22-4-2008

Privacy, Value and Control Issues in Four Mobile Business Applications

Benjamin D. Renegar
University of Wollongong, mail@bentranet.com

Katina Michael
University of Wollongong, katina@uow.edu.au

M G. Michael
University of Wollongong, mgm@uow.edu.au

Privacy, Value and Control Issues in Four Mobile Business Applications

Abstract

This paper presents four case studies that explore the adoption and acceptance of mobile technologies and services within the context of the privacy-value-control (PVC) trichotomy. The technologies studied include: the mobile phone, electronic toll payment tags, e-passports, and loyalty card programs. The study shows that despite the potential barriers to adoption in each of the depicted cases, the applications were embraced with great success soon after their introduction. An understanding of why these mobile innovations succeeded in spite of the concerns surrounding them will serve to help practitioners understand other issues currently plaguing emerging technologies like radio-frequency identification (RFID) tags and transponders. The contribution of this paper is not only in its usage of secondary sources to support case development and subsequent cross-case analysis but on the importance of emphasizing the value proposition to the consumer to ensure the success of an innovation. The PVC trichotomy emphasizes the need to harmonize privacy, value and control.

Keywords

privacy, value, control, mobile business applications, adoption, diffusion, consumer acceptance

Disciplines

Physical Sciences and Mathematics

Publication Details

Privacy, Value and Control Issues in Four Mobile Business Applications

Benjamin D. Renegar, Katina Michael and M.G. Michael
School of Information Systems and Technology, Faculty of Informatics
mail@bentranet.com, {katina,mgm}@uow.edu.au

Abstract

This paper presents four case studies that explore the adoption and acceptance of mobile technologies and services within the context of the privacy-value-control (PVC) trichotomy. The technologies studied include: the mobile phone, electronic toll payment tags, e-passports, and loyalty card programs. The study shows that despite the potential barriers to adoption in each of the depicted cases, the applications were embraced with great success soon after their introduction. An understanding of why these mobile innovations succeeded in spite of the concerns surrounding them will serve to help practitioners understand other issues currently plaguing emerging technologies like radio-frequency identification (RFID) tags and transponders. The contribution of this paper is not only in its usage of secondary sources to support case development and subsequent cross-case analysis but on the importance of emphasizing the value proposition to the consumer to ensure the success of an innovation. The PVC trichotomy emphasizes the need to harmonize privacy, value and control.

1. Introduction

Surrounding the invention of every new information and communication technology (ICT) are a myriad of challenges that need to be resolved so that the innovation will not fall by the wayside. For example, some technologies face technical limitations, while others face consumer backlash. This paper uses a new paradigm to investigate mobile innovations- the privacy-value-control trichotomy. While themes of privacy and control have been addressed in the literature, the value proposition of a given service has only been considered within a business context. The four mobile business applications explored in this investigation include location-based services (LBS), e-tollway, e-passport and loyalty programs. In each case the key research issues are identified and discussed. The main question asked is why innovations that have

endured such difficult beginnings- in terms of consumer acceptance- have gone on to become engrained in our everyday lives.

2. Definitions

The concept of *value* is an all-encompassing term which references the value proposition a technology or service affords the end user. Whilst many analyze technologies in terms of benefits or simply convenience, the value proposition is an equation of all the positive factors that interest the individual. It can include cost savings, time reductions, efficiency, personalization, safety and security, as well as convenience and other tangible and intangible benefits. All the case studies that will be discussed in this paper provide some form of value to the end user. Understanding this value is critical in examining how it affects acceptance given the inherent privacy threats that the technology may impose. *Privacy* refers to the information privacy needs of consumers. Of primary concern in regard to RFID usage in retail, is the collection of personal information that pertains to consumer shopping preferences, actions and behavior. It is the collection, use and disclosure of this information, particularly when it may be incorrect or unverified, to track and monitor individuals without their awareness or express approval, that is commonly recognized as one of the most prominent threats. This privacy concern is similar across all the case studies to be explored in this paper, which will again provide an important platform for assessing how value and privacy is related. Finally, the dimension of *control* is another important variable in consumer acceptance of technologies. It relates to the individual's ability to control the information that is collected and stored by the technology or its ability to record, track or identify that individual's actions. The level of control that is provided either inherently through the technology or by the service provider, whether that be perceived or real, is seen as an important element that, when combined with the value proposition, can affect consumer

acceptance. Interestingly, the case studies to be discussed all provide different means or levels of control in regard to end users and their privacy.

2.1 Key works

There was a scarcity of *holistic* qualitative and quantitative studies for review. Studies either addressed privacy, value and control separately, or no more than two of these concepts [1, 2, 3, 4, 5]. Key quantitative studies reviewed for this work are shown in Table 1, alongside the respective key outcomes.

Table 1. Key quantitative study outcomes

Study	Outcome
(Günther & Spiekermann, 2005; Spiekermann, 2005)	Regardless of which privacy-enhancing technologies are used, fear remains.
(Roussos & Moussouri, 2004)	Consumers understood the value proposition but were still concerned about privacy implications.
(Ng-Kruelle, Swatman, Hampe & Rebne, 2006)	Cultural dimensions affect the way in which consumers view the privacy threat.
(Ng-Kruelle, Swatman, Rebne & Hampe, 2002)	Consumers feel a lack of control over the technology and a great power distance.

3. Case 1: Mobile phone

Cellular coverage is now accessible by 80 percent of the world's population of over six billion, and over 90 percent will have coverage by 2010 [6]. The actual number of mobile phone users is estimated to be around 1.8 billion, which equates to a global penetration rate of nearly 28% [7]. In developing countries where mobile communications allow them to "leapfrog" traditional wired telephony networks, growth rates are staggering. Between 1998 and 2003, mobile phone usage exploded in Africa by 5000% [8]. Similarly, India and China are now being viewed as potential "cash cows" for the industry, where the sheer number of potential subscribers is seen as a highly lucrative source of growth [9]. In many developed regions, mobile penetration exceeds the population, the greatest example shown by Luxembourg where mobile penetration is at 151.61%, although figures around 90% to 100% are more common [10]. Taking into account young children, penetration rates of around 80% would still equate to a clear majority of adults using mobile services. Even in developing countries,

reports have shown that penetration rates are stabilizing at around 80-85% [11].

3.1 Convenience- communications on the go

The value proposition of the mobile phone extends from the convenience offered by its inherent mobility. Its ability to provide location-based, and even location-aware services, enabling rich communication not confined to a single location, affords individuals great power and convenience. Without being tied to a landline, or to a computer, users can communicate in a multitude of ways with others, on the move in a completely seamless fashion. Furthermore, new technologies such as 3G mobile services are further positioning mobile phones as extremely powerful mobile computing devices.

3.2 Location ID & the threat of interception

In a study conducted by Häkkilä and Chatfield [12] regarding perceptions of mobile phone privacy, it was shown that over 82% of respondents considered their mobile phone a "private device." The mobile phone presents a number of unique privacy threats, yet interestingly, as indicated by the aforementioned statistic, such privacy threats are seldom considered by end users [13]. Richtel [14] explains how many citizens in the U.S. are completely unaware that government authorities can track their movements by monitoring the signals that are emitted from the handset.

In 1994, as O. J. Simpson infamously fled down a Los Angeles freeway, he was talking on his mobile phone, and engineers were able to use his mobile signal to triangulate his position and direct police to his location [15]. By 1996, the U.S. Federal Communications Commission (FCC) had mandated as part of the E-911 initiative that by 2001 mobile carriers must be able to identify the location of a caller with reasonable accuracy. In the United Kingdom, tracking records for mobile phones must be retained by providers for at least two years and be available to law-enforcement agencies when required [16]. Whilst the intended use of such tracking information is deemed valuable for emergency or law enforcement purposes, it is also seen that such data opens the door for mobile phone providers to unleash a multitude of location-based services that take advantage of knowing exactly where consumers are located or to generate patterns which represent their typical movements. As most mobile phone users generally carry their phone on them at all times, Charny [17] describes the potential to create a highly lucrative market on emerging services whereby providers can know the exact locations of millions of subscribers at any given time.

There are a number of methods that can be used to track mobile phone users. The first such method [18] is "network based," and involves the triangulation of signals by using a number of fixed cellular base-stations. Such a system however can be impractical for wide-scale usage due to bandwidth constraints, and furthermore the accuracy of this method is greatly affected by cell size, which in rural areas in particular can be too great to provide reasonable accuracy. Nonetheless, newer 3G mobile networks can provide location information at even finer granularity than before [19]. Another method involves the use of GPS, a feature which many phones are now incorporating. According to Best [20], leading manufacturer Nokia has already stated that the incorporation of GPS into mobile phones will soon be as "ubiquitous as the camera phone." Unlike cell-based triangulation, GPS provides greater accuracy and can operate independent of the phone itself, meaning that location information could be obtained even if the phone is not in use. Many services are now being offered around the world allowing individuals to track a mobile phone that is GPS-enabled via the Internet. Such services are typically positioned to parents who wish to monitor their children's activities or to employers who want to track where their mobile employees are [14]. Consider the case of teacher John Halpin who was given a mobile phone by the Department of Education which incorporated a GPS tracking device, and who was later fired from his position after records revealed inconsistencies with the times he had been lodging, showing that he was leaving work earlier than stated [21].

The mobile phone also presents other privacy concerns in regard to the interception of signals by third parties. Whitaker [15] describes how commercially available mobile phone listening devices can record multiple conversations and locate the geographical position of callers at the same time. Importantly, he emphasizes that whilst such products are marketed and sold to government agencies and telecommunications companies, they can easily find their way into the hands of unscrupulous individuals who can use them against unsuspecting mobile phone users. Many security experts will openly acknowledge that all wireless communications are inherently flawed, as there will always be the potential for some degree of interception [22].

3.3 Control maintained by opting out
Theoretically, users can exercise control over other parties tracking their location by simply turning off their phone. However, in doing so, they prevent access to the phone's features which provide the value in the first place. Given the high penetration rates of mobile phones throughout the world, it would seem that the potential for unwanted third parties to track a mobile phone's location or to intercept the signals transmitted by the phone is far outweighed by the value the technology offers and its apparent "necessity" for living in the modern world. In the case of the U.S., access to mobile phone tracking data is not openly accessible to any third parties. Even law enforcement agencies must apply for court permission and demonstrate "probable cause" that a crime is being committed before such information will be released by the phone operators [13]. Whilst such controls are put in place to protect the privacy of individuals, it is still important to recognize that where the technology provides the capability, it will almost always be exploited in some way by unscrupulous people [15]. Furthermore, with such a massive market of mobile phone users who increasingly possess ever more sophisticated mobile handsets, the potential of offering location-based services will most certainly prevail as consumers once again become lured by the value such services would provide [23].

4. Case 2: Electronic toll collection
Electronic toll collection (ETC) systems are now widely deployed in most countries throughout the world and are the cornerstone for Intelligent Transportation Systems (ITS). One of the first such systems was implemented in Trondheim, Norway by the Q-Free company in 1988 [24]. International ETC examples include: TollTrax in India, Hi-Pass in South Korea, Autotoll in Hong Kong, E-Pass in Manila, Telepass in Italy, Eazy Pass in Ireland, AutoPASS in Norway, E-ZPass in north-east USA, and the e-Tag in Australia [25]. It would seem that RFID-powered toll collection systems are making their way to freeways and cities as an effective solution to the ever-increasing congestion problem and the necessity to fund new roads through the collection of tolls. By 1996 alone, there were already several thousand ETC-equipped lanes throughout the U.S., Europe and Japan [26].

An ETC system typically involves the use of an RFID powered tag which is placed on an individual's vehicle. As the vehicle passes through a toll plaza, RFID readers mounted above the road identify the individuals through the RFID tag and will then typically deduct the toll amount from their accounts [27], [28]. RFID allows the system to operate such that drivers do not necessarily have to slow down, and can even maintain highway speeds with the tag still being read accurately. Advances in technology have also

facilitated the ability to read tags and deduct tolls even in multi-lane free-flow situations; that is where cars are not restricted to staying in a single lane and are free to change lanes as required [26], [29]. Furthermore, such a system can also accurately identify vehicles even in dense traffic without requiring direct visibility to the license plate as some vehicle-recognition systems require [28].

4.1 No need for cash and less traffic

Historically, toll payment involved an individual stopping their vehicle to pay a collector or place cash into an automated collection machine which ultimately resulted in congestion [26]. The key value proposition that electronic toll collection systems offer is convenience and time saving. Such a system eliminates the burden to have cash available to make toll payments and provides individuals and corporations the convenience of an account which can provide better tracking of toll expenditure with more convenient payment options [30]. In regard to time savings, traffic flow is greatly improved and congestion reduced [27]. Furthermore, ETC systems have also been shown to significantly reduce environmentally harmful emissions at toll-collection points by as much as 63 percent [24]. Toll operators themselves have seen great value in ETC as a means of increasing throughput, generating additional revenue, reducing operating costs, and improving the level of customer service to road users [25].

4.2 Function creep and the loss of anonymity

The electronic tag which an individual places inside their vehicle typically contains at least a unique identification number which allows the toll system to identify and subsequently charge that individual [25]. In some installations, the tag may contain further information such as license details, the account holder's name, account details and tag balance. Whereas cash payment in the past provided almost complete anonymity, electronic toll collection systems have opened up the possibility of tracking individuals' movements by monitoring the locations and times when the electronic tag is used [31]. In some countries where toll roads are common and such systems are widespread, drivers' actions can be inferred in great detail simply by monitoring their toll payment activities. Caldwell [29] highlights two potential privacy concerns with regard to electronic toll collection. The first is illegitimate use of drivers' personal information regarding their payment details, movement and driving habits that could be accessed if electronic records are compromised through a "cyber-

break-in." This was demonstrated when the New Jersey Turnpike electronic toll collection system was "hacked" in 2000 by a programmer who worked on the system [32]. He was successfully able to view account details and usage information for users of one of the largest ETC systems in the United States [31].

The second potential concern is legitimate use of such information by government authorities or road operators who wish to monitor driving patterns and behavior of motorists. This could extend to include other potential uses such as traffic surveillance in regard to monitoring driver speeds and stolen vehicles [24]. Court cases in the U.S. have already demonstrated the potential for toll-tracking information to be used to verify an individual's whereabouts and movements. The conviction against a nurse in New Jersey, who was accused of murdering her husband, was aided by E-ZPass toll records which verified to prosecutors where she had been, and when [33]. In another example, 30 New York police detectives were reportedly re-assigned after E-ZPass toll records suggested they were making false overtime claims based on their driving behavior [34].

4.3 Towards mandatory electronic collection

In some installations, cash payment options still operate in tandem with electronic toll payment. It is becoming increasingly common, however, for electronic toll collection systems to become the de facto means by which individuals can make their toll payment. Studies show that for maximum efficiency, ETC systems provide greatest benefit when used in isolation, as opposed to hybrid systems which allow traditional payment mechanisms [26]. It is becoming inherently mandatory for individual's to install an electronic tag in their vehicle if they wish to use particular routes or avoid paying higher toll prices if they pay by cash [33]. Ultimately in the case of electronic toll collection systems, it is apparent that convenience is winning out over potential privacy threats. For both toll road operators and users, this is highlighted by the high growth rates in ETC usage around the world [25].

With an ever-increasing base of tag users, the potential for privacy misuse will become more apparent over time. As road operators see value in monitoring individual driver behavior, to forecast or evaluate traffic patterns for instance, individual driver tracking may become more prevalent. It should be noted, however, that regulatory efforts in many countries can still protect ETC users with regard to the usage of their personal information. In Australia, for example, the Australian Standard AS/4721-2000, *Personal Privacy*

Practices for the Electronic Tolling Industry attempts to address privacy issues by applying the ten National principles for the handling of personal information [35]. This standard explicitly recognizes the potential commercial use of such toll information and allows for such usage provided that the data is "de-identified" and made anonymous to protect individuals from identification [34].

5. Case 3: e-Passports

For centuries, passports have been used as a standard means of providing diplomatic protection and identification of the bearer when traveling through borders and into foreign jurisdictions [36]. The passport in the form we know today is the result of conferences held following the First World War in 1920 which sought to standardize passport and visa standards for all member states of the League of Nations (later The United Nations) [35]. Passport standards have been administered by the International Civil Aviation Organization (ICAO) since 1944. Passports, which are referred to by the ICAO as Machine Readable Travel Documents, will typically contain information such as an individual's full name, nationality, place of residence, place of birth and date of birth, with a mandatory full-color photograph. Their "machine readable" capability comes from the inclusion of a two-line machine readable zone (MRZ) of characters in Optical Character Recognition-B style that incorporates key information from the passport in a manner that can be easily recognized by a machine [37].

RFID-enabled passports, which have also been termed e-Passports or biometric passports, possess all the same information, but in digital form. This includes a digitized photograph of the individual which can be used to enable biometric comparison through facial recognition [38], [39], [40]. It is this facial recognition that is the only mandatory, globally interoperable biometric for individual identification purposes [41]. Although ICAO standards for passports also allow for iris or fingerprint data to be used as well, this is at present optional [37], [42]. The development of the e-Passport has also resulted in the development of standards which support a worldwide Public Key Infrastructure (PKI). Public Key Cryptography is utilized in e-Passports to encrypt the data contained within the RFID chip [40]. Digital signatures produced by the issuing country ensure the validity, authenticity and integrity of data stored in the RFID chip and thus theoretically prevent against fraudulent modification, copying or access [40].

5.1 Greater national security

The drive towards e-Passport adoption was spurred directly by the United States and the ICAO. In 2002 the U.S. mandated through the *Border Security and Visa Entry Reform Act 2002,* that countries participating in their Visa Waiver Program must have provisions in place by October 2004 to comply with the biometric and document identification standards established by ICAO in 2003 [38]. This deadline was extended to October 2006 after significant delays caused by revisions to the e-Passport's design [38]. It is important to note, however, that moves towards biometrics to enable more effective, automated verification of individuals was already progressing long before the e-Passport was given an impetus to introduction. The INSPASS system was introduced into the United States in the late 1990s as a means of allowing frequent visitors to the country unattended, automated entry through the use of biometrics to verify identity [43]. Whilst the system was discontinued in 2002, it bears a striking similarity to much of the same *value* governments and the ICAO have promoted with the e-Passport.

The value proposition of the e-Passport is typically couched in terms of security and convenience. Common claims include the e-Passport's ability to allow automated identity verification, faster immigration inspections, and greater border protection and security [44]. Whilst it is intended that passports will still be read by human personnel to verify the information, some countries such as Australia have already announced plans to provide self-service kiosks. The technology to be used in Australia, referred to as SmartGate, has already undergone successful trials in 2005 and is to commence operation in international airports around the country in the near future [45]. Such technology, if implemented in airports around the world, would allow much quicker processing times of passengers for travelers entering the country (Australia Customs Service, 2007). Many countries, including the UK, have already begun work on similar systems [46].

The greatest value of the e-Passport as stressed by most issuing authorities is the enhancement to security they are purported to provide through the digital storage of passport information [38]. Certainly, given the current level of importance placed on national security, governments have been keen to push this technology as a means of providing more stringent monitoring of individuals entering and exiting the country. The use of biometric information, it is claimed, will greatly aid in countering identity fraud which had become a major issue with traditional passports [41].

5.2 The risk of identity theft and civil rights

The privacy concerns surrounding e-Passports are primarily related to the ability to access passport information without contact, a capability afforded by the use of RFID to store the passport's data contents. It is this potential for surreptitious access, perhaps by a criminal attempting to commit identity fraud that has caused much controversy over e-Passport adoption [47]. Potential misuse by the government is particularly evident in the controversial USA PATRIOT Act introduced just 43 days after 11 September, 2001 whereby the U.S. Federal Bureau of Investigation was given authority to seize personal information without notifying the individual concerned [48]. It is theoretically possible for governments to use such acts in order to link passport biometric databases with other surveillance mechanisms to monitor individuals without their awareness [47]. Juels, Molnar and Wagner [49] identify six key areas of concern regarding privacy and e-Passports: clandestine scanning, clandestine tracking, skimming and cloning, eavesdropping, biometric data leakage and cryptographic weaknesses. Juels [50] also notes the threat of function creep. He explains how over time, consumer demands for convenience may give way to e-Passports being used as authenticators for a range of consumer transactions. Such a move, it is feared, could undermine or erode the data-protection measures that have been incorporated to protect privacy and furthermore spread such identification information amongst more widely divergent systems [48].

Given the global reach of e-Passport initiatives, there has understandably been much concern raised over such privacy issues. Civil rights campaigners in particular stress how such e-Passport developments have created the potential for a global database containing biometric information for over a billion people [51]. Interestingly, in development of the U.S. passport, open comments by citizens revealed that of over 2300 responses, 98.5 percent received were negative, and 86 percent were explicitly concerned about privacy [38]. Nonetheless, the U.S. e-Passport initiative has proceeded, and as of 2006, over 13 million e-Passports had been issued [52]. Globally, it is reported that over 50 million e-Passports have been issued, which again emphasizes that despite the privacy concerns, the technology has undoubtedly been deployed "successfully" [53].

The media has also been quick to highlight potential failures with the technology, demonstrated by the exposure given to Lukas Grunwald who successfully cloned the U.S. e-Passport and then dumped the contents onto an ordinary contactless smart card [54].

A further threat was also exposed by Kevin Mahaffey and John Hering who demonstrated how an explosive device connected to an RFID reader could be triggered when a U.S. citizen carrying an e-Passport came within reach of the reader [53].

5.3 Total State control

Given the mandatory nature of passports there is very little individuals can do to avoid using one for traveling abroad. As most countries are now issuing e-Passports, there is also no option for individuals to request a non-RFID passport. There is also little an individual can do to control how government authorities access and use the information on the passport when they are entering a foreign country. However, beyond the border control point, individuals concerned about the privacy threats mentioned earlier can still retain some control over their e-Passport by ensuring they manage it carefully. Companies such as Paraben have already begun marketing "strong hold bags", which are essentially Faraday cages in which a passport can be stored when not being used, to provide a protective barrier against unwanted third-party access [55]. Such a move was even recommended as a means of completely preventing unauthorized readings by the ICAO itself, who stated that the potential for unauthorized reading could not be "completed ruled out" [56].

6. Case 4: Loyalty programs

Loyalty programs have been in widespread existence now since the 1980s, when retail organizations began to focus on building lasting customer relationships instead of focusing purely on short-term profitability [57]. The first modern loyalty program was instituted by American Airlines in 1981 with its "frequent flyer" program [58]. However, such programs quickly spread across a range of consumer industries including hotels, credit card companies, retailers, car rental companies, restaurants and entertainment firms [57]. A loyalty program will typically involve consumers identifying themselves at the retail outlet, usually through a magnetic-swipe or bar-coded plastic card, in order to receive immediate or delayed benefits for purchasing certain brands or for simply using that particular outlet [56]. Astonishingly, grocery store loyalty program usage within the United States is more widespread than Internet and personal computer penetration, with statistics showing that over 86 percent of adults are members of at least one, and in many cases, multiple loyalty programs [59]. In Canada that figure is around 97 percent and in the UK, penetration had reached 85 percent [60].

6.1 Greater consumer rewards

In the case of loyalty programs, the value proposition is critical for encouraging consumer use and for developing the brand loyalty which the programs aim to achieve. A number of elements are described by Yi and Jeon [61] that determine such value in a loyalty program. They include: (1) the cash value of rewards, (2) the choice of rewards, (3) the aspirational value of rewards, (4) the likelihood of achieving the rewards, and (5) how easy the loyalty scheme is to use. Typical examples of value that loyalty programs offer members include discounts on individual items or the entire shopping bill, points which can be redeemed for a range of rewards such as flights, accommodation, homewares, clothing and entertainment, and preferential "VIP" treatment. Studies conducted by the Boston University College of Communication demonstrate that 69 percent of consumers believe that their membership in a loyalty program benefits them in the form of lower prices and special promotions [58].

6.2 Consumer data profiling and warehousing

The major privacy threat that extends from the use of loyalty programs is the ability to tie purchases of specific products to individual consumers and monitor their purchasing behavior over time. Retailers collect such information to build profiles on their consumers. They even admit that such consumer profiles are commonly shared and exchanged with "preferred partners" [59]. Almost half of people who are members of loyalty programs are completely unaware of the tracking and monitoring that is occurring by participating in such schemes [58]. Moreover, studies have shown that consumers will trade their personal information if they perceive that the loyalty program is providing substantial value to them [58]. A study conducted by Graeff and Harmon [62] also found that in regard to loyalty programs, consumer perceptions were typically positive and most consumers did not associate such schemes with the collection and use of personal information. Loyalty programs are the ultimate demonstration of the trade-off consumers make of their privacy in order to gain something of value: a benefit, reward, convenience or saving. Given the high penetration rates and evident success of these programs, it would seem that consumers have been easily won over by the premise of "something for nothing," with many oblivious or unconcerned about the privacy transaction that they are conducting.

6.3 Opting-in for maximum returns

A key element of consumer loyalty programs is their opt-in nature. As is highlighted by Bosworth [59], consumers are not forced into participating in such programs and can, if they wish, take their business elsewhere, or simply pay cash (minus any potential savings the loyalty card may provide). Consumers are also given control over their personal information by government regulations which in most countries give consumers the right to know exactly what information retailers are collecting and how it is being used. Furthermore, access to such information will typically be provided or the information removed altogether if requested. Ultimately loyalty programs are about choice, and thus given the potential privacy invasion that participation in such schemes entails, the value proposition is clearly a very important element in convincing consumers to participate. It is important to note, that whilst loyalty programs involve voluntary participation, many such schemes have come under criticism for discriminatory pricing, in which non-members may be unfairly disadvantaged by not participating in the scheme [57]. This may ultimately drive consumers into participation to avoid being forced into paying higher prices or feeling ostracized.

7. Cross-case comparison

The most important facet common to all of these case studies is their dramatic levels of penetration and usage. Mobile phone penetration has reached remarkable levels, even in developing countries, and in many, penetration has grown to over 100%. Electronic toll collection is becoming increasingly common as the primary means for facilitating toll payments in busy cities around the world, with millions of tags now in use. E-Passports have become the new standard in global identification and have all but replaced traditional, chip-less passports in most countries. And consumers have embraced loyalty programs enthusiastically, with the majority of adults in countries such as the U.S., the UK, Canada and Australia, actively participating in such schemes. Keeping in mind such usage rates, it is also important to note another commonality between the mobile innovations, that of the presence of a range of privacy threats. It would appear given the widespread usage of the cases detailed, that privacy has not been a barrier to their adoption and consequent acceptance by society. Whilst the privacy concerns still exist and indeed, many individuals remain concerned about their privacy in relation to such technologies and services, on the whole it would seem that consumers have accepted each technology either because:

- The value proposition or level of control present, balances against the privacy issues (mobile phones, electronic toll collection, and loyalty programs), or
- Participation/usage is mandatory and the appropriate safeguards to privacy are in place (e-Passports).

In the case of the mobile phone, the value has become so ubiquitous that it is no longer even thought of or discussed. This ubiquity in terms of value would explain the lack of concerns consumers have towards their privacy in regard to mobile phone usage – it is simply not something most people would even think about. For electronic toll collection, individuals have embraced the convenience aspects presented by the technology in regard to simplifying toll payment, and it would seem that the simplicity of the technology (simply install the tag and forget about it) has again resulted in a general lack of concern about privacy issues. Loyalty programs are also clearly driven by their value proposition, without which, would provide little incentive or reason for consumer participation. Furthermore, given the amount of personal information collected, there must be equally significant value provided to ensure consumers feel the scheme is fair. Of the four case-studies discussed, the e-Passport is the only one where usage is almost completely mandatory for those wishing to travel internationally and also where individuals have very little control over how their e-Passport is used by authorities. In this situation, control in the form of legislation guarantees and reassures that personal information will be protected.

8. Balancing privacy, value and control

A key outcome that arises from the case studies presented is the varying relationship between these three elements and thus the balance each technology or service provides. It is clear, that in order to gain acceptance, privacy issues must be offset by value and control. This trichotomous relationship is illustrated in figure 1. In the case of mobile phones, it is evident that a somewhat low level of control is acceptable, given the relatively low vulnerability of individual privacy and the "medium" level of value the technology provides. With electronic toll collection, the vulnerability of user privacy is depicted to be in the "medium" range, yet as users can exercise some degree of control over their privacy by removing the tag or opting to use alternative routes or payment methods, control is depicted as being in the "medium" range. This "medium" range in regard to privacy and control, is offset by a high level of value evident in the convenience the technology affords. With regard to e-

Passports, the provider (i.e. the government) provides very little control. Furthermore, the value offered to the individual is realistically very low as well. This is reflected in the relatively high vulnerability of the individual's privacy which stems not from flaws in the technology, but the importance of the information to the individual and the consequences that could arise if it were compromised by another party. Finally, with loyalty programs, a high vulnerability of individual privacy which arises from the vast amount of personal information collected, is offset by a high level of control offered by providers by allowing consumers to freely to opt-out of such programs. The privacy risk is also further offset by the high level of value which such schemes must offer to encourage consumers to participate. In the case of mobile phones, electronic toll collection and loyalty programs, it is apparent that acceptance had to be earned through a favorable balance that was offered to consumers. In the case of e-Passports where the balance is unfavorable (as shown in figure 1), acceptance was not generally required as the technology was made mandatory by government authorities and the ICAO.
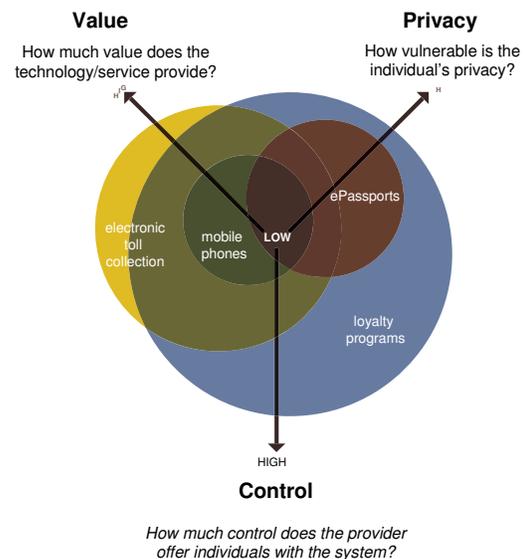

Figure 1. Privacy-Value-Control trichotomy

10. Conclusion

The purpose of this paper has been to provide a "walk" through the privacy-value-control paradigm as it applies to a number of mobile innovation. The study attempted to show how privacy concerns for specific mobile innovations have been offset by strong value propositions, or differing levels of control that allows the individual to perceive a sense of privacy, or bypassed through mandatory usage. The key outcome

that has been established by this paper is that a balance between privacy, value and control depends largely on the individual, the technology and the provider of the service; that is, the vulnerability of the individual's privacy, the value inherent in the technology or service, and the level of control provided by the service provider. What has been highlighted most importantly is that privacy is not a barrier to adoption; rather, technologies and services will still be accepted and used by the population provided that *the balance* is favorable to the individual – whether that be perceived or otherwise – unless the technology is mandated into use in a manner which can be justified by society.

References

[1] S. Inoue and H. Yasuura, "RFID privacy using user-controllable uniqueness," *RFID Privacy Workshop*, Cambridge, MA, 2004.

[2] R. Bansal, "Now you see it and now you don't," *IEEE Microwave Magazine*, vol. 5, pp. 32-34, 2004.

[3] S. Spiekermann, "Perceived Control: Scales for Privacy," International Conference on User Modeling, Scotland, 2005.

[4] L. Hyangjin and K. Jeeyeon, "Privacy threats and issues in mobile RFID," *International Conference on Availability, Reliability and Security*, Vienna, 2006.

[5] M. Ohkubo et al., *RFID Privacy Issues and Technical Challenges*, vol. 48: ACM, 2005.

[6] AFP, "Mobile operators aim to cover 90 percent of planet," in *Taipei Times Singapore*, 18 Sept. 2006.

[7] Informa, "1.8 bln mobile subscribers worldwide," 2005, http://www.itfacts.biz/index.php?id=P3359

[8] BBC, "Mobile growth 'fastest in Africa'," in *BBC Business*, 2005, http://news.bbc.co.uk/2/hi/business/331863.stm

[9] M. Reardon, "Emerging markets fuel cell phone growth," in *CNET News.com*, 2007, http://www.news.com/Emerging-markets-fuel-cell-phone-growth/2100-1039_3-6159491.html

[10] ITU, "Mobile cellular subscribers," 2007, http://www.itu.int/

[11] Telecomworldwire, "Many countries now have a mobile penetration rate above 100%, report says," 2006, http://findarticles.com/p/articles/mi_m0ECZ/is_2006_June_9/ai_n16464839

[12] J. Häkkilä and C. Chatfield, "Toward social mobility," in *Human computer interaction with mobile devices and services*, Salzburg, Austria, 2005.

[13] N. Swartz, "Mobile Phone Tracking Scrutinized," *Information Management Journal*, vol. 40, p. 16, 2006.

[14] M. Richtel, "Live tracking of mobile phones prompts court fights on privacy," in *The New York Times*, 2005.

[15] A. Brandt, "Privacy watch: soon, your cell phone may be tracking you," in *PC World*, 2004.

[16] R. Whitaker, *The End of Privacy: How total surveillance is becoming a reality*. New York, New York: The New Press, 1999.

[17] B. Charny, "Cell phone tracking raises privacy issues," in *CNET News.com*, 2002, http://www.news.com/Cell-phone-tracking-raises-privacy-issues/2100-1033_3-846744.html

[18] S. C. Swales, J. E. Maloney, and J. O. Stevenson, "Locating mobile phones and the US wireless E-911 mandate," *Novel Methods of Location and Tracking of Cellular Mobiles*, pp. 2/1 - 2/6, 1999.

[19] D. Cvrcek et al., "A study on the value of location privacy," in *5th ACM workshop on Privacy in electronic society*, Virginia, 2006, pp. 109-118.

[20] J. Best, "Nokia: GPS will be in every phone," in *CNET Mobile Phones*, 2007, http://www.cnet.com.au/mobilephones/phones/0,239025953,339279768,00.htm

[21] D. Seifman, "'Track' Man is Sacked: GPS Nails Ed. Guy," in *New York Post*, 2007, http://www.nypost.com/seven/08312007/news/regionalnews/track_man_is_sacked.htm.

[22] J. Voorbees, "The Limits on Wireless Security: 802.11 in early 2002," in *SANS*, 2001, http://www.sans.org/reading_room/whitepapers/wireless/164.php.

[23] P. Wayner, "What's Next; Tracking down cell-phone users," *The New York Times*, 1999, http://query.nytimes.com/gst/fullpage.html?res=9A01E4D81631F93AA15754C0A96F958260.

[24] Q-Free, "Company History," 2007, http://www.q-free.com

[25] D. Loukakos and M. Benko, "Electronic Toll Collection," in *ITS Decision*, 2007, http://www.calccit.org/itsdecision/serv_and_tech/Electronic_toll_collection/electronic_toll_collection_summary.html

[26] SRI Consulting, "Electronic Toll Collection," in *ITS Canada*, 1996, http://www.infoworld.com/articles/hn/xml/00/10/25/001025hnezpass.html

[27] P. Blythe, "RFID for road tolling, road-use pricing and vehicle access control," in *IEE Colloquium on RFID Technology*, 1999, pp. 8/1-8/16.

[28] K. Waersted and K. Bogen, "No stop electronic toll payment systems," in *Second International Conference on Road Traffic Monitoring* 1989, 1989.

[29] Q-Free, "ETC Systems - White Paper," 2003, http://www.q-free.com

[30] C. Caldwell, "A Pass on Privacy?," in *The New York Times*, 2005, http://www.nytimes.com/2005/07/

17/magazine/17WWLN.html?ex=1279339200&en=c1f 10d3de06adea6&ei=5088

[31] T. Wright, "Eyes on the Road: Intelligent Transportation Systems and Your Privacy," in *Information and Privacy Commissioner/Ontario*, 1995, http://web.archive.org/web/20010910204521/http://www.ipc.on.ca/english/pubpres/papers/ITS-E.HTM#ITS

[32] E. Grygo, "New Jersey Turnpike electronic toll collection system hacked," in *InfoWorld*, 2000, http://www.infoworld.com/articles/hn/xml/00/10/25/001025hnezpass.html

[33] Anonymous, "E-ZPass Bypasses Your Privacy," 2007, http://www.digitaljournal.com/article/216089/E_ZPass_Bypasses_Your_Privacy

[34] B. Sullivan, "E-ZPass, Now with a higher price," in *The Red Tape Chronicles: MSNBC*, 2006, http://redtape.msnbc.com/2006/02/ezpass_now_with.html

[35] ETC Working Party, "Second Report to the ATC of the ETC Working Party," *Australian Transport Council* 2001.

[36] ICAO, "History - The League of Nations," in *Machine Readable Travel Documents*, 2006, http://mrtd.icao.int/content/view/21/194/

[37] ICAO, "MRTD Overview," in *Travel Documents*, 2006, http://mrtd.icao.int/content/view/18/199/

[38] Australia Government, "The Australian e-Passport," in *Department of Foreign Affairs and Trade*, 2007, http://www.dfat.gov.au/dept/passports/

[39] M. Meingast et al., "A case study of the security & privacy risks of the US e-Passport," *IEEE International Conference on RFID*, Texas, 2007, pp. 7-14.

[40] U.S. Department of State, "The U.S. Electronic Passport Frequently Asked Questions," *in Bureau of Consular Affairs*, 2007, http://travel.state.gov/passport/eppt/eppt_2788.html

[41] D. Lekkas and D. Gritzalis, "E-Passports as a means towards the first worldwide public key infrastructure," *Lecture Notes in Computer Science*, vol. 4582/2007, pp. 34-48, 2007.

[42] Home Office, "Why has the UK introduced biometrics in its passport?," in *Identity and Passport Service*, 2007, http://www.passport.gov.uk/general_biometrics_passports.asp

[43] R. J. Hays, "INS Passenger Accelerated Service Systems (INSPASS)," in *Biometric Consortium*, 1996, http://www.biometrics.org/REPORTS/INSPASS.htm

[44] U.S. Department of State, "The U.S. Electronic Passport," in *Bureau of Consular Affairs*, 2007, http://travel.state.gov/passport/eppt/eppt_2498.html

[45] Australia Customs Service, "SmartGate 2007, http://www.customs.gov.au/site/page.cfm?u=5555

[46] C. Edwards, "Borderlands of confusion [biometric passports]," *IEE Review*, vol. 51, pp. 34-37, 2005.

[47] B. Schneier, "The ID Chip You Don't want in Your Passport," in *The Washington Post*, 2006, p. 21, http://www.washingtonpost.com/

[48] T. Lupick, "E-Passports may unlock doors to your privacy," in *Straight.com*, 2006, http://www.straight.com/e-passports-may-unlock-doors-to-your-privacy

[49] A. Juels et al., "Security and privacy issues in e-Passports," in *International Conference on Security and Privacy for Emerging Areas in Communications*, Greece, 2005, pp. 74-88.

[50] A. Juels, "RFID Security and Privacy: a Research Survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 381-394, 2006.

[51] BBC, "Concern over biometric passports," in *BBC Technology*, 2004, http://news.bbc.co.uk/2/hi/technology/3582461.stm

[52] Anon, "RFID Tagging Isn't a Privacy Issue Unless You Make It One," *New Media Age*, vol. 16, 2006.

[53] Scarmig, "E-Passport: Doorway to the Panopticon," 2006, http://www.strike-the-root.com/62/scarmig/scarmig1.html

[54] K. Zetter, "Hackers clone e-Passports," in *Wired*, 2006, http://www.wired.com/science/discoveries/news/2006/08/71521?currentPage=1

[55] Paraben Corp, "Paraben's Passport Stronghold Bag," 2007, http://www.paraben-forensics.com/catalog/product_info.php?cPath=26&products_id=373

[56] C. Swedberg, "U.S. Tests E-Passports," in *RFID Journal*, 2004, http://www.rfidjournal.com/article/articleview/1218/1/1/

[57] O. Hinz et al., "Customer loyalty programs and privacy concerns," in *Merging and Emerging Technologies, Processes and Institutions*, Bled, 2007.

[58] R. Lacey and J. Z. Sneath, "Customer loyalty programs: are they fair to consumers?," *Journal of Consumer Marketing*, vol. 23, pp. 458-464, 2006.

[59] Anonymous, "Grocery store loyalty card use is strong despite privacy concerns," in *About.com: Coupons/Bargains*, 2007, http://couponing.about.com/od/groceryzone/a/loyalty_cards.htm

[60] M. Bosworth, "Loyalty cards: Reward or threat?," *Consumeraffairs.com*, 2005, http://www.consumeraffairs.com/news04/2005/loyalty_cards.html

[61] Y. Yi and H. Jeon, "Effects of loyalty programs on value perception, program loyalty, and brand loyalty," *Academy of Marketing Science*, vol. 31, p. 229, 2003.

[62] T. Graeff and S. Harmon, "Collecting and using personal data: consumers' awareness and concerns," *Journal of Consumer Marketing*, vol. 19, pp. 302-318, 2002.