Mobile Identity Management: An Enacted View

George Roussos, Don Peterson, and Uma Patel

Abstract. Growth of mobile business requires the ability to provide context aware services when and where needed, the development of trust relationships between trading partners and the ever-expanding capability for reconfiguration of value chains. These issues become even more prominent by the emergence of converged architectures for next generation public networks, a result of integration of the Internet, traditional telephony networks and consumer electronics, which brings mobile business to the forefront. In this context, mobile identity management can play a central role to address usability and trust issues in mobile business. For this reason, it is being established as a core service for next generation mobile telecommunications infrastructures. Mobile identity management is used to identify, acquire, access and pay for services that follow the user from device to device, location to location and context to context and thus, becomes the network component that holds together novel services on novel networks using innovative business models. In contrast to previous generation mobile business infrastructures, this represents a pivotal shift in focus from identification to identity. In this paper we advocate that this shift calls for the enacted view of technology since the level of involvement of human qualities is unprecedented when discussing identity. We introduce a view of identity in mobile business based on three principles and we find that this approach is useful in explaining some recent research findings in ubiquitous retailing. We expect that widening the discipline boundaries for future research on identity in mobile business will be essential for the development of effective mobile service provision systems.

Keywords: mobile identity management, pervasive computing, ubiquitous computing, next generation mobile communication systems, service provision.

1. Introduction

Mobile business is perceived as the main driving force for the next phase of electronic commerce growth primarily due to the rapid adoption of second-generation mobile telecommunication systems that have created a market opportunity of several hundred million consumers worldwide. The growth of mobile commerce is expected to accelerate with the emergence of converged Internet-telephony networks and hybrid computing-communications devices, either with the introduction of third generation mobile networks or through the operation of hybrid fourth generation networks. Crucial success factors for the provision of mobile services are the issues of usability and trust: the small form factor of mobile devices implies that both application navigation and content delivery should be adapted on the fly to reflect the particular needs of the particular user; and acceptable mobile information service provision systems need to operate within a trustworthy environment for the user. In this context, trust is primarily dependant on the perception that identification credentials, financial transactions and personal profile are kept secure and private. Furthermore, the emergence of a converged architecture for next generation public networks, resulting from the integration of Internet, traditional telecommunications networks and consumer electronics, brings issues related to mobility to the forefront.

Mobile identity management is viewed as an approach that can address both usability and trust concerns in mobile business and for this reason it is being established as a core service for next generation mobile telecommunications infrastructure. It is used to identify, acquire, access and pay for services that follow the user from device to device, location to location and context to context and thus, becomes the network component that holds together novel services on novel networks using innovative business models. In contrast to previous generation mobile business infrastructures, there is a pivotal shift of focus from identification to identity. Indeed, this change in focus plays a central role in the arguments developed in this paper: while identification is a static concept, the concept of identity is altogether more dynamic because it is situated, negotiated and underpinned by trust.

Issues of identity, being fundamentally personal and cultural become integral to everyday life and thus require appropriate treatment. To this end, we propose that a suitable perspective on mobile identity management is provided by the so-called enacted view, that is a stance that considers mobile business as an evolving party to human activities. Indeed, the enacted view approaches mobile business as an open-ended socio-technical production: a mass of particular actions taken as individuals and groups make their own uses of technologies. The result may be dynamic, unpredictable and strongly mediated by the idiosyncrasies, needs, and preferences of individuals and groups. Following the enacted view we attempt to establish a three-principle approach for the study of mobile identity management. We find that the three principles are a useful conceptual framework to explain findings from our research on ubiquitous retailing.

The paper is structured as follows: In section two we discuss the elements and the properties of mobile identity management systems. In section three we investigate the role of mobile identity management systems as well as that of the identity service provider for current mobile business markets. At the end of this section we also present briefly a selection of the first generation mobile identity management systems available today. In section four, we introduce the architecture of next generation mobile communications systems and the novel types of federated business services that can be developed on them. In particular, we focus on the development of the so-called ubiquitous retail and report on recent results that provide some evidence for the relevance of mobile identity management in this context. Finally, we introduce a conceptual framework based on three principles following the enacted view. We expect this framework to be useful for the study of mobile identity management systems and indeed we find that it can provide a consistent and concrete foundation to explain our findings from ubiquitous retail.

2. An Overview of Mobile Identity Management

Identity is an essential characteristic of the experience of being human. It encompasses elements that make each human being unique but also all the characteristics that signify membership to a particular group or culture and establish status within that group. However, Internet mediated communication filters out a significant proportion of cues that can reveal identity in the physical world thus obscuring recognition of individuals or of characteristics pertinent to particular groups [42, 56]. Today, the effect of poor identity visibility in Internet mediated communications is becoming critical primarily due to the proliferation of electronic commerce over the Internet and via mobile telecommunications networks. The split between our perception of human identity and its electronic representation will only increase with the introduction of ubiquitous technologies and systems.

Digital identification systems have been used for decades [8] to record and preserve the electronic representation of personal information of an individual including name, address, phone numbers and demographics. The emergence of the Internet as a common communications infrastructure requires that digital identification becomes digital identity, the basis of the digital-self. Identity systems materialise as the keeper of not only personal electronic information (credit card numbers, biometrics, personal health records, personal preferences) but also the channel through which individuals communicate, interact, transact, share reputations and create trust relationships with people, businesses, and devices. The operations performed to support the lifecycle of the digital identity are referred to as identity management. The distinction between identification and identity is pivotal to this paper. Identification is a restricted concept that refers to some combination of facets by which an entity is recognised. Digital identification is a set of data that represent the personal information of an individual or an organisation. Misconceptions are caused by the fact that frequently digital identification is erroneously referred to as digital identity. Whereas identification is a static concept, the concept of identity or of the digital self is altogether more dynamic because it is arguably situated, negotiated and underpinned by trust. It is a core premise of this paper that whereas the current dominant design paradigm is concerned with solutions to management of digital identification, consumers perceive and behave as if digital identification is a synonym of digital identity. This line of reasoning is supported by findings from studies on consumer confidence in electronic commerce (cf. references later in this section), research findings on consumer perceptions of ubiquitous commerce (cf. section four) and arguments which explain consumer mistrust in terms of the three principles we discuss in section five.

Mobile (digital) identity is an extension of the concept of digital identity that illuminates the importance of mobility. Indeed, identity is mobile in many respects. The first mode of mobility is from device to device. This means mobile identity can be used to certify the authority of a particular individual to gain access to information and resources while using different mobile devices. A good example is when an employee gains access to her corporate email account from a workstation, a mobile telephone and a personal digital assistant. The second mode of mobility is from (physical) location-to-location that is, where an individual moves between different locations but still requires access to systems and information according to her role and credentials. For example, the case where a salesperson moving from city to city to visit clients requires access to personal sales performance data from the corporate portal. An issue closely related to location mobility is that of coordination of authority domains, since a person moving from location-to-location is also usually moving between areas controlled by different organisations. When employees access information systems from their desk both the access medium and the information storage are physically located within a single authority domain regulated by their employer whereas, when they access information via one of their trading partner’s extranet, they cross organisational boundaries and the trust relationship between the two organisations must be negotiated as well.

The third mode of mobility is from context-to-context that is where a person receives services based on different societal roles: as a professional, as a sports fan, as a parent and so on. For example, by adapting to context –which includes time, date, location and so forth— individuals might have widely different entertainment needs depending on whether they act, for example, in their professional capacity or as a parent. Of course, the three modes of mobility are not isolated but more often than not, different modes are concurrently modified and thus create much more complex situations than what implied from a single mode in isolation. Finally, the elements (described in detail below) that make up the mobile identity may not be stored at the same location but they may be distributed between different locations, authority domains and devices. For example, personal information may be held at a home service gateway server (most probably a set-top box), payment information may be held at an associated bank, music preferences may be held at an entertainment service provider and gaming results may be held at an on-line game service provider.

Mobile identity has three components: identification, payment and personalisation. Identification is the association of a set of tangible and structured credentials with a particular person that is valid within a particular formal system and can be used to explicitly distinguish the particular individual from any other in the same system. Examples of identification methods are national identity cards in Germany, social security numbers in the United States and credit cards or driver's licenses in the United Kingdom. In contrast to identity, identification is a concrete concept which is well understood and with a long social history and specific significance within a particular system (for a historical review of identification see [8]). Identification is also a well-understood concept from the point of view of information systems --as a matter of fact identification methods and management have been a consistent strand in information systems research [57]. Issues affecting identification in information systems are authentication, authorisation and access control mechanisms, directories, electronic payment, trust management and public key infrastructures, all mechanisms representing incremental developments in managing identification information and controlling access to resources as well as managing relationships between persons and groups across administrative domains.

Although identification methods are well developed and established they are not without problems. A recent report by the US Federal Trade Commission [51] states that identity theft is the fastest growing crime in America with over 900,000 victims each year. Identity theft is the replication of identification credentials and the use of them to either obtain access to individual resources (for example computer files, bank accounts, credit rating) or to establish new accounts or credit using the victim's credential and without their consent. Although the emotional cost at the individual level is significant, arguably the financial cost is also important [28]. In the UK alone, fraud related to identity theft has been estimated to 293 million pounds sterling in the year 2000 and is expected to rise to 800 million by 2005 [26].

Indeed, identification is closely related to payment in the sense that financial transactions are between two named and identifiable parties and hence they are based on the exchange of personal data. What sets payment information apart from other types of identification information is the fact that the two parties involved in a financial transaction are almost always bound in a contractual agreement and thus, the appropriate commerce law also regulates use of identification data. In mobile business, provision of payment services as part of mobile identity management can form the basis for the development of a trust relationship with the consumer. This relationship can play a significant role in the development of mobile commerce since the primary benefits offered by mobile transactions, that is convenience, lower prices, and lower search costs, are offset by costs associated with risk taking and loss of privacy; in particular, the economic risk arising from potential monetary loss could be significant [44]. In fact, widespread consumer concerns about risk have been repeatedly identified as one of the main reasons for the slower than expected growth of electronic and mobile commerce [4, 17, 20, 50]. It is characteristic that recent studies have estimated that more than 94 per cent of consumers have refused to provide data to a web site and more than 40 per cent have provided fake data [33].

In the context of mobile business, personalised service provision is even more important due to the inherent limitations of mobile access devices, which make personalisation a fundamental component of mobile user interfaces. Indeed, context aware service delivery [25] has been recognised as a fundamental requirement for mobile users due to the continuous change of the point where their mobile device attaches to the network; the small screen size of the mobile unit and its limited resources (including computational power and battery); and the limited bandwidth offered by wireless communications. Context awareness is required for both the application functionality and the content delivered. A significant element of context is identity and thus personal profile [25]. Furthermore, versioning of information goods to maximise revenue via differential pricing is a well-established practice [52] and taken to the limit the concept implies personalised content delivery, that is, an adapted version of the good that facilitates the individual needs, preferences and habits of the particular consumer. Several existing applications exhibit adaptable behaviour based on identity information of their user, for example RoboForm and the collection of applications under the Freedom network. Experimental systems like the Vallet [10] go a long way towards developing an intelligent context aware agent that independently caters to the needs of its owner and there are significant resources invested to research efforts towards the development of the so-called "enduring personalized cognitive assistant". The development of these applications is also justified by the perception of mobile consumers that the overhead required for the management of multiple accounts with multiple trading partners is significant and the repetitive effort of form filling as part of security and privacy mechanisms has been proven to be the source of error as well as regular security compromises.

Hence, part of mobile identity is also the personal profile. What data exactly constitutes a personal profile differs significantly depending on the particular profiling method and technology used. Explicit personalisation occurs when the individual specifically chooses from a number of options on a list, such as selecting colour schemes, welcome messages or areas of interest for news messages (for example favourite sport or team). Implicit personalisation results from the construction (and continuous update) of a personal profile based on historical usage data. Implicit personalisation methods have three advantages over explicit methods: they do not require a pre-configuration step, they evolve over time and they capture unconscious as well as conscious actions and responses. On the downside, they are significantly more complex and thus computationally expensive but also require a longer period of training before they can produce reliable results. Examples of implicit systems include rule-based systems as well as content based and collaborative filtering systems. No matter which method is used, all personalisation methods require that the users accept to give up some of their personal data to the service provider. This fact raises privacy issues and increasingly consumers are concerned not only about the use of their personal data but also about their ability to be involved in the uses of the information they supply either through explicit permission or economic incentives [7].

Finally, it is worth noting that mobile identity has different interaction modes. The first and simplest is peer-to-peer where identification and credential exchange is performed without the mediation of a certification authority, in a distributed decentralised manner. Trust is developed at a local, ad-hoc interaction level. The second type of interaction is the nomadic mode –existing within a single administrative domain-- where there is a single authority that certifies identity credentials. For the support of nomadic interactions some infrastructure is required: identification and credential exchange protocols, mechanisms for group member identification, membership control and access to common resources. The third mode of interaction is inter-domain nomadic interactions that is, interactions between entities across authority domains or even at a global scale. For this operational mode employed protocols and mechanisms should conform to well-known open standards and management of relationships between authority domains must be catered for.

3. Identity and Mobile Business

In this section we identify the interactions between different types of mobile business [27, 40] and mobile identity management, including business-to-consumer, consumer-to-consumer and enterprise-to-employee. Then we proceed to discuss the role of the mobile identity service provider for mobile business. Finally, we briefly discuss technology alternatives in first generation identity management systems.

Business-to-Consumer. Mobile business is perceived as the main driving force for the next phase of electronic commerce growth [53, 54] primarily due to the rapid adoption of second generation mobile telecommunication systems. Indeed, this development has created a market of several million consumers worldwide. The growth of mobile commerce is expected to continue with the emergence of converged Internet and telephony networks either with the introduction of third generation mobile networks or as hybrid fourth generation networks (cf. section four for more details on fourth generation systems). Indeed, demand for data driven applications and mobility are the main growth and convergence factors. As a measure of the expected impact of the shift towards a mobile Internet eMarketer a market research firm, estimates that 57 per cent of Internet users will be mobile by 2007. On the other hand, it is less clear what proportion of mobile users will actually be mobile consumers. Indeed, while initial estimates (Gartner 1999) talked about 200 billion US dollars of mobile business revenue by 2004 current revised estimates predict revenues between 1 and 20 billion US dollars by the same date. According to Forrester Research a market research firm, although mobile users allude to different aspects to justify their reluctance to adopt mobile commerce their main concerns are security (for 52 per cent of the study participants) and unsatisfactory user experience (for 35 per cent of the study participants). Also, the Gartner Group a market research firm, state that for mobile telephone users usability and trust are the critical factors for the widespread adoption of mobile business. According to the same study, if mobile business does not take off it will be primarily due to the high risk level perceived by mobile consumers as well as to non-standardisation of mobile business systems which will restrict interoperability and thus mobility.

Mobile identity management addresses both of the two main challenges identified above that is, usability via context awareness and trust based on the perception of secure operation and protection of privacy. Indeed, mobility creates new opportunities but at the same time is also a limiting factor: to best serve their purpose, mobile devices have to be small with a correspondingly small display. A consequence of the small form factor is lower computational capability. For this reason it becomes essential that services offered on mobile devices require little or no navigational effort which further implies that the service itself should be adaptive to the needs of the particular person using the service as well as responsive to the situation that person is in. In fact, in order to be successful, mobile Internet services will have to be highly personalised and context aware or else they will have to be adaptable to identity information. Although identity information has an important role to play in supporting adaptable and personalised service provision, deployments of mobile identity management systems today are primarily a component of branded application service provision solutions. This approach appears to have certain advantages as the main interaction mode in mobile commerce since it facilitates the transparent operation of virtualised value chains [16, 23, 29]. To the user at the receiving end of a mobile service the moving boundary between business partners is imperceptible and irrelevant at large. Indeed, the consumer develops and maintains a trust relationship with a single trading partner rather than having to renegotiate the relationships whenever the virtualised value chain is reconfigured. Thus, any risk for consumers as well as any trust management issue is mitigated to the provider of the service. Despite advances in security standards and technologies there is still significant divergence between consumers perception of security and that actually available in deployed digital payment systems [36]. By having a single point of interaction consumers are also confident that they can maintain some level of control over their personal details and payment transactions irrespective of the service provider of the service [7].

Consumer-to-Consumer. Another area of mobile business that is affected by identity management issues is that of consumer-to-consumer (C2C) commerce which is one of the first e-commerce activities that was extended to mobile. Indeed, there are certain advantages in timely notification of specific events in C2C marketplaces, particularly with regard to the availability of new items and the monitoring of specific auctions in which the consumer is interested. A recent study in C2C commerce [43] identified price and trustworthiness as the two main factors affecting online seller choice. Trust between seller and buyer in this situation is seen to depend on the reputation of the seller (constructed via recorded commentary by other consumers and the available rating of satisfaction levels of previous transactions) as well as the quality and number of previous interactions between the particular C2C pair. In this context strong identity credentials can be seen to directly translate to a price premium.

Enterprise-to-Employee. Mobile identity management also plays a significant role within the boundary of a single organisation. Indeed, organisations require their employees to be increasingly mobile either by working in remote locations or teleworking or as an extension of a mobile sales force. From the point of view of a corporate entity, the impact of mobile identity can be evaluated along three major areas: increasing operational efficiencies without compromising security; increasing the degree of personalization of services as well as active consumer management; and, finally, increasing the speed of deployment of novel services and subsequently, increasing revenue streams. Furthermore, mobile identity services reduce access management infrastructure costs, improve process efficiencies, free critical human resources and eliminate duplication of tasks. Also, mobile identity management facilitates tighter relationships between trading peers including and employees, through accurate prediction and delivery of appropriate content at the time of engagement. Finally, mobile identity management allows for the rapid re-deployment of human resources to support novel services to meet shifting market needs. Mobile identity management supplies the infrastructure required to contain and control costs while expanding channels of business, regardless of the location of end user.

Identity Service Provision. This discussion leads naturally to the observation that a new entity, the mobile identity service provider (MIDSP), acquires a central role in the mobile commerce value chain. First generation manifestations of the MIDSP are observed today and it is expected that its role will become central with the development of next generation networks (cf. section four). Although the role of the MIDSP as a mediator of consumer transactions and the guard of personal information is significant, one of its more important assets is the ability to direct the attention span of the consumer towards particular choices which implies that it can exploit its advantage to developing market segments through access control to end users [37]. From the point of view of the supplier, the mediation of the consumer relationship by the MIDSP may also have essential utility for its participation in dynamically created and adaptable value networks in real time. It appears that, mobile identity management infrastructures seem to offer an opportunity for unprecedented flexibility in real-time reconfiguration of value streams.

The MIDSP may also assist mobile business in mitigating liability arising from regulations that protect consumer privacy and govern the sharing of personal information without consumer consent. The proliferation of Internet and mobile business has multiplied the number of access points to confidential information. Without an appropriate security policy and superior security controls, the possibilities for data compromise are greatly increased, hence the need for more flexible standardized and context-based forms of managing identity that are device and application agnostic. Through specialisation, MIDSPs can support a wider range of information technologies and devices with mission-critical levels of scalability and reliability.

The strength of the MIDSP concept is that it exploits the property that mobile identity management is most valuable when individual identity providers federate their resources to provide identity services with wider scope. Such services can quickly mature from the initial risk management and analysis stage to advanced collaborative service provision. In the simplest case, mobile identity management infrastructure provides the foundation for the engineering of business processes. Provisions for the evaluation and subsequent mitigation of business risks associated with the introduction of this approach will also accompany this stage. On the other hand, if organisations initiate the delivery of services based on their own infrastructure they are restricted by the non-availability of identity credentials from other organisations. Although the organisation has the capability to support development of new services and enhance existing ones with the incorporation of functionality of secure role-based access control and trust management, the usefulness of this approach is restricted by the closed nature of the system. MIDSP mediation allows for the extension of internal infrastructures via federated identity services. This alternative allows the organisation to expand its operational limits and its collaborations with its business peers, as well as the market segment that can be approached via trusted (potentially global) mobile identity infrastructure while at the same time achieving advanced interoperability.

Before concluding this section it is appropriate that we discuss the technologies used for the implementation of first generation identity services. Although the technologies discussed here have their roots in traditional identification system they are deemed here to be identity rather than identification based either because they already incorporate truly identity technologies or because they are committed to a roadmap that realises this transition. Identity technologies can be classified in two main categories: Network or device based though some more recent approaches combine both. This distinction highlights the primary location where identity data are stored. Network based mobile identity management systems are by far the most prevalent form of system and have been developed primarily as a response to the lack of trust by consumers in electronic commerce. Examples of network based mobile identity management systems are the SourceID open source specification and systems, AOL Screenname, Liberty Alliance, Microsoft Passport, Genio and Oblix. From a technological point of view, they inherit their legacy from single sign-on, public key infrastructure and Internet directory systems and they are characterised by the use of public networks and the safeguarding of identity credentials at web-enabled servers. The current trend is for such systems to incorporate trust management and access control mechanisms for Web Services primarily as part of industry voluntary standards (for example the Liberty Alliance consortium works closely with the Organisation for the advancement of Structured Information Standards OASIS).

However, no single approach has achieved market domination[1] and none is expected to achieve this in the foreseeable future.

Device based mobile identity systems offer a decentralised alternative to the management of credentials, since more often than not the data is stored locally on a mobile device carried by the user. In fact, the users themselves have the responsibility to authorise access to their own data as well as maintain, protect and update them. Although this would seem to imply a significant overhead for all parties involved the advantage for users is that his data are stored under their control. The issue of trust is a recurring theme in this paper and, if not resolved, can potentially represent a significant barrier for their wider adoption by consumers. Devices that have been used for this purpose include mobile telephones (for example via the inclusion of ECML e-wallet capabilities by several handset manufacturers) and smart cards (primarily in the healthcare sector but also Visa's 3D Secure system). Finally, an emerging form of mobile identification is the development of devices embedded in the human body (for example radio frequency identification RFID transponders) that store the identity information and interact wirelessly with the information infrastructure.

4. Identity in Next Generation Mobile Systems

The Internet, telephony and the consumer electronics market are rapidly converging towards a novel global information architecture, driven by increasing demand for data centred applications and mobility [30]. Depending on the point of view taken, the

[1] Microsoft's Passport available primarily via the Hotmail messaging service has approximately 200 million subscribers at the time of writing and AOL's Magic Carpet which uses Liberty Alliance compatible systems from Sun Microsystems has approximately 150

emerging architecture is referred to either as ubiquitous or pervasive computing or as fourth generation (4G) mobile telecommunication networks or in some cases simply as next generation Internet (NGI) [19]. Whatever name is selected, it refers to a pervasive fabric of intelligent instruments, appliances, information sources and information analysis tools all tied together by high-speed wired and wireless networks which may include personal software service agents that remove the burden of constantly searching for, gathering, and analysing information in a data rich environment. However, the roadmap to convergence is not perfectly clear. Indeed, there are considerable technical as well as cultural differences between Internet, telephony and consumer electronic engineering as well as business practice. On the one hand, the Internet has been built on top of physically and administratively distributed, open systems while telephony and consumer electronics are leveraging the advantages of centralised and proprietary systems and protocols, systems that are closed to third parties. These differences create friction between the three approaches but at the same time open up significant opportunities.

In the emerging fourth generation systems the network core is based on Internet technologies extended via application layer routing, that is routers more aware of the data content being transported [2]. Building on the application layer routing capability, at the edges of the core network the main architectural element will be the overlay network. Overlays have the advantage of producing on the fly systems of systems thus connecting application services to processing capability embedded in the network fabric [21]. At the user end, service delivery will be available over radically different access networks (including PSTN, wired and wireless LAN, personal area networks including Bluetooth,

million subscribers.

second and third generation cellular, DSL, cable, satellite) as well as a variety of post-PC user devices (including converged mobile telephone-portable computer and information appliances). Another source of heterogeneity will be due to all sorts of new sensors that will be attached to the network providing access to physical space data [34]. Indeed heterogeneity is one of the main characteristics of fourth generation networks and extends from the physical up to the service layer. Heterogeneity is abstracted in the software infrastructure thus making possible for services to be deployed and redeployed rapidly and even on demand. In fact, one of the most apparent implications of the new systems is their capability to support new types of service architectures [31].

Next generation mobile devices are fundamentally different from today's mobile telephones being primarily a core connectivity device which, to a great extend, derives its functionality from embedded networked components that it can discover: first in its immediate locality, then within its accessible environment and finally over wide area networks [58]. Discovery and adaptation to the available computational resources and services requires mechanisms that are now being developed and are extending service provision architectures from the Internet era (for example IETF Service Location Protocol [55] and Salutation [32]). Fourth generation service discovery and configuration frameworks are designed to support vertical and horizontal service aggregation, interoperability bridges for access to networked data sources (for example, personalised recommendations on the Grid via OGSA web services [48]), vocabularies for machine-to-machine interactions as well as adaptability, that is the ability to acquire the required functionality to perform specific tasks [45]. Built on top of the primary service discovery mechanisms, a basic set of fundamental services is needed. Mobile identity together with domain specific ontologies, semantic querying, environmental monitoring, reactive event notification and distributed modelling services have been repeatedly identified as good candidates for the core set of services [34, 38, 58]. Adaptability to discovered resources and services would be accompanied by adaptability of the run-time behaviour of applications as well as to active context delivered following the informational context of the user situation. In addition to time and locality [25], context-awareness requires tracking of different roles in different contexts to provide personalised and up-to-date content.

The emerging architecture of fourth generation networks is already visible in several cases [1, 6, 9, 10, 12, 21, 38, 39] but one of the most interesting questions is how should this new infrastructure be used for conducting business. Some generic considerations of the implications of such technologies for commerce are discussed in [10] but here we will focus on the particular case of ubiquitous retail. Ubiquitous computing technologies were first introduced in retail by IBM [6, 18, 24] and the concept was further developed by project Albatros [47] though little attention had been paid to business issues, with the focus solely on technology. Here we will discuss lessons learnt during our involvement in the development and deployment of an experimental ubiquitous retail system which was founded on a business rationale and evaluated at field trials in a realistic application environment. A full technical description of the system is outside of the scope of this paper and the interested reader should consult [39] for details. In brief this system is perceived to extend or complement the reach of the retail supply chain in two ways: first to include the consumer home through ambient intelligence devices and to provide a richer shopping experience within the supermarket space [1, 9, 12, 37]. The business rationale for the deployment of this system was founded on the capture of rich, real time information regarding consumption and this information being fed back to the supply chain in a collaborative manner between trading partners. This design offers more accurate predictions of demand and the opportunity to optimise just-in-time manufacturing in particular for the fast moving consumer goods (FMCG) sector.

Deployment of the system in realistic conditions raised significant concerns by consumers. In particular, most concerns were related to acceptance of the system for personal use. In the following paragraphs, we will discuss some of the findings of a research study conducted during the requirements capture phase and we will point to the criticality of mobile identity management as a component of the system (a detailed description of this study has been published in [38]). The aim of the study was to assess the appeal of ubiquitous commerce as a value proposition to the consumer as well as to identify barriers to acceptance. The approach adopted was qualitative in nature and used focus groups. Market Analysis a market research firm, was commissioned to conduct the field research. The target audience consisted of: women between the age of 25-34, responsible for grocery shopping within their household who demonstrated some familiarity with information and communication technologies, either as regular users of PC and mobile telephony at home or at work; women with the same background but from the 35-50 age range; married couples with both partners between the ages of 25 and 34, both responsible for shopping and with similar background as groups one and two; and, couples as in the previous group but from the 35-50 age range. During the discussion the participants were first introduced to ubiquitous retail concepts through a presentation based on concept drawings with explanatory text, which the moderator used to discuss selected usage scenarios. Following the introduction, participants were encouraged to discuss their thoughts, feelings and reactions to this novel approach to retail as well as to express their response regarding attitudes and purchase behaviour in this environment. The discussions of all groups were recorded in audio and video with the permission of the participants. At the end of the discussions participants were given a voucher for one of the retailers participating in the project. In section five, the findings reported in the following paragraphs will be reframed and described in terms of the three principles that compose the enacted view on identity management.

The analysis of the findings highlighted one of the main concerns of the participants to be the use of personalized purchase statistics by the retailer and collaborating service providers. A large number of participants were particularly concerned about the collection and storage of personal data, even though they were aware of the provisions (albeit not the practicalities) of the data protection act. Their negative reaction to data collection was triggered primarily after the eponymous authentication during the initial use of the shopping cart when, after entering personal identification credentials, they were presented with a personalized shopping list derived through the analysis of their purchase history. The two main issues arising related to the immediate recognition of the fact that for the construction of the personalised shopping list their data is recorder, preserved and processed. This reaction was more pronounced when trust of third parties was also involved –a core property of fourth generation systems. The main source of concern was that private data, collected in the sheltered space of the home could be delivered to external sources without the explicit consent of the consumer. The vast majority of participants did not trust a service provider to protect their privacy, irrespective of whether it was a contractual obligation or not.

Another major concern related to the overall shopping experience, which was perceived to point towards a technology controlled, fully standardized life-style. Two issues interrelate on this point: On the one hand, participants rejected the claim that a software system could predict accurately their wishes just by collecting historical data and monitoring habitual purchases. Indeed, due to its ability to pre-empt their wishes, this aspect of the system appeared patronizing and overtly rationalized but most importantly contrary to the experience of being human. In fact, the majority of participants discarded the possibility of a computer system that could successfully predict their wishes, while some of them were offended by this suggestion. On the other hand, the participants of the study perceived that the ubiquitous retail system reviewed promoted primarily the interests of the supplier while the consumer only received marginal benefits.

Finally, several participants observed that adoption of ubiquitous retail would result in a fundamental transformation of the traditional family roles. They emphasised that product selection and maintenance of appropriate home inventory levels are a means to establish roles within the family unit and the responsibility to carry out these activities an integral part of the identity of the person or persons in charge. Elimination of this responsibility was perceived to undermine the status quo and ubiquitous retail was consequently treated with mistrust and hostility.

5. The Enacted View of Mobile Identity

There are different ways of conceptualising mobile business, and hence different ways of understanding what is needed for its success. One perspective is the 'objective' view in which technologies are seen as singular entities with specific powers and consequences. Thus, in the vein of technological determinism, these powers and consequences are regarded as predictable. And in the vein of strategic choice, success is seen as depending on decisions made by management in selecting and deploying technologies. As argued by [31] however, it is crucial also to recognize the 'enacted' view of technologies. According to this view, the digital economy is an open-ended socio-technical production: a mass of particular actions taken as individuals and groups make their own uses of technologies. The result may be dynamic, unpredictable and strongly mediated by the idiosyncrasies, needs, and preferences of individuals and groups. The enacted view argues that if we ignore individual human agency in the actual and day-to-day use of technologies then we achieve an artificial and unhelpful understanding of their success [31]. Hence, we need to attend to 'technologies-in-use' that is, the actual results of introducing technologies into particular situations, contexts, tasks and communities, rather than just to 'espoused technologies' that is general expectations about the functions of systems.

The use of mobile business technology, then, is situated, and a crucial dimension of this situatedness is identity. We exploit mobile communications, the Internet and consumer electronics technologies not in a vacuum but within human relationships, and these relationships are, in turn, mediated by issues of identity. Thus we find issues of trust, rights, duties, expectations, privacy and so on as central to the use of technology, not simply as subsidiary or occasional 'human factors'. Our concern is that identity is intrinsic to mobile business, and if not addressed appropriately may slow mobile business growth. We therefore need a general framework for understanding identity in the context of mobile business which brings existing resources and new developments together. In the humanities, the study of identity and related issues goes back at least to the thinkers of ancient Greece: Aristotle and the ancient Stoic thinkers, for example, discussed the competing demands of individuality and community, and the many forces which bear on a person's sense of self [15]. This has been a long debate with many differences in point of view. However, three points stand out as issues which cannot be ignored in adequate treatments of identity.

- The *locality principle* says that identities are situated in particular contexts, relationships, roles and communities, and that we may have different or overlapping identities attaching to different contexts.
- The *reciprocity principle* says that both sides in a relationship need to know what is going on so that they can check and correct each other’s perceptions.
- The *principle of understanding* says that identity serves in two-way relationships as a basis for mutual understanding.

The locality principle has been identified in various treatments of the self [14, 46], and has significant implications for mobile business. It implies, for example, that a global or universal identity makes little sense. We cannot expect consumers of mobile services to be comfortable with a single identity profile in relation to a universe of activities and services that entail all aspects of their life. Rather, we can expect a strong preference to maintain different identities attaching to different functions, roles and communities, and to have control over these. This would explain the overall negative reaction of the participants of the focus groups to ubiquitous retail since users of the system were characterised singularly as consumers. We believe that since the system extends to all types of activities including professional and family, refusing to acknowledge the different identities, the system did not address locality concerns. For this reason it was perceived as being designed to benefit the business only without taking into account the users needs. The locality principle also highlights the need to balance two forces in ubiquitous retail or any other mobile business: first, the need to respect the consumer's localized and multiple identities, and second, the significant advantages of open, collaborative and ubiquitous mobile business. Although it may be convenient to share consumer data with trading partners this action is liable to destroy trust. It is not that the details in question involve anything profoundly secret or private to the consumer, but rather that the localized identity developed via significant personal investment is forcefully removed by an external entity and used beyond the locality that has been developed.

The reciprocity principle concerns the negotiation and knowledge of identity in human relationships [49]. In mobile business this principle bears primarily on issues of privacy, profiling and surveillance, and implies that collecting identity data by tracking the activities of individuals will be unacceptable if it is not reciprocal. Not knowing who is the peer collecting the data, how the data will be used, how to correct errors in the data and whether to expect a return describes the relationship as non-reciprocal and introduces asymmetry. Part of the relationship formed is invisible to us and, thus, we cannot influence the identity which we have to the other party. This is certainly true also for most electronic commerce technologies currently in use including mobile business but, as technology becomes more pervasive and ambient, this type of informational asymmetry will increase. Mobile business service providers should consider that respecting reciprocity often involves a trade-off: a consumer may find profiling useful since it allows a personalised service to be offered but, on the other hand, it may be uncomfortable if the relationship is asymmetrical with regard to control and access to information. At the very least, the consumer should be remunerated for the informational asymmetry either directly or indirectly in a fair and acceptable to both parties way. There is already some work underway in valuation of privacy [22] but we advocate that the asset to be valued should be identity instead. In the case of the ubiquitous retail system examined here, consumers were not offered a comprehensive means to either review or modify information collected about them neither were they offered the opportunity to directly benefit from the use of their personal information. In fact, the perceived benefit was some degree of automation in the replenishment task of home supplies but on balance this was not seen as a fair trade-off for the information they gave up. This observation justifies the reluctance of the focus groups participants to accept the use of personal information by the system.

The principle of understanding concerns the role of identity in the mutual comprehension which supports relationships [5, 11]. In mobile business, this principle implies that consumers need to understand the service provider and vice versa. Thus, although technologies may lower the barrier of entry to the mobile marketplace consumers prefer to engage in business activities with parties for whom they have access to a comprehensible company identity. Indeed, the experience in consumer-to-consumer commerce has already shown that perception of identity of the seller affects directly the perceived risk of the transaction, the willingness of the buyer to transact with the particular seller and last but not the least the price paid. Such understanding frequently involves what psychologists have called 'simulation': the ability to see things from the point of view of another agent. If the materials for this understanding are not provided, trust and consequently mobile business may suffer. Furthermore, the principle of understanding affects the relationship in both directions. At the same time when the consumer needs to understand the supplier that is engaged with in mobile commerce, the business has also to understand and respect the identity of the consumer and modify its practices accordingly. When this did not occur in the ubiquitous commerce scenario the consequence was that it created a threat for the balance of family structure. Of course, this resulted in creating a considerable barrier to adoption of the system.

These three principles provide a basic framework or conceptualisation for issues of identity in mobile business. They derive from existing resources in the humanities, and can be applied to contemporary conditions and refined through this process. Most cases, of course, can be subtle and complex and two or more of the basic principles given here would undoubtedly appear intertwined together in any situation: When does anonymised data mining become individual profiling? Is it practicable to inform individuals when their profile has been sold on and what is a fair use of identity information by the service provider? How sharp a distinction exists between the data used in the *identification* of a person, for example in authenticating a transaction, and that person's basic *identity* or identities? With the proliferation of next generation mobile systems and ubiquitous computing these questions will acquire greater urgency. In terms of identity, this advanced form of mobility implies that old principles manifest in new contexts: foundational issues of human relationships are reappearing in circumstances and situations created by a fabric of ambient and pervasive information and communications technologies. The clear implication for next generation mobile business, therefore, is that we need to better understand this relationship, and the requirements due to identity placed on the design and deployment of novel mobile business services.

6. Concluding Remarks

Mobile identity management systems are emerging as a response to the emerging crisis of personal information management for consumers as well as the slower than expected growth of electronic and mobile business due to the lacking development of trust relationships between consumers and suppliers. Next generation converged public communication networks will offer novel opportunities for business through the provision of dynamic, re-configurable, federated constellations of services. In this context, mobile identity management would become a core infrastructure component for the deployment of next generation mobile business services. However, such services affect humans in intimate ways by challenging their notions of identity and of self. It is, thus, important that in order to be effective and acceptable the emerging service architectures should accommodate these needs in a usable and inclusive approach.

Factors that are deemed as important to understand human identity and the construction of the self include the competing demands of individuality and community membership, privacy, trust, duties, rights and expectations. Mobile business forces these issues to manifest themselves in new shapes and forms, and although a re-examination of these factors and their relationships may be required, the issues themselves have not gone away. We advocate that in designing novel mobile business systems that inevitably incorporate mobile identity management as a core component, the enacted view is the appropriate basis for analysis. Last but not least, we anticipate that the level of involvement of human factors in discussing mobile identity management is crucial. We expect that widening the discipline boundaries for future research on identity in mobile business will be essential for the development of acceptable mobile service provision systems.

References

1. Abowd, G.D.; Mynatt, E.D. and Rodden, T. The Human Experience, *IEEE Pervasive Computing*, 1, 1 (January 2002), 48-57.
2. Asunmaa, P.; Inkinen, S.; Nykänen, P.; Päivärinta, S.; Sormunen, T. and Suoknuuti, M. Introduction to Mobile Internet Technical Architecture, *Wireless Personal Communications*, 22, 2 (August 2002), 253-259.
3. Bakos, Y The emerging landscape for internet e-commerce, *Journal of Economic Perspectives*, 15, 1 (January 2001), 69-80.
4. Bellman, S.; Lohse, G. and Johnson, E. Predictors of online buying behavior. *Communications of the ACM*, 42, 12 (Dec. 1999).
5. Boer S. and Lycan, W.G. *Knowing Who,* Bradford, 1986.
6. Burkhardt, J.; Henn, H.; Hepper, S.; Rindtorff, K. and Schaeck, T. *Pervasive Computing*, Addison-Wesley, 2001
7. Cheskin Research *eCommerce Trust Study*, Research Report, 1999.
8. Clark, R. Human identification in information systems: management challenges and public policy issues, *Information Technology & People*, 7, 4 (December 1994), 6-37.
9. Davies, N. and Gellersen, H.W. Beyond Prototypes: Challenges In Deploying Ubiquitous Systems, *IEEE Pervasive Computing*, 1,1 (March 2002), 26-35.
10. Fano, A. and Gershman, A., The Future of Services in the Age of Ubiquitous Computing, *Communications of the ACM,* 45, 12 (December 2002), 83-85.
11. Flanagan, O. *Varieties of Moral Personality: Ethics and Psychological Realism,* Cambridge, MA: Harvard University Press, 1991.

12. Global Commerce Initiative *The GCI Intelligent Tagging Model, An examination of product and supply chain opportunities*, Whitepaper, 2001.

13. Godwin J.U. Privacy and security concerns as major barriers for e-commerce: a survey study, *Information Management & Computer Security*, 9, 4 (September 2001), 165-174.

14. Goffman, E. *The Presentation of Self in Everyday Life,* New York: Doubleday, 1956.

15. Guthrie, W.K.C. *The Sophists, A History of Greek Philosophy, Vol 1,* Cambridge University Press, 1971.

16. Hagel III, J. and Rayport J. The new infomediaries, *The McKinsey Quarterly*, 4 (April 2000), 54-70.

17. Hoffman, D.L., Novak, T.P. and Peralta, M.A. Building consumer trust online, *Communications of the ACM*, Volume 42, Number 4 (April 1999), 80-85.

18. IBM Corporation, *Project Smart Pad.*

19. IIR *The Path to 4G*, London, UK, 2002.

20. Jarvenpaa, S.; Tractinsky, N. and Vitale, M. Consumer trust in an Internet store. *Information Technology and Management,* 1, 1(January 2000), 45–71.

21. Katz, R. The post PC era: It's all about services, *Networking 2002*, Pisa, Italy February 2002.

22. Kleinberg, J.; Papadimitriou, C.H and Raghavan, P. On the value of private information, *Eighth conference on Theoretical Aspects of Rationality and Knowledge,* July 2001.

23. Kraut, R.; Chan, A.; Butler, B. and Hong, A. Coordination and virtualisation: the role of electronic networks and personal relationships, *Journal of Computer Mediated Communication*, 3, 4 (September 1998).

24. Lawrence, G.S.; Almasi, V.; Kotlyar, M.S.; Viveros, S. and Duri, S. Personalization of Supermarket Recommendations, *Data Mining and Knowledge Discovery*, 5, (August 2001), 11-32.

25. Lucas, P. Mobile Devices and mobile data-issues of identity and reference, *Human-Computer Interaction*, 16, 2 (April 2001), 323-336.

26. Mintel International *Credit Cards*, Research report, 2000.

27. May P. *Mobile Commerce - Opportunities, Applications, and Technologies of Wireless Business*, Cambridge: Cambridge University Press, 2001.

28. Matejkovic, J. and Lahey, K.E Identity theft: no help for consumers, *Financial Services Review*, 10 (July 2001), 221-235.

29. Muller-Veerse, F. Mobile commerce report, Durlacher Corporation, London, 1999.

30. National Research *Council Looking Over the Fence at Networks: A Neighbor's View of Networking Research*, National academies Press, 2002.

31. Orlikowski W. and Iacono, C.S. The truth is not out there: An enacted view of the Digital Economy, In Brynjolfsson, E. and Khim, B. (eds.) *Understanding the Digital Economy: Data, Tools and Research*, MIT Press, 2001.

32. Robert Pascoe Building Networks on the Fly, IEEE Spectrum, 38, 3 (March 2001), 61-65.

33. Pew Research Center *Pew Internet and American Life Project Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, August 20, 2000. http://www.pewinternet.org/reports

34. Raman, B.; Agarwal, S.; Chen, Y.; Caesar, M.; Cui, W.; Johansson, P.; Lai, K.; Lavian, T.; Machiraju, S.; Morley Mao, Z.; Porter, G.; Roscoe, T.; Seshadri, M.; Shih, J.; Sklower, K.; Subramanian, L.; Suzuki, T.; Zhuang, S.; Joseph, A.D.; Katz, R.H. and Stoica, I The SAHARA Model for Service Composition across Multiple Providers In Mattern, F. and Naghshineh, M. (eds.): *Pervasive Computing: First International Conference*, *Lecture Notes in Computer Science*, 2414 (August 2002), 1-14.

35. Rannenberg, K. Multilateral Security A Concept and Examples for Balanced Security, *ACM New Security Paradigms Workshop*, (September 2000), 151-162.

36. Reichenbach M. Individual Risk Management - Defining User Requirements for Secure and Efficient Electronic Payments, *Proceedings of the Fourth International Conference on Electronic Commerce Research*, 2001.

37. Reid, R. and Brown, S. I hate shopping! An introspective perspective, *International Journal of Retail & Distribution Management*, 24, 4, (June 1996), 4-16

38. Roussos, G.; Koukara, L.; Kourouthanasis, P.; Tuominen, J.; Seppala, O.; Giaglis, G. and Jeroen F. A case study in pervasive retail, *ACM MOBICOM Second International Workshop in Mobile Commerce*, (September 2002), 90-94.

39. Roussos, G.; Spinellis, D.; Kourouthanasis, P.; Gryazin, E.; Pryzbliski, M.; Kalpogiannis, G. and Giaglis, G. Systems Architecture for Pervasive Retail, *ACM SAC E-Commerce*, (March 2003), 350-356.

40. Sadeh N. M-Commerce - Technologies, Services, and Business Models, New York, NY John Wiley, 2002.

41. Shapiro, Carl and Varian, Hal *Information Rules: A strategic Guide to the New Economy*, Harvard Business School Press, 2000.

42. Sproull, L. and Kiesler, S. Reducing social context cues: Electronic mail in organizational communication, *Management Science*, 32, 11, (November 1986), 1492- 1512.

43. Strader, T.J. and Ramaswami, S.N. The value of seller trustworthiness in C2C online markets, 45, 12 (December 2002), 45-49.

44. Strader, T. and Shaw, M. Consumer cost differences for traditional and Internet markets, *Internet Research*, 9, 2 (February 1999), 82–92.

45. Storey, M.; Blair, G. and Friday, A. MARE: Resource Discovery and Configuration in Ad Hoc Networks, *Mobile Networks and Applications*, 7 (August 2002), 377–387.

46. Taylor, C. *Sources of the Self: The Making of the Modern Identity,* Cambridge, MA: Harvard University Press, 1989.

47. Trigueros, C. *ALBATROS: Electronic tagging solutions for the retail sector*, Informatica El Corte Inglés, Madrid, Spain, 1999.

48. Tuecke, S.; Czajkowski, K.; Foster, I.; Frey, J.; Graham, S.; Kesselman, C. and Vanderbilt, P. *Open Grid Service Infrastructure: Grid Service Specification, Global Grid Forum*, October 2002.

49. Tugendhat, E. *Self-Consciousness and Self-Determination,* Cambridge, MA: MIT Press, 1986.

50. U.S. Federal Trade Commission *Privacy Online: Fair Information Practices In The Electronic Marketplace*, 2000.

51. U.S. Federal Trade Commission *Identity theft complaint data: Figures and Trends in Identity Theft*, 2001.

52. Varian, H.R. Price discrimination, In Schmalensee, R and Willig, R. *Handbook of Industrial Organisation*, 1989, North-Holland Press, Amsterdam.

53. Varshney, U.; Vetter, R. and Kalakota, R. Mobile commerce: A new frontier, IEEE Computer, 33, 10 (October 2000), 32-38.

54. Varshney, U. and Vetter, R. Mobile commerce: Framework, applications, and networking support, *ACM/Kluwer Journal Mobile Networks Applications*, 7, 3 (June 2002), 185–193.

55. Veizades, J.; Guttman, E.; Perkins, C. and Kaplan S. *RFC 2165: Service Location Protocol*, Internet Engineering Task Force, 1997.

56. Walther, J. and Burgoon, J.K. Relational communication in computer-mediated interaction, *Human Communication Research*, 19, 1 (January 1998), 50-88.

57. Wiederhold, G. Mediators in the architecture of future information systems, *IEEE Computer*, 18, (November 1992), 38-48.

58. Wireless World Research Forum *Book of Visions*, Whitepaper, Temple, Arizona, 2002.