and Perceived Control on Privacy Concerns," in *Proceedings of 28th International Conference on Information Systems*, December 9-12, Montreal, Canada.

Xu, H., Dinev, T., Smith, H. J., and Hart, P. 2008. "Examining the Formation of Individual's Information Privacy Concerns: Toward an Integrative View," in *Proceedings of 29th Annual International Conference on Information Systems*, December 14-17, Paris, France, Paper 6.

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

Xu, H., Teo, H-H., and Tan, B. C. Y. 2005. "Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk," in *Proceedings of 26th International Conference on Information Systems*, December 11-14, Las Vegas, NV, pp. 897-910.

Yi, M. U., and Hwang, Y. 2003. "Predicting the Use of Web-Based Information Systems: Self-Efficacy, Enjoyment, Learning Goal Orientation, and the Technology Acceptance Model," *International Journal of Human–Computer Studies* (59:4), pp. 431-449.

Youssef, M., Atluri, V., and Adam, N. R. 2005. "Preserving Mobile Customer Privacy: An Access Control System for Moving Objects and Customer Profiles," in *Proceedings of 6th International Conference Mobile Data Management*, pp. 67-76.

Zakaria, N., Stam, K., and Stanton, J. M. 2003. "Exploring Security and Privacy Issues in Hospital Information Systems: An Information Boundary Theory Perspective," *American Medical Informatics Association Annual Symposium: Foundations of Informatics*, Washington, D.C., November 8-12.

Zakaria, N., Stanton, J. M., and Sarker-Barney, S. T. M. 2003. "Designing and Implementing Culturally-Sensitive IT Applications: The Interaction of Culture Values and Privacy Issues in the Middle East," *Information Technology & People* (16:1), pp. 49-75.

Zeng, L. 2011. "More than Audio on the Go: Uses and Gratifications of MP3 Players," *Communication Research Reports* (28:1), pp. 97-108.

About the Authors

Juliana Sutanto is an assistant professor, and Chair of Management Information Systems at ETH Zürich, Switzerland. Her articles have appeared in top-tier information systems conferences and journals such as *Journal of Management Information Systems*, *IEEE Transactions on Engineering Management*, *Information & Management*, and *Long Range Planning*. Her research addresses two related questions: How can organizations successfully implement the information systems? Once it is successfully implemented, how can organizations realize the potential business values of the information systems?

Elia Palme is currently CEO of a Swiss start-up, Newscron AG, a spin-off company of ETH Zürich. Elia received his Ph.D. in Management Information Systems from the ETH Zürich. His research interests include mobile technology design and its impacts on adoption and usage.

Chuan-Hoo Tan is an assistant professor of Information Systems at City University of Hong Kong. His articles have appeared in top-tier information systems conferences and journals such as *Information Systems Research*, *Journal of Management Information Systems*, *IEEE Transactions on Engineering Management*, *Information & Management*, *Decision Support Systems*, and *Long Range Planning*. His current research interests include the design and evaluation of consumer-based decision support interfaces, electronic commerce, and mobile commerce, as well as technology adoption and usage.

Chee Wei Phang is an associate professor at the Department of Information Management and Information Systems, Fudan University. His work has appeared in top-tier information systems journals such as *Journal of the Association for Information Systems*, *IEEE Transactions on Engineering Management*, *Information & Management*, *European Journal of Information Systems*, and *Long Range Planning*. His current research interests include social media, virtual communities, and mobile commerce.

MIS Quarterly

RESEARCH ARTICLE

ADDRESSING THE PERSONALIZATION–PRIVACY PARADOX: AN EMPIRICAL ASSESSMENT FROM A FIELD EXPERIMENT ON SMARTPHONE USERS

Juliana Sutanto
Department of Management, Technology, and Economics, ETH Zürich, Weinbergstrasse 56/58, Zürich, SWITZERLAND {jsutanto@ethz.ch}

Elia Palme
Newscron Ltd., Via Maderno 24, Lugano, SWITZERLAND {elia.palme@newscron.com}

Chuan-Hoo Tan
Department of Information Systems, City University of Hong Kong, Tat Chee Avenue, Kowloon, HONG KONG {ch.tan@cityu.edu.hk}

Chee Wei Phang
Department of Information Management and Information Systems, Fudan University, 670 Guoshun Road, Shanghai, CHINA {phangcw@fudan.edu.cn}

Appendix

Table A1. Post-Experiment Short Survey

Question	Mean (Std Dev.) Responses from Users of the Respective Mobile Advertising Applications		
	Non-Personalized *(34 responses)*	Personalized, Non-Privacy-Safe *(26 responses)*	Personalized, Privacy-Safe *responses)*
Q1. Do you find the advertisements excessive? [Likert scale of 5 with 1 (Not at all) and 5 (Always)]	3.29 (1.088)	3.04 (1.241)	2.77 (1.032)
Q2. Do you find the advertisements annoying? [Likert scale of 4 with 1 (Not at all) and 4 (Very)]	1.53 (.662)	1.44 (.507)	–
Q3. Are you concerned about your personal data when using the application? [Likert scale of 4 with 1 (Not at all) and 4 (Very)]	–	2.64 (1.075)	2.38 (1.329)
Q4. Are you concerned with answering the questions? [Likert scale of 4 with 1 (Not at all) and 4 (Very)]	–	2.32 (1.406)	1.80 (1.118)

Table A2. Construct Measurements

Construct	Measurement items	Source
*For the questions below, "application" refers to the mobile advertising application; and "company" refers to the entity providing the "application"		
Privacy concern [Scale: From "Not at all" to "Very much"] * This construct was measured with respect to each of the followings: 1) Browsing advertisements 2) Viewing advertisements 3) Saving advertisements	1. I am concerned that I could be identified by the company when using the application for [the focal activity]	Chellappa and Sin (2005)
	2. I am concerned with how information about me may be exploited by the company when using the application for [the focal activity]	
	3. I am concerned with how the information captured during my use of the application to perform [the focal activity] can be employed by the company to identify me as an individual	
	4. It bothers me when my personal information is gathered when I use the application for [the focal activity]	
	5. I am concerned that my personal information gathered during my use of the application for [the focal activity] may be accessed by unauthorized people	
	6. I am concerned that my personal information that is captured when I use the application for [the focal activity] may be kept in a non-accurate manner	
	7. To what extent are you concerned that your privacy will be compromised when using the application for the specific activity?	
Sensitivity of information released [Scale: From "Not at all" to "Very much"]	When the application obtains the following information from me, I am concerned that my privacy will be compromised: • Gender • Age • Dietary preference • Daily products used • Preference of soft drink • Preference of snack • Whether consume alcoholic beverages • Advertisements saved into the application	Self-developed
Trust [Scale: From "Strongly disagree" to "Strongly agree"]	1. The company providing the application would be trustworthy in handling my information	Malhorta et al. (2004)
	2. The company providing the application would tell the truth and fulfill promises related to the information provided by me	
	3. I trust that the company providing the application would keep my best interests in mind when dealing with my information	
	4. The company providing the application is in general predictable and consistent regarding the usage of my information	
Reputation [Scale: From "Strongly disagree" to "Strongly agree"]	1. The company providing the app is well-known	Gefen (2000)
	2. I am familiar with the company providing the app	
	3. The company providing the app has a good reputation in the market	
Psychological comfort [Scale: From "Strongly disagree" to "Strongly agree"]	1. I am comfortable providing information to this application in return for personalized advertising messages	Chellappa and Sin (2005)
	2. I feel at ease in using the application to obtain personalized advertising messages	

Table A2. Construct Measurements (Continued)

Construct	Measurement items	Source
Intrusion of personal information boundary [Scale: From "Strongly disagree" to "Strongly agree"]	1. I feel that if I save advertisements into the application, the company may know about me more than I feel at ease with	Xu et al. (2008)
	2. I believe that if I save advertisements into the application, the information about me which I consider should only be kept to myself will be more readily available to others than I would want to	
	3. I believe that if I save advertisements into the application, the information about me is out there that, if used, will invade my boundary of revealing about myself	
	4. I feel that if I save advertisements into the application, my limit of disclosing information about me would be invaded by the company that provides the application	
Personalization benefits [Scale: From "Strongly disagree" to "Strongly agree"]	1. The application provides personalization services that are based on my information	Chellappa and Sin (2005)
	2. The application personalizes my advertisement viewing experience	
	3. The application personalizes the advertising messages for my viewing by acquiring my personal preferences	
	4. The application personalizes and delivers advertising messages to me according to my information	
	5. The application delivers personalized advertising messages to me based on the previous information I indicated	
Perceived effectiveness of privacy-safe feature [Scale: From "Strongly disagree" to "Strongly agree"] *Privacy-safe feature was explained to be the feature that stores user information locally	1. I believe I can preserve my personal information space with the privacy-safe feature.	Adapted from the Privacy control measures (Xu et al. 2008)
	2. I think the privacy-safe feature restricts the release of my information from my mobile phone.	
	3. I believe my information is kept in the mobile phone only to myself with the privacy-safe feature.	
	4. I believe I have control over my information with the privacy-safe feature	
Intention to save advertisements into the application [Scale: From "Strongly disagree" to "Strongly agree"]	1. I would like to save the advertisement I am interested in to the application as soon as I saw it	Adapted from Taylor and Todd (1995)
	2. If possible, I would like to save the advertisement I am interested in to the application at the moment I saw it	
	3. In near future, I would like to save the advertisement of interest to me into the application as much as possible	

Table A3. Reliability, Convergent Validity, and Discriminant Validity Test Results of the Constructs

	Cronbach's Alpha	Composite Reliability	AVE	Inter-construct Correlation*						
				1	2	3	4	5	6	7
Ad. saving intention	0.78	0.87	0.69	0.83						
Psychological comfort	0.84	0.92	0.86	0.39	0.93					
Boundary intrusion	0.94	0.95	0.83	-0.24	-0.30	0.91				
Personalization benefits	0.86	0.90	0.64	0.40	0.45	-0.17	0.80			
Privacy-safe feature	0.95	0.96	0.86	0.44	0.38	-0.21	0.45	0.93		
Trust	0.88	0.92	0.74	0.47	0.54	-0.29	0.45	0.58	0.86	
Reputation	0.88	0.92	0.80	0.38	0.35	-0.04	0.21	0.31	0.38	0.89

*Diagonal cells represent the square-root of AVE of the respective construct

Table A4. Factor Analysis Results

	Component						
	1	2	3	4	5	6	7
Personalization_benefit1	.213	.022	.766	-.050	-.005	.124	.271
Personalization_benefit2	.148	-.102	.704	-.076	-.082	.171	.277
Personalization_benefit3	.127	.094	.807	.335	.143	.044	-.001
Personalization_benefit4	.084	.055	.835	.249	.137	.109	-.081
Personalization_benefit5	.218	-.361	.640	.104	.034	.152	.164
Boundary_intrusion1	-.229	.835	-.059	-.124	.055	-.070	-.164
Boundary_intrusion2	-.007	.941	-.040	-.043	-.053	-.099	-.055
Boundary_intrusion3	.063	.911	-.005	-.084	-.006	-.016	.032
Boundary_intrusion4	-.056	.920	.004	-.110	.022	-.097	-.093
Privacy_safe1	.837	-.133	.253	.158	.059	.161	.102
Privacy_safe2	.875	-.089	.233	.179	.052	.150	.128
Privacy_safe3	.862	-.044	.150	.236	.161	.158	.050
Privacy_safe4	.873	.020	.072	.179	.204	.090	.067
Trust1	.292	-.054	.178	.575	.177	.394	.348
Trust2	.379	-.048	.190	.649	.131	.246	.343
Trust3	.237	-.139	.205	.814	.087	.003	.039
Trust4	.178	-.209	.030	.800	.123	.081	.150
Reputation1	.070	.002	-.050	.150	.896	.059	.072
Reputation2	.124	.054	.063	.114	.870	.185	.087
Reputation3	.199	-.048	.148	.046	.800	.159	.165
Psychological_comfort1	.125	-.039	.174	.276	.235	.088	.778
Psychological_comfort2	.130	-.271	.263	.171	.145	.124	.778
Ad_saving1	.071	-.019	.184	-.019	.330	.766	.123
Ad_saving2	.206	-.163	.222	.072	.113	.821	-.051
Ad_saving3	.217	-.123	.062	.268	.039	.697	.182

Table A5. Sensitivity with Disclosing Different Information

	Mean	Std. Deviation
Gender	2.7 | 2.7	1.53 | 1.53
Age	3.3 | 2.9	1.67 | 1.52
Dietary preferences	2.6 | 2.7	1.46 | 1.44
Daily product consumed	3.2 | 3.2	1.65 | 1.51
Alcohol consumed	3.2 | 2.9	1.65 | 1.53
Advertisements saved	4.2 | 3.9	1.88 | 1.72

*Privacy concerns attached by users (non-privacy-safe (N=80) | Privacy-safe (N=113))

Table A6. Information Privacy Concern with Performing Different Activities

	Mean	Std. Deviation
Browsing adverts.	5.2 | 5.2	1.25 | 0.99
Viewing adverts.	5.4 | 5.3	1.09 | 0.92
Saving adverts.	5.6 | 5.3	0.98 | 1.06

*Privacy concerns attached by users (non-privacy-safe (N=80) | Privacy-safe (N=113))

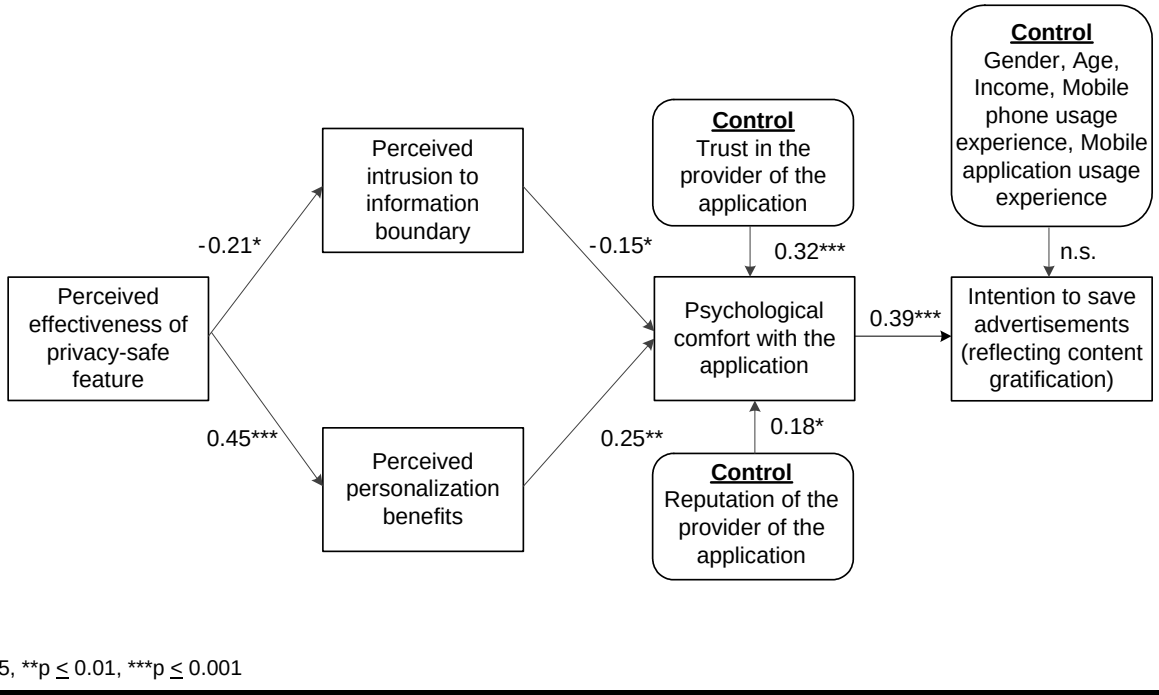


Figure A1. Statistical Test Results of the Effects of Privacy-Safe Feature

References

Chellappa, R. K., and Sin, R. 2005. "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management* (6:2-3), pp. 181-202.

Gefen, D. 2000. "E-Commerce: The Role of Familiarity and Trust," *Omega* (28:5), pp. 725-737.

Malhotra, N., Kim, 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.

Taylor, S., and Todd, P. A. 1995. "Understanding Information Technology Usage: A Test of Competing Models," *Information Systems Research* (6:2) , pp. 144-176.

Xu, H., Dinev, T., Smith, H. J., and Hart, P. 2008. "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," in Proceedings of the 29th International Conference on Information Systems, December 14-17, Paris, France, Paper 6.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 423 866 A1**

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
29.02.2012 Bulletin 2012/09

(51) Int Cl.:
G06Q 30/00 *(2012.01)*

(21) Application number: **10008973.9**

(22) Date of filing: **30.08.2010**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR
Designated Extension States:
BA ME RS

(71) Applicant: **ETH Zurich**
8092 Zürich (CH)

(72) Inventors:
- **Palme, Elia**
  6913 Carabbia (CH)
- **Gasimov, Anar**
  1009 Pully (CH)
- **Sutanto, Juliana**
  8047 Zürich (CH)
- **Magagna, Fabio**
  6460 Altdorf (CH)

(54) Method and devices for targeted distribution of data

(57) A network server (2) distributes data objects comprising user data and match estimator instructions via a telecommunication network (3) to a plurality of communication terminals (4, 4') for rendering the user data at the communication terminals (4, 4'). Based on locally stored user profile data, the communication terminals (4, 4') compute an affinity value according to the match estimator instructions. Depending on the computed affinity value, the communication terminals (4, 4') select in each case the user data to be rendered. Thus, the invention makes possible targeted distribution of user data whereby the distribution/selection strategy is controlled centrally by the network server (2). At the same time, privacy of the users is guaranteed since, from outside of the communication terminal (4, 4'), it is neither possible to access the local user profile data, nor is it possible to track which user data is actually selected and rendered.

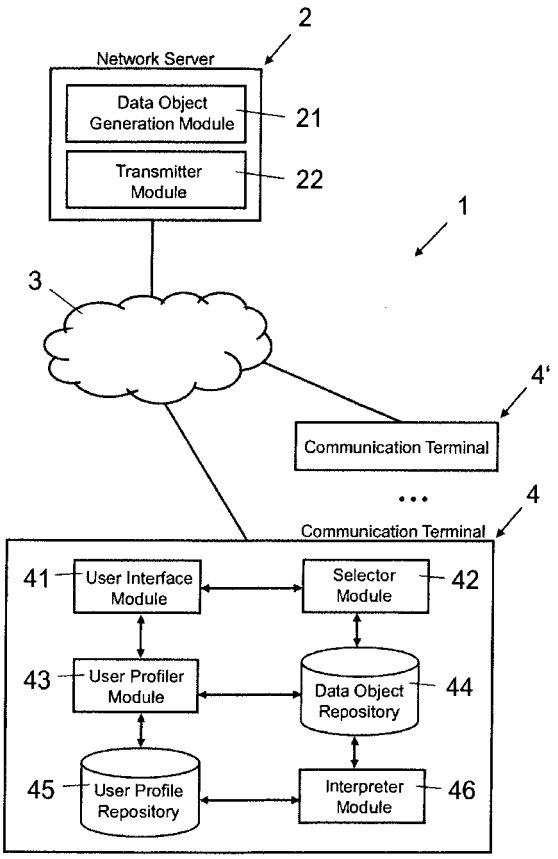


Fig. 1

EP 2 423 866 A1

Description

Field of the Invention

[0001] The present invention relates to the targeted distribution of data via telecommunication networks. Specifically, the present invention relates to a method and devices for distributing data to a plurality of communication terminals for rendering selectively the data at the communication terminals.

Background of the Invention

[0002] The continuing expansion of the Internet has led to the widespread practice of electronic distribution of data such as e.g. multimedia files, digital advertisement, or software in general. The publish/subscribe model is one method of distributing data over the Internet. In this model, a user may decide to subscribe to a certain service based on his preferences. Whenever new content, e.g. news, stock market data or other information, is available, the service will send the new content to the user. For many application scenarios such as mailing groups and newsletters, it has turned out that this kind of targeted distribution of data is more effective than simply broadcasting the data to all users.

[0003] Another example of targeted distribution of data is targeted advertisement. The goal of targeted advertising is to present captivating advertisement only to those customers which are in the marketing target of a certain product. Only if the user is potentially interested in the product according to his user profile, the advertisement is presented to the user.

[0004] However, in many scenarios targeted information dissemination relies on local and personal user information. In those scenarios, users are concerned about their personal data, and privacy becomes an important issue that needs to be taken into account. The most common solution to protect the privacy of a user communicating with e.g. a network server is to use a third trusted party component. A third trusted party component is an actor which is supposed to be secure and trusted and helps to establish a secure data transfer between the user and the network server.

[0005] US2005/0038698A1 describes a computer which receives an advertisement together with a target profile via a communication network. The computer logs user activities, e.g. visited web sites of a user and stores the logged user activities in a local user profile. Moreover, the local user profile may comprise user-specified criteria pertaining to which advertisements are to be shown on the computer. If user activities specified in the target profile are contained in the user profile of the computer, the computer may display an advertisement on a monitor. The user of the computer is provided with an editing interface to make changes to the user profile by deleting and/or adding information to the user profile.

[0006] US2008/0004954A1 describes a method that facilitates advertising on a computer system. For this purpose, the operating system of the computer and client applications, such as computer games or word processors, are used to present the advertisement. The computer system receives advertisement content from an advertisement server. A local analysis on the computer system considers e.g. personal content and activities of the user of the computer system. The latter information is used by local learning, reasoning and matching methods to select which advertisement content is inserted into the client application for presentation and where the advertisement content is displayed in the client application. Hence, the computer system controls autonomously which and how the received advertisement is presented.

[0007] US2006/0265283A1 describes a computer system including a web browser toolbar that collects information on the preferences of a user based on the user's online activities. The web browser toolbar includes a user interface configured to receive a query from a user and to transmit the received query to a web search engine. Based on e.g. the input search terms, the web search engine analyzes the preferences of the user and determines advertisement targeted at the preferences of the user. The determined advertisement is then displayed in a browser. When the user uses a displayed link in the advertisement to access an advertiser's website and generates revenue for the advertiser, the advertiser initiates a payment to the operator of the web search engine.

[0008] Thus, in systems for targeted distribution of data known from state of the art, the selection of data is controlled locally by the communication terminals or performed externally by a third party. In the latter case, privacy strongly depends on the reliability and trustworthiness of the third party.

Summary of the Invention

[0009] It is an object of this invention to provide a method and devices for distributing data to a plurality of communication terminals for selective rendering of the data by the communication terminals.

[0010] According to the present invention, these objects are achieved through the features of the independent claims. In addition, further advantageous embodiments follow from the dependent claims and the description.

[0011] According to the present invention, the above mentioned objects are particularly achieved in that for distributing data from a network server to a plurality of communication terminals for rendering the data at the communication terminals, the communication terminals in each case receive from the network server via a telecommunication network a data

object comprising user data and match estimator instructions. At the communication terminals, the user data and the match estimator instructions are extracted from the data object, and an affinity value is computed according to the match estimator instructions based on user profile data stored at the communication terminal. Specifically, the affinity value is computed by interpreting or executing the match estimator instructions. Depending on the computed affinity value, the communication terminals select in each case user data to be rendered by the communication terminal. Thus, the invention makes possible targeted distribution of user data from a central network server to communication terminals whereby the distribution/selection strategy is controlled centrally by the network server. At the same time, privacy of the users is guaranteed since, from outside of the communication terminal, it is neither possible to access the local user profile data, nor is it possible to track which user data is actually selected and rendered. Due to the distributed computation of affinity values, only a comparatively simple infrastructure of the network server is required and the number of communication terminals is highly scalable.

[0012] In an embodiment, the communication terminal executes or interprets the match estimator instructions for computing the affinity value by combining and weighting values of the user profile data. Thus, it is possible to design sophisticated selection strategies at the central network server for automated, distributed selection of user data at the communication terminals.

[0013] In a preferred embodiment, the communication terminal determines from the data object the user profile data required for computing the affinity value. Hence, an automated mechanism is provided for generating the user profile data at the communication terminals as needed for computing the affinity values for specific user data.

[0014] In another embodiment, the communication terminal requests the user of the communication terminal via a user interface to enter the user profile data required by the match estimator instructions for computing the affinity value. Thus, it is possible to dynamically update and extend the user profile stored at the communication terminal as needed for computing the affinity values for specific user data.

[0015] In yet another embodiment, the communication terminal stores the data objects received from the network server in a data object repository, stores the affinity value assigned to the respective data object in the data object repository, continuously monitors the data object repository and selects, depending on the affinity values assigned to the data objects, the user data to be rendered by the communication terminal. Thus, it is possible to dynamically evaluate new data objects and new user profile data in order to select user data for rendering.

[0016] In another embodiment the communication terminal executes the match estimator instructions for computing a certitude value which indicates reliability of the computed affinity value, and selects, depending on the affinity value and the certitude value, the user data to be rendered by the communication terminal. Thus, a more differentiated and flexible selection of user data becomes possible and the handling of missing user profile data is facilitated by computing the certitude value depending on the user profile data required for computing the affinity value and available at the communication terminal.

[0017] In addition to a method of distributing user data to a plurality of communication terminals for rendering selectively the user data at the communication terminals, the present invention also relates to a network server which is configured to generate data objects comprising user data and match estimator instructions, whereby the match estimator instructions are configured to instruct a communication terminal to compute affinity values based on user profile data locally stored at the communication terminal. The network server is further configured to transmit the data object via a telecommunication network to the communication terminal for enabling the communication terminal to select user data to be rendered depending on the computed affinity value.

[0018] In addition to a method and network server for distributing user data to a plurality of communication terminals for rendering selectively the user data at the communication terminals, the present invention also relates to a computer program product comprising computer program code; particularly, a computer program product comprising a tangible computer-readable medium having the computer program code stored thereon. The computer program code directs one or more processors of a communication terminal, such that the communication terminal receives via telecommunication network from a network server a data object comprising user data and match estimator instructions, and extracts the user data and the match estimator instructions from the data object. Moreover, the computer program code directs the one or more processors of the communication terminal, such that the communication terminal computes an affinity value according to the match estimator instructions based on user profile data stored at the communication terminal, selects the user data to be rendered by the communication terminal depending on the computed affinity value, and renders the selected user data.

Brief Description of the Drawings

[0019] The present invention will be explained in more detail, by way of example, with reference to the drawings in which:

Figure 1 shows a block diagram illustrating schematically a system for transmitting user data from a network server to a communication terminal for selective rendering of the user data by the communication terminal based on local

user profile data.

Figures 2 to 4 show flow diagrams illustrating examples of sequences of steps performed by a communication terminal for receiving user data from a network server and for selective rendering of the user data based on local user profile data.

Detailed Description of the Preferred Embodiments

[0020] In Figure 1, reference numeral 1 refers to a system for transmitting user data from a network server 2 to communication terminals 4 for selective rendering of the user data by the communication terminals 4. The system comprises a network server 2 and a plurality of communication terminals 4, 4' which are connected to the network server 2 via, e.g. direct communication links or a telecommunication network 3.

[0021] The network server 2 includes one or more operational computers with one or more processors. Furthermore, the network server 2 includes various functional modules, including a data object generation module 21 and a transmitter module 22. The transmitter module 22 is configured to transmit data objects generated by the data object generation module 21 via a direct communication link or the telecommunication network 3 to one or more communication terminals 4, 4'.

[0022] The telecommunication network 3 comprises a fixed communication network and/or a mobile radio communication network. Preferably, the telecommunication network 3 comprises the Internet.

[0023] The communication terminal 4, 4' includes one or more processors. The communication terminal 4, 4' is, for example, a fixed or mobile personal computer, a smart phone, a cellular phone, or a personal digital assistant (PDA) for data communication. For example, the communication terminal 4, 4' is a mobile phone or a mobile computer connected to a WLAN (Wireless Local Area Network), or equipped with other communication modules for mobile communication, compliant to standards such as GSM (Global System for Mobile Communication) or UMTS (Universal Mobile Telecommunication System).

[0024] Moreover, the communication terminal 4, 4' includes various functional modules, including a user interface module 41, a selector module 42, a user profiler module 43, and an interpreter module 46. The communication terminal 4, 4' further includes a user profile repository 45 such as a memory subsystem, a data base system or another system for efficient storage of user profile data. The data object repository 44 includes a memory subsystem, a data base system or another system for efficient storage of e.g. received data objects as well as computed affinity and certitude values assigned in each case to a data object. For privacy and data confidentiality reasons the user profile repository 45 and the data object repository 44 are not accessible for reading from outside of the communication terminal 4, 4'.

[0025] The communication terminal 4, 4' further includes a user interface which is controlled by the user interface module 41. The user interface comprises conventional devices for input and output of data. For example, the devices for input of data include a keyboard, keypad, mouse, joystick or touch screen monitor and devices for output of data include a monitor, loudspeaker or - for the case of a fixed personal computer - a printer.

[0026] Preferably, the functional modules are implemented as programmed software modules comprising computer program code for directing a processor of a computer or communication terminal 4, 4', respectively, to perform functions as described later in more detail. The computer program code is stored on a tangible computer-readable medium which is connected fixed or removably to the respective processor(s). One skilled in art will understand, however, that in alternative embodiments the functional modules may be implemented fully or at least partly by way of hardware components.

[0027] In the following paragraphs, described with reference to Figures 2 to 4 are possible sequences of steps performed by the functional modules for distributing user data from the network server 2 to the communication terminals 4, 4' for selective rendering of user data by the communication terminals 4, 4'.

[0028] In Figure 2 to 4, all steps are performed by the functional modules of the communication terminal 4, 4'.

[0029] In optional step S1 in Figure 2, the communication terminal 4, 4' sends a request to the network server 2 for requesting the network server 2 to transmit one or more data objects to the communication terminal 4, 4' (pull mode). In another embodiment, the network server 2 proactively transmits data objects to the communication terminal 4, 4' (push mode).

[0030] The data object includes for example a mobile agent comprising data and software (executable and/or interpretable code). The data object is forwarded through the telecommunication network 3 or a direct connection to the communication terminal 4, 4'. However, to avoid security risks and protect the privacy of the user, once the data and software contained in the data object is extracted at a communication terminal 4, 4' (see step S23) and the software is executed/interpreted, the data object is not transmitted again by the communication terminal 4, 4' (for example to another communication terminal 4, 4').

[0031] In step S2, a data object transmitted from the network server 2 is received by the communication terminal 4, 4'. In Figure 3, the receiving of a data object by the communication terminal 4, 4' is explained in more detail, by subdividing

step S2 into steps S21 to S25.

[0032] Table 1 illustrates an exemplary structure of a data object including user data, match estimator instructions, an expiration date, a digital signature, and an optional evaluation profile.

Table 1

Data Object				
User Data	Match Estimator Instructions	Expiration Date	Digital Signature	Evaluation Profile

[0033] The user data comprises data and information sent from the central server 2 to the communication terminals 4, 4'. The user data can be seen as payload of the data object the content of which is not necessarily associated with the user of the communication terminal 4, 4'. The user data includes data files and/or executable files for various purposes such as information, entertainment or advertisement. Examples for user data include digital multi-media files (audio, image and video files), e-mail, rich text files, Portable Document Format (PDF) files and Hypertext Markup Language (HTML) documents. Moreover, the user data includes software applications for example games. Further examples for user data include references to external documents for example hyper text links to web pages. External documents are provided e.g. by the network server 2, the telecommunication network 3 and/or the Internet.

[0034] Preferably, the user data does not contain references or links to external documents or services, i.e. the user data is completely embedded in the data object. For instance, small data items (e.g. images) are included as embedded data in HTML documents, according to the definition of the Uniform Resource Locator (URL) scheme "data" in RFC 2397 of the Internet Society (ISOC). Hence, the privacy of the user is protected since it is not possible to track which user data is selected and rendered by the user of the communication terminal 4, 4'. Since no external web content is downloaded by the communication terminal 4, 4', the security is increased since no malicious scripts, web viruses or the like can be downloaded from the Internet. Furthermore, additional internet traffic and costs are avoided since no further internet connections are required.

[0035] The match estimator instructions include executable and/or interpretable files which cause the interpreter module 46 of the communication terminal 4, 4' to perform tasks according to the encoded instructions. In a preferred embodiment, the match estimator instructions include a scripting language source file (such as a JavaScript source file) to control one or more software applications at the communication terminal 4, 4'. Alternatively, match estimator instructions include a file containing instructions (such as bytecode) for a software interpreter. In a variant, match estimator instructions also include machine code instructions executable by one of the physical processors of the communication terminal 4, 4'.

[0036] Preferably, match estimator instructions are written in the JavaScript scripting language. Since many mobile platforms are offering Application Programming Interfaces (API) to run JavaScript source files in a sandboxed environment, this embodiment constitutes a secure, fast and effortless solution. Furthermore, when using JavaScript based match estimator instructions and HTML encoded user data, the same instance of a WebKit engine can be used for (a) executing the match estimator instructions and (b) rendering the user data on a screen of the communication terminal 4, 4'. In this way, memory requirements of applications running at the communication terminal 4, 4' are reduced.

[0037] The expiration date comprises an absolute or relative time value after which the data object or parts of the data object are removed from the communication terminal 4, 4'. The digital signature certifies that the data object and its content are genuine and stem from a trustable source.

[0038] In general, the evaluation profile includes (a) specifications which user profile elements are retrieved from the user of the communication terminal 4, 4' and stored in the user profile repository 45 and (b) how the respective user profile data is retrieved from the user. Hence, the evaluation profiles sent from the network server 2 explicitly or implicitly define the structure and the content of the user profile data stored in the user profile repository 45 at the communication terminal 4, 4'.

[0039] Table 2 illustrates an exemplary structure of the evaluation profile, including entries with a name element, a question element and an answer element.. The illustrated evaluation profile defines how the user profiler module 43 collects user profile data by interacting with the user interface module 41 and the user profile repository 45.

Table 2

Evaluation Profile		
Name	Question	Answer
...	...	...
Name	Question	Answer

[0040] The name element indicates the content of the respective entry. Examples for names include e.g. "Age", "Gender", "Religion", "Food pattern", "Nationality", "Language", "Residence Location" or "Current Location". For a question element in the evaluation profile, there are entries with a plurality of possible answer elements. As will be explained later in more detail, the user profiler module 43 creates data records at the user profile repository 45. The data records comprise user profile elements according to the evaluation profile. As illustrated in Table 3, the user profile element comprises a name element (which is identical to the name element of the evaluation profile) and a value element.

Table 3

User Profile Element	
Name	Value
...	...
Name	Value

[0041] The user profiler module 43 asks the user via the user interface module 41 the question and the user chooses one or more of the possible answers. For example, the entry of the evaluation profile with the name element "Gender" is associated with the question element "What is your gender?" and with two possible answer elements "Male" and "Female". The question "How old are you?", for example, has the following answer elements: "<18", "18-30", or ">30". The answer chosen by the user is stored by the user profiler module 43 as value element of a user profile element with the respective name. As will be explained later in more detail, the match estimator instructions will compute the affinity value and the certitude value of a received data object from the value elements stored at the user profile repository 45.

[0042] Optionally, the evaluation profile includes instructions for instructing the user profiler module 43 of the communication terminal 4, 4' to retrieve user profile data without directly querying the user via the user interface module 41. Instead, the user profile profiler is instructed to log user statistics during operation of the communication terminal 4, 4'. Such user statistics include logging visited web sites, software applications used, web searches performed and/or email usage. Furthermore, the user profiler module 43 logs which user data received from the network server 2 has been selected and rendered by the communication terminal 4, 4'. In addition, the user profile module 43 receives data from e.g. a Global Positioning System (GPS) about the current location of the communication terminal 4, 4'. The location is stored in the user profile repository 45 to collect statistics about e.g. preferred locations of the user.

[0043] In Figure 3, the data object is received in step S21. In optional step S22, using the digital signature, the communication terminal 4, 4' verifies that the data object is genuine and received from a certified source.

[0044] In step S23, the interpreter module 46 extracts the user data, the match estimator instructions, the expiration date, the digital signature, and the evaluation profile from the received data object.

[0045] Subsequently, in step S24, the extracted user data, match estimator instructions, expiration date, digital signature and evaluation profile are stored in the data object repository 44. Specifically, the user data, match estimator instructions, expiration date, digital signature and evaluation profile are stored in a suitable data structure (e.g. a record or an array) such that the user data, match estimator instructions, expiration date, digital signature and evaluation profile are assigned to each other.

[0046] Optionally, in optional step S25, no or only some evaluation profiles are contained in the data object and received by the communication terminal 4, 4'. The interpreter module 46 determines the required user profile data e.g. by analyzing the match estimator instructions. The interpreter module 46 further requests additional evaluation profiles from the network server 2. When the network server 2 transmits the requested evaluation profiles to the communication terminal 4, 4', an additional digital signature is transmitted with the requested evaluation profiles in order to guarantee their authenticity.

[0047] Alternatively, the evaluation profile is encoded in the match estimator instructions and the interpreter module 46 determines the evaluation profile by decoding the evaluation profile in the match estimator instructions.

[0048] In step S3 of Figure 2, the user profiler module 43 is populating the user profile repository 45 according to the evaluation profile stored in the data object repository 44. Figure 4 displays a more detailed sequence of steps S31 to S36 for populating the user profile repository 45.

[0049] In step S31, the user profiler module 43 analyzes the user profile data stored at the user profile repository 45 and the evaluation profile stored at the data object repository 44. Based on this analysis, the user profiler module 43 decides for each data object which user profile data is required as input to execute the match estimator instructions.

[0050] In step S32, the user profiler module 43 checks for each data object stored at the data object repository 44 whether a corresponding data record at the user profile repository 45 exists. The data record comprises e.g. user profile elements according to the evaluation profile. If no corresponding data record exists, in step S33, the user profiler module 43 generates a new data record according to the evaluation profile and corresponding to the data object in the user

profile repository 45.

[0051] In step S34, the user profiler module 43 checks for each data object stored at the data object repository 44 whether the user profile data in the user profile repository is sufficient for the computation of the match estimator instructions.

[0052] For example, the decision whether the user profile data is sufficient depends on the certitude value which is computed from the user profile data by executing the match estimator instructions. As will be explained later in more detail (see step S4), the certitude value is stored in the data object repository 44 and associated with the data object. If the certitude value is e.g. higher than a certain minimum certitude value, the user profile data is regarded as sufficient.

[0053] If the user profile data is not sufficient, step S35 is executed. In step S35, the user profiler module 43 is populating the user profile repository 45. As already mentioned the user profiler module 43 asks the user via the user interface module 41 questions and provides possible answers according to the evaluation profile. The selected answers are stored as values of a user profile element in the user profile repository 45.

[0054] If the user profile data is sufficient in optional step S36, the user profiler module 43 updates the user profile data in the user profile repository 45. Updating the user profile data includes asking the user of the communication terminal the same questions again and/or collecting new user statistics. In this way, the user profiler module 43 accounts for changing habits or preferences of the user.

[0055] Since there may be several applications running at the communication terminal 4, 4' and the user of the communication terminal 4, 4' may be interactively working with the user interface module 41, the user profiler module 43 chooses a suitable point in time to query the user using a question according to the evaluation profile.

[0056] Optionally, the user profiler module 43 also decides in which order questions are asked to the user of the communication terminal 4, 4'. For this purpose, the user profiler module 43 estimates e.g. the importance of user profile data by identifying user profile data which is required by a plurality of data objects to run the match estimator instructions. The user profiler module 43 further accelerates the retrieval of missing user profile data according the estimated importance.

[0057] In step S4, the interpreter module 46 executes or interprets the match estimator instructions. Pseudocode A shows an exemplary pseudocode of the function evaluate() which is executed in step S41 for computing the affinity and certitude values of a data object. The computed affinity and certitude values are integer numbers between 0 and 6, for example. In general, the affinity value and the certitude value comprise Boolean, integer and real numbers.

```
1  function evaluate(){
2      //Default affinity and certitude values
3      affinity = 0;
4      certitude = 3;
5      //Check the age of the user
6      if (repository['Age'] != undefined){
7          //User data is targeted at young adults
8          if (repository['Age'] = '<18'){
9              affinity += 0;
10             certitude += 2;}
11         if (repository['Age'] = '18-30'){
12             affinity += 4;
13             certitude += 2;}
14         if (repository['Age'] = '>30'){
15             affinity += 3;
16             certitude += 2;}
17     }else{certitude -= 2;}
18     //Check the gender of the user
19     if (repository['Gender'] != undefined){
20         //User data is targeted at males
```

(continued)

21	if (repository['Gender'] = 'Male){
22	affinity += 2;
23	certitude += 1;
24	}else{
25	affinity += 1;
26	certitude += 1;
27	}else{
28	certitude -= 1;}
29	return affinity;
30	return certitude;}

Pseudocode A

[0058] In the exemplary Pseudocode A, a high affinity value indicates that the user data contained in the data object may be of high interest to the user. As will be explained later in more detail, the maximum possible affinity value for this data object is 6. The certitude value indicates to what extent the required user profile data in the user profile repository 45 is complete and, hence, the reliability of the respective affinity value. A high certitude value indicates that the computed affinity value exhibits a high reliability. The maximum possible certitude value for this data object is also 6.

[0059] In lines 3 and 4 of Pseudocode A, the affinity value and the certitude value are initialized and assigned the default values 0 and 3, respectively.

[0060] In line 6, the interpreter module 46 examines whether the user profile element with the name "Age" exists in the user profile repository 45 and whether the value element has been determined by the user profiler module 43. In other words, the interpreter module 46 examines whether the user profiler module 43 has successfully queried the age of the user. If the user profile element with the name "Age" exists, the affinity and certitude values are incremented dependent on the age of the user. In lines 8, 11, and 14, the interpreter module 46 tests whether the user's age is below 18, between 18 and 30, or over 30 and increments the affinity value and the certitude value dependent on the user's age. If the value element of the user profile element with the name "Age" is not available, the certitude value is decremented by 2 in line 17.

[0061] Accordingly, in line 19, the interpreter module 46 examines whether the user profiler module 43 has successfully queried the gender of the user, and increments the affinity value and the certitude value dependent on the user's gender in lines 22, 23, 25, and 26. If user profiler module 43 did not manage to query the gender of the user and store the respective user profile element, the certitude value is decremented by 1 in line 28. In line 29 and 30, the computed affinity and certitude values are returned.

[0062] If the user is male and between 18 and 30 years old, the affinity value reaches its maximum value 6. If, for example, the user profile data specifies that the user is a female and older than 30 years, the computed affinity value is 4.

[0063] For example, the user data comprises digital advertisement for a product, the user of the communication terminal 4, 4' is a potential customer and a high affinity value indicates that the user is in the marketing target of the product.

[0064] In the exemplary Pseudocode A, the age of the user is of greater importance for deciding whether to render the user data than the gender of the user. Hence, the certitude value is incremented/decremented by 2 if the age of the user is known/unknown and only incremented/decremented by 1 if the gender of the user is known/unknown, respectively.

[0065] Match estimator instructions as the ones in Pseudocode1 facilitate a great flexibility in computing affinity and certitude values from the user profile data available at the user profile repository 45. Using an interpretable/executable code, numerous strategies become possible how user data is distributed for selective rendering at the communication terminals 4, 4'. In more sophisticated implementations, various weighting factors, conditions and mathematical formulas are used to compute the affinity values and certitude values.

[0066] For example, user data containing an invitation to a social event is targeted to persons older than 30 years. However, females are also allowed to join the social event if the are younger, e.g., older than 18. Suitable match estimator instructions can easily be designed. Pseudocode B shows a corresponding evaluate()-function.

1	function evaluate(){
2	//Default affinity and certitude values

(continued)

3	affinity = 0;
4	certitude = 3;
5	//Check the age and the gender of the user
6	if (repository['Age') = '>30' OR
7	(repository['Gender'] = 'Female' AND repository['Age'] = '18-30')){
8	affinity += 6;
9	certitude += 3;}
10	return affinity;
11	return certitude;}

Pseudocode B

[0067] In step S42, the interpreter module 46 stores the computed affinity and certitude value in the data object repository 44 such that the affinity value and the certitude value are assigned to the respective data object.

[0068] In step S5, the selector module 42 selects which and how user data stored at the data object repository 44 is rendered based on the affinity and certitude values associated with the user data. A user data selection algorithm is performed in order to compute whether and how user data is rendered.

[0069] For example, an initial screening is performed to identify the user data with a certitude value higher than a minimum certitude value. The minimum certitude value is e.g. a fixed threshold value which depends on the maximum possible certitude value. Alternatively, the minimum certitude value is received within the data object from the network server 2 or is specified by the user of the communication terminal 4, 4' via the user interface module 41. In the following, only user data with a certitude value higher than the minimum certitude value is considered.

[0070] In a next step, the selector module 42 decides dependent on the affinity value, the type of the user data and other applications running on the communication terminal 4, 4', whether and how the user data is rendered. For example, a minimum affinity value is used as threshold value to decide whether user data is rendered. Again, the minimum affinity value depends on the maximum achievable affinity value. If the affinity value is high enough, the respective user data is rendered for a certain amount of time according the affinity value. For example, an image file containing digital advertisement with a high affinity value is rendered for a longer period of time than image files with low affinity values.

[0071] In another embodiment, the selector module 42 further schedules when the user data is rendered based on the information available to the selector module 42. For example, certain user data is rendered at a particular time of the day.

[0072] In step S6, the communication terminal 4, 4' checks whether user data has been selected for rendering.

[0073] If user data has been selected for rendering by the selector module 42, the respective user data is rendered in step S7 by the user interface module 43. One or more of the devices for input and output of data are used for rendering of the user data. For example, information contained in the user data pops up in a pop up window on a screen. The size, position and duration of rendering of the popup window are determined by the selector module 42 and depend on, e.g., the affinity value associated with the user data. Alternatively, a digital advertisement is rendered in a small banner on the screen.

[0074] As already mentioned, the selector module 42 decides dependent on e.g. media type and affinity value of the user data how the user data is rendered. For example, text information and images are printed on a printer connected to the communication terminal 4, 4'.

[0075] Optionally, the process of rendering user data also involves interaction with the user of the communication terminal 4, 4'. For this purpose, devices for input of data are used. For example, the process of rendering user data involves displaying a list of user data ready for rendering on the screen. The user selects specific user data to activate the rendering of the specific user data on the screen.

[0076] After the user data is rendered in step S7 or if no user data is selected by the selector module 42 in step S5, the communication terminal 4, 4' proceeds to request new data objects from the network server 2 in step S1. In further embodiments of the present invention, as indicated by the dashed arrows in Figure 2, a computer program running at the communication terminal 4, 4' alternatively loops back to steps S3, S4 or S5.

[0077] In Figure 2, steps S1 to S7 are executed as a sequential program. In yet another embodiment of the present invention, the computer program is implemented in form of independent processes with appropriate inter-process communication using the data object repository 44 and the user profile repository 45 as shared memories. For example, a first process is responsible for receiving data objects from the network server 2 and storing the data objects in the data

object repository 44 (steps S1 and S2). While a second process is populating the user profile repository 45 by querying the user via the user interface module 41 (step S3), a third process is executing match estimator instructions based on the user profile data stored in the user profile repository 45 and storing the computed affinity values in the data object repository 44 (step S4). Finally, a forth process is selecting, based on the affinity values and certitude values in the data object repository 44 which user data is rendered by the user interface module 41 (steps S5, S6, S7).

[0078] The above mentioned four processes are repeatedly executed. Specifically, the second process monitors the user profile repository 45 for missing user profile data and updates the user profile repository 45. The third process is repeatedly executing/interpreting the match estimator instructions to re-evaluate the user profile data as soon as new user profile data becomes available. The forth process is continuously monitoring the data object repository 44 for computed/updated affinity values and computed/updated certitude values, and repeatedly re-selects user data for rendering by re-evaluating the computed/updated affinity and certitude values.

[0079] As already mentioned, the network server 2 is configured to compose and transmit the data objects. The network server 2 is further configured to stream a plurality of data objects to the communication terminals 4, 4', and to transmit the evaluation profiles to the communication terminals 4, 4' upon request. The network server 2 further provides interfaces and services for system administrators. For this purpose, the network server 2 is configured to receive and modify data objects or elements of data objects. Specifically, the network server 2 is configured to receive evaluation profiles for defining the structure and content of the user profile data at the communication terminals 4, 4'.

[0080] For example, web services provided by the network server 2 are implemented based on the Representational State Transfer (REST) software architecture. In an alternative embodiment, the web services are implemented based on the Simple Object Access Protocol (SOAP) protocol.

[0081] It should be noted that, in the description, the computer program code has been associated with specific function modules and the sequence of the steps has been presented in a specific order, one skilled in the art will understand, however, that the computer program code may be structured differently and that the order of at least some of the steps could be altered, without deviating from the scope of the invention.

Claims

1. A communication terminal (4, 4') comprising user profile data and being configured to receive via a telecommunication network (3) from a network server (2) a data object comprising user data, wherein the communication terminal (4, 4') further comprises:

   an interpreter module (46) configured to extract match estimator instructions included in the data object, and to compute according to the match estimator instructions an affinity value based on the user profile data; and
   a selector module (42) configured to select, depending on the affinity value computed by the interpreter module (46), the user data to be rendered by the communication terminal (4, 4').

2. The communication terminal (4, 4') of claim 1, wherein the interpreter module (46) is further configured to execute the match estimator instructions for computing the affinity value by combining and weighting values of the user profile data.

3. The communication terminal (4, 4') of claim 1 or 2, wherein the interpreter module (46) is further configured to determine from the data object user profile data required for computing the affinity value.

4. The communication terminal (4, 4') of one of claims 1 to 3, further comprising a user profiler module (43) configured to request the user of the communication terminal (4, 4') via a user interface to enter the user profile data required by the match estimator instructions for computing the affinity value.

5. The communication terminal (4, 4') of one of claims 1 to 4, further comprising a data object repository (44) for storing data objects received from the network server (2); wherein the interpreter module (46) is further configured to store the affinity value in the data object repository (44) assigned to the respective data object; and the selector module (42) is further configured to continuously monitor the data object repository (44), and to select, depending on the affinity values assigned to the data objects, the user data to be rendered by the communication terminal (4, 4').

6. The communication terminal (4, 4') of one of claims 1 or 5, wherein the interpreter module (46) is further configured to execute the match estimator instructions for computing a certitude value which indicates reliability of the computed affinity value, and the selector module (42) is further configured to select, depending on the affinity value and the certitude value, the user data to be rendered by the communication terminal (4, 4').

7. A network server (2) comprising:

a data object generation module (21) configured to generate data objects comprising user data and match estimator instructions, wherein the match estimator instructions are configured to instruct an interpreter module (46) of a communication terminal (4, 4') to compute affinity values based on user profile data locally stored at the communication terminal (4, 4'), and
a transmitter module (22) configured to transmit the data objects via a telecommunication network (3) to the communication terminals (4, 4') for enabling the communication terminals (4, 4') to select, depending on the computed affinity value, user data to be rendered.

8. A computer program product comprising computer program code configured to direct one or more processors of a communication terminal (4, 4'), such that the communication terminal (4, 4')
receives via a telecommunication network (3) from a network server (2) a data object comprising user data and match estimator instructions;
extracts the user data and the match estimator instructions from the data object; computes an affinity value according to the match estimator instructions based on user profile data stored at the communication terminal (4, 4');
selects, depending on the computed affinity value, the user data to be rendered; and renders the selected user data.

9. A method of distributing user data from a network server (2) to a plurality of communication terminals (4, 4') for rendering the user data at the communication terminals (4, 4'), the method comprising in each case at the communication terminals (4, 4'):

receiving (S21) at the communication terminal (4, 4') via a telecommunication network (3) a data object comprising the user data and match estimator instructions from the network server (2);
extracting (S23) the user data and the match estimator instructions from the data object at the communication terminals (4, 4');
computing (S41) an affinity value according to the match estimator instructions based on user profile data stored at the communication terminal (4, 4'); and
selecting (S5) by the communication terminal (4, 4'), depending on the computed af finity value, the user data to be rendered.

10. The method of claim 9, further comprising the communication terminal (4, 4') executing the match estimator instructions for computing (S41) the affinity value by combining and weighting values of the user profile data.

11. The method of claim 9 or 10, further comprising the communication terminal (4, 4') determining (S31) from the data object user profile data required for computing the affinity value.

12. The method of one of claims 9 to 11, further comprising the communication terminal (4, 4') requesting (S35) the user of the communication terminal (4, 4') via a user interface to enter the user profile data required by the match estimator instructions for computing the affinity value.

13. The method of one of claims 9 to 12, further comprising storing (S24) data objects received from the network server (2) in a data object repository (44) at the communication terminal (4, 4'), storing (S43) the affinity value assigned to the respective data object in the data object repository (44), continuously monitoring (S4) the data object repository (44), and selecting (S5), depending on the affinity values assigned to the data objects, the user data to be rendered by the communication terminal (4, 4').

14. The method of one of claims 9 to 13, further comprising the communication terminal (4, 4') executing (S41) the match estimator instructions for computing a certitude value which indicates reliability of the computed affinity value, and selecting, depending on the affinity value and the certitude value, the user data to be rendered by the communication terminal (4, 4').

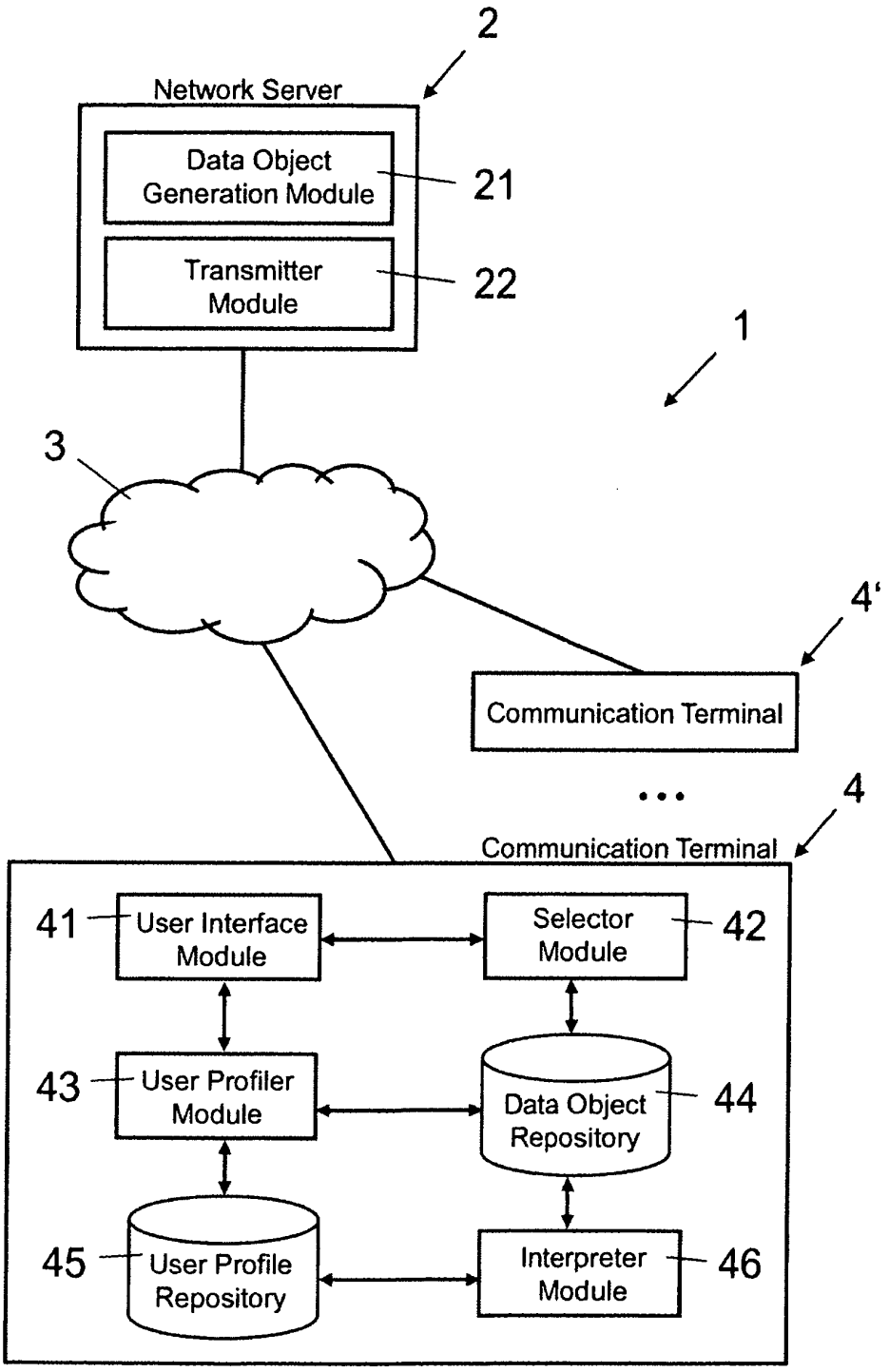

2
Network Server
Data Object Generation Module
21
Transmitter Module
22
1
3
4'
Communication Terminal
...
4
Communication Terminal
41
User Interface Module
Selector Module
42
43
User Profiler Module
Data Object Repository
44
45
User Profile Repository
Interpreter Module
46

Fig. 1

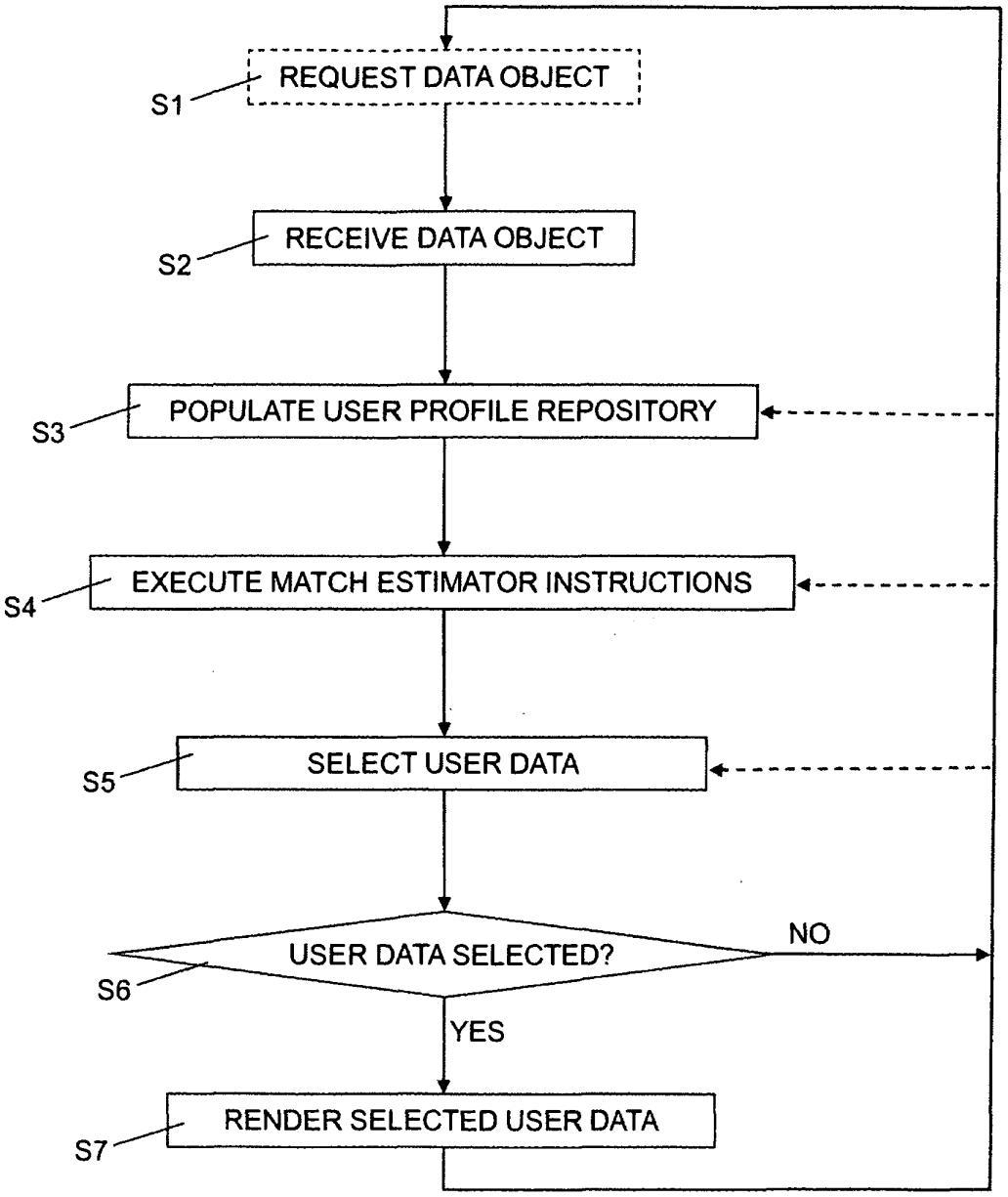

S1
REQUEST DATA OBJECT
S2
RECEIVE DATA OBJECT
S3
POPULATE USER PROFILE REPOSITORY
S4
EXECUTE MATCH ESTIMATOR INSTRUCTIONS
S5
SELECT USER DATA
S6
USER DATA SELECTED?
NO
YES
S7
RENDER SELECTED USER DATA

Fig. 2

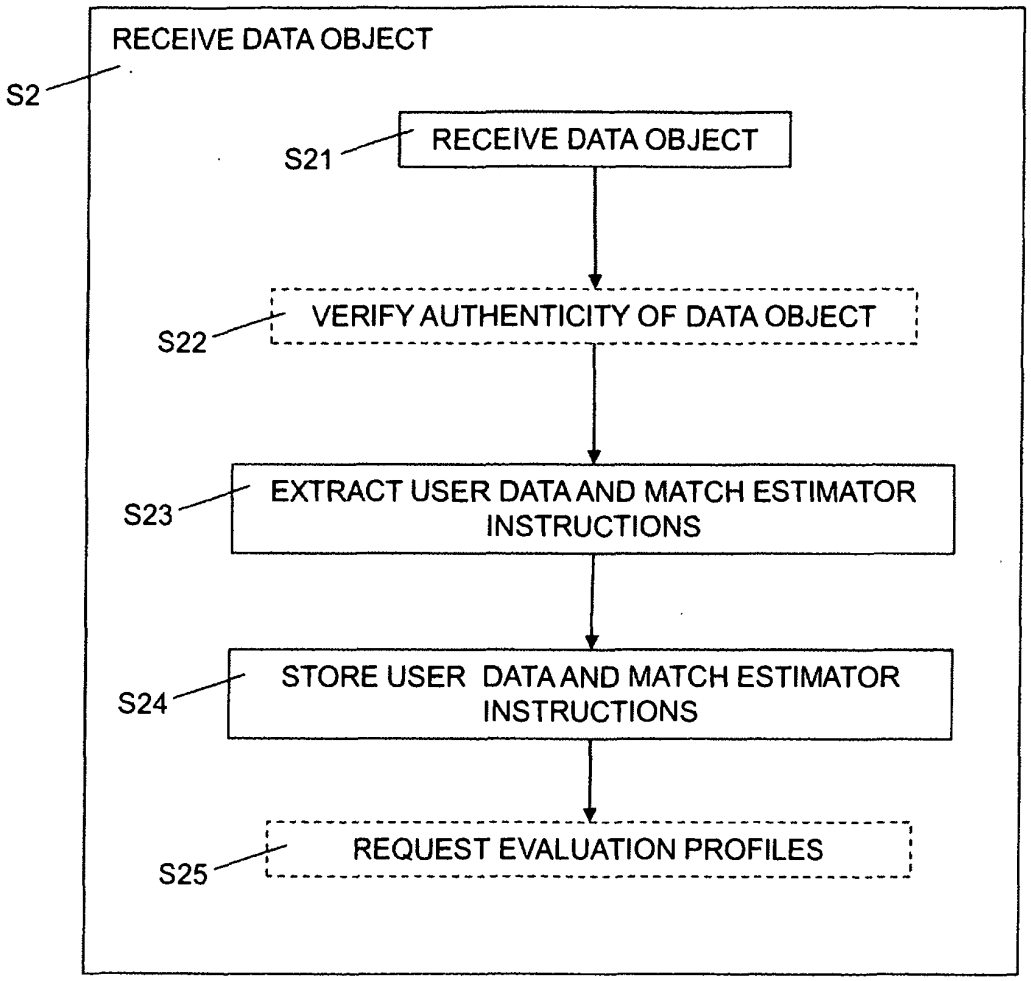

RECEIVE DATA OBJECT
S2
S21
RECEIVE DATA OBJECT
S22
VERIFY AUTHENTICITY OF DATA OBJECT
S23
EXTRACT USER DATA AND MATCH ESTIMATOR INSTRUCTIONS
S24
STORE USER DATA AND MATCH ESTIMATOR INSTRUCTIONS
S25
REQUEST EVALUATION PROFILES

Fig. 3

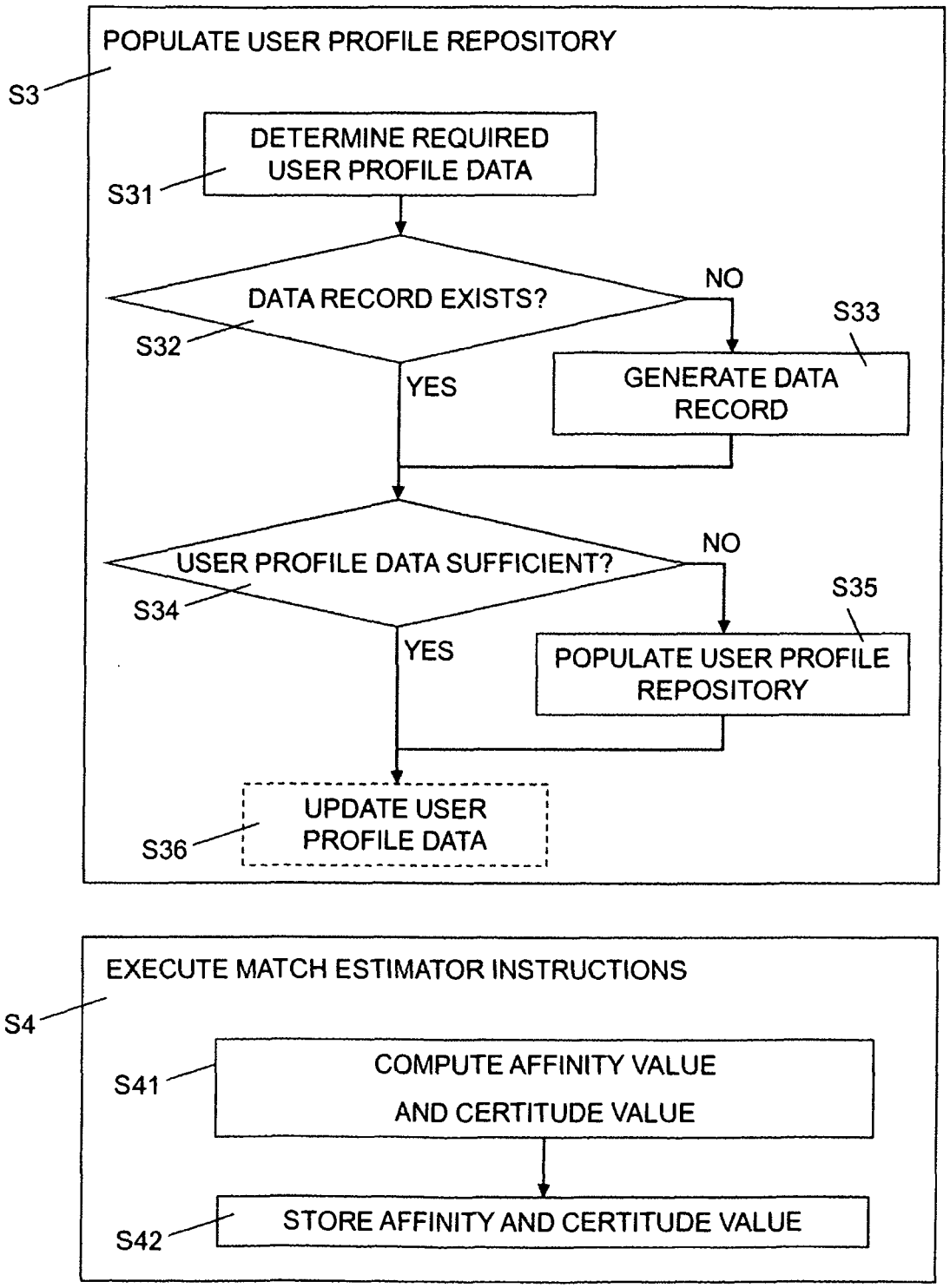

POPULATE USER PROFILE REPOSITORY
S3
DETERMINE REQUIRED USER PROFILE DATA
S31
DATA RECORD EXISTS?
S32
NO
S33
GENERATE DATA RECORD
YES
USER PROFILE DATA SUFFICIENT?
S34
NO
S35
POPULATE USER PROFILE REPOSITORY
YES
UPDATE USER PROFILE DATA
S36
EXECUTE MATCH ESTIMATOR INSTRUCTIONS
S4
COMPUTE AFFINITY VALUE AND CERTITUDE VALUE
S41
STORE AFFINITY AND CERTITUDE VALUE
S42

Fig. 4

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 10 00 8973

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X,D	US 2005/038698 A1 (LUKOSE RAJAN M [US] ET AL) 17 February 2005 (2005-02-17) * abstract * * paragraph [0014] - paragraph [0021] * * paragraph [0025] - paragraph [0027] * * paragraph [0030] - paragraph [0031] * * paragraph [0035] - paragraph [0036] * * paragraph [0042] - paragraph [0043] * * figures 1-4 * -----	1-14	INV. G06Q30/00

TECHNICAL FIELDS SEARCHED (IPC)

G06Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	9 December 2010	Cîrstet, Andrei

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
.....
& : member of the same patent family, corresponding document

1

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 10 00 8973

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

09-12-2010

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005038698 A1	17-02-2005	US 2005038699 A1	17-02-2005
		US 2005038774 A1	17-02-2005

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 20050038698 A1 **[0005]**
- US 20080004954 A1 **[0006]**
- US 20060265283 A1 **[0007]**