Near Field Communications;
Privacy, Regulation & Business Models

A white paper of the LSE/Nokia research collaboration

Jonathan Liebenau, Silvia Elaluf-Calderwood,

Patrik Karrberg and Gus Hosein

Department of Management

London School of Economics and Political Science

The final version of this report including any addenda and/or updates can be downloaded from: http://www2.lse.ac.uk/management/research/initiatives/nokia-near-field-communications-and-privacy-study/home.aspx

October 2011

Abstract

The implications of extended and intensive use of near field communications (NFC) are far reaching for new business applications, for the delivery of public services such as transport, and for public policy. This technology is transformative for a large number of applications and has stimulated innumerable innovative forms, but so far there has been insufficient insight expressed in discussions about its impact and risks. The purpose of these studies is to assess the character and use of contactless payment technologies and the future of NFC with a focus on what are by far its most extensive applications in public transport. We use our evidence to structure a new understanding of the economic, business, legal and policy aspects of its anticipated widespread growth, especially as embodied in mobile devices.

NFC wireless technology allows information to be exchanged, via radio signals, between two NFC-enabled devices over short distances. To date the most extensively used form of payment is contactless travel card tickets. However, NFC is increasingly being used on mobile phones with an 'electronic wallet' function, which allows people to make payments and manage other forms of exchange.

The lack of insightful discussion of these far reaching effects brings significant risks. They include a new level of intensity of the pressure to undermine (or alter) principles and practices of safeguarding privacy. They raise concerns about the special status of children and other unwary users whose privacy might be compromised. They also intensify the concern we might have about breaches of data security or data loss, given the ability of NFC data to include location as well as payment information.

We review the regulations and policies governing NFC in Europe and Asia and the incentives and barriers to the commercial development of NFC. The use of contactless payment technologies in public transport ticketing schemes – such as the Oyster card in London and the Octopus card in Hong Kong provide case studies for the research. Our investigation is based on legal and business analyses, case studies and considerations of the changing functionalities of NFC. We have also interviewed numerous experts in regulation, policy and business about trends in investment and policy.

An overriding concern is that NFC will fail to achieve its potential. Until problems such as those

associated with privacy and regulations are overcome there will be insufficient progress on extending the business models in ways stakeholders such as public authorities, consumers and investors expect. Given the large scale of activities, any such delay would be extremely costly both in terms of investments and in terms of the expectations of this element of the ubiquitous digital infrastructure.

This report has eight sections. The first section covers the introduction to the research. Section two is a summary of the aspects to be taken into account for NFC and its application for public transport. Section 3 describes the theoretical foundations of the analysis. Section 4 focuses on the contentious issues emerging from NFC, privacy and business models. Section 5 discusses the implications of extending the NFC public transport experiences to other business cases. Section 6 presents our view on the future of NFC and its competitive environment. Section 7 addresses the key relationships that will determine NFC's future, and section 8 presents our conclusions and our views on policy implications. We also present our case about the implications for business models development. The document concludes with an appendix of cases studied.

1. Introduction

The rate and direction of the diffusion of near field communication (NFC) technologies and the very character of business applications will be deeply affected by privacy considerations. Hundreds of millions of people are familiar with payment and ticketing cards that use contactless techniques because of the expansion of public transport payment systems such as those in Hong Kong, Tokyo and London since the late 1990s. Each of the cities researched is currently operating –at different levels of development – some kind of NFC implementation plan. While the potential utility of these technologies is clear, the business models that are likely to succeed are going to rest on the extension of such systems. Herein we can see the shaping powers of the interactions among the technology, the commercial applications that take hold, their legal environment and the public policies that emerge.

Increasingly, every transaction a user makes, overtly or not, generates data. Even as concerns about privacy increase amongst consumers, most are unaware of how every action they take generates particular kinds of transactional information. Yet, users are keen to have more extensive services and equally demand that they remain in control over how consequent data are processed. With NFC, this seemingly contradictory situation is going to grow even more complicated as new services and the emergence of concerns of abuse will develop complementarily. If the risks of privacy abuse are not properly assessed at an early stage, NFC may suffer from the same levels of criticism that have damaged confidence in technologies such as biometrics and RFID. NFC commercial proponents have been trying to distinguish NFC from RFID, in part because of the heavy regulatory burden associated with RFID. This has to some degree obfuscated public discussion about NFC's potential uses. Yet in our discussions with regulators we found that they are inclined to regard NFC and RFID as the same types of technologies, and will likely regulate similarly.

NFC is a technology that traces its technical heritage to radio-frequency identification [RFID] that was first applied on a large scale to public transport in the late 1990s. It lends itself to various business models that integrate the social, legal and practical features of its functionality. Since 2004 when the industry body, the NFC Forum, was founded, it has attracted a great deal of investment focused on applications for business areas beyond public transport. Although there has been a spate of tentative

business models for mass applications, there is still a confusion of regulatory, legal and policy responses to the use of the technology.

Any transaction that involves the sharing of information additionally requires us to consider security implications. Any transaction that involves personal information requires us to consider privacy implications. In turn, when we are considering transactions such as payments, both privacy and security play essential roles and complement each other. In these ways the expansion of mobile payments has significant effects upon privacy for users and the sharing of data. These effects in turn have a strong impact upon the creation of new business models. Since the late 1990s the expansion of RFID and NFC cards used for public transport payments have made many ordinary people familiar with the use of these technologies. However, familiarity with a technology does not mean that the privacy and security issues have been resolved adequately.

The privacy regulations applied to electronic ticketing operations, in principle, fall under national data protection laws. It has become fashionable to complain that regulation is always behind innovation; but this has always been the case. This criticism could be applied to data protection law; though data protection law is the instantiation of a set of principles about how personal information is to be governed, and processed and are, for the most part, technology-neutral. What tends to be lacking is adequate awareness amongst regulators until they are called into action, if action is even within their remit. NFC poses a set of unique problems for understanding the implications for privacy, and in turn, privacy regulations. Despite that, NFC does not necessarily pose many radically new conditions. We can come to comprehend the privacy risks and opportunities based on prior experiences in other domains.

A major complication is that users rarely seek legal or regulatory remedies for perceived privacy infringements arising from new technologies. In turn, courts and regulators tend to be unaware of how new technologies function and understandably base their judgments on established precedents that often refer to technologies that no longer bear close resemblance to those in current use. It may take years, and sometimes decades for adequate legal responses to arising privacy cases. Users of new technologies need new abilities to comprehend their threats, just as the providers of new technologies need new methods to promote confidence in their techniques. The combination of that comprehension and the techniques and services that businesses and public bodies offer will be a determining factor in

the character and rate of the diffusion of NFC.

The maturity of the NFC technology and its embedding in mobile phones raises new opportunities for contactless payments. At the same time the creation of virtual wallets containing not only transport cards but also any other type of card, from credit cards to identity cards, loyalty cards, and bonus cards, etc. has stimulated the formation of many new business models. One implication of this technology is the pervasiveness of data collection about contactless payments. Data include the location and volume of transactions, as well as time and date. Many users do not sufficiently understand or have a full appreciation of what data are collected, where they are held and how they might be used in the future. Although there is a comprehensive legal framework aimed to protect the privacy of individuals, with some international variations, the application of this technology gives rise to new challenges and the legal ramifications are not yet well understood. These have contributed to an industry-wide sense of uncertainty about the future of the technology.

The resulting period of instability is likely to continue for a bit longer, during which time a common list of risks/problems/challenges will continue to arise. These include strategies (and also tactics) associated with business models to introduce mass applications of NFC and contractual agreements associated with working out how to distribute the risks and rewards.

Our research approach therefore includes engaging with experts, as they have experiences and perspectives that may assist in illuminating some of the risks. In essence, we learn from past experiences and hear their thoughts on future developments. Our goal is not to provide a comprehensive statement of risks, but rather to identify the key discourses, the technological options, and the tools available to developers that could promote confidence in new applications of NFC.

2. NFC and Public Transport

The cases of Oyster in the UK and Octopus in Hong Kong are examples of the successful implementation of contactless cards and they have stimulated applications in hundreds of other municipal transport systems. The Oyster case is significant in terms of how the card emerged as a brand, the problems that came from the use and abuse of the technology, and the later "openness" of transactions on London public transport. These will soon be extended to other types of contactless cards e.g. contactless credit cards and NFC mobile payments (a goal for the London Olympics of

2012). The Octopus card in Hong Kong, which was initiated in 1997/98, is a contrasting case as the Hong Kong authorities tried very hard from the start to create a brand and added value to the use of the card beyond its function as a transport ticket. It has also suffered from a number of well-publicised violations of prohibitions on privacy rules, which have influenced policy actions taken by regulators to tighten those rules.

2.1 Travel card technology systems

A key objective of new transport payment systems is to improve public transport service levels while satisfying passenger needs. A typical transport card system has the following three main components as shown in Figure 1:

1. An interoperable card: A passenger should need only one travel card through which it is possible to use the transportation system and its different modes in full.

2. A one-stop-shop: A passenger should be able to buy all necessary public transport tickets/tokens through one sales channel (online, over the counter, and/or at vending machines).

3. An interoperable reader: A single interoperable reader should be able to validate all forms of travel transactions, such as when entering and exiting the transport system.

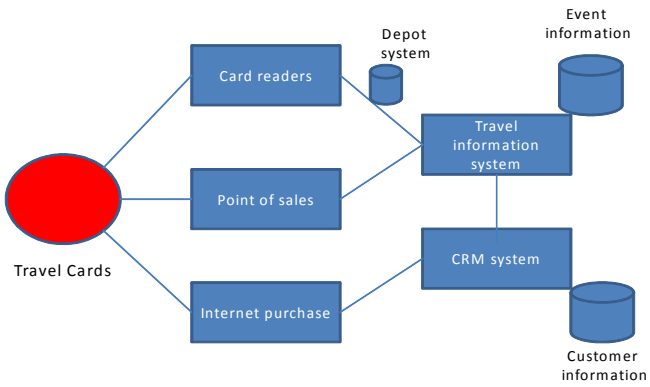

Figure 1.The simplest form of public transport travel card based payment systems can be divided into three parts: the travel card, service points, and the central system (adapted from Sulonen et al., 2010).

The travel card is a smart contactless card that transmits data over short distances. The card contains stored data including the travel currency and amount, transactional information, and a unique identifier. The current trip is stored in a card application that acts as a ticket. Typically millions or tens of millions of cards are issued in an urban or regional card scheme.

Card readers collect data stored on the travel card. A reader interacts with the travel card and communicates to the information handling system where that passenger starts and ends the current journey. With various levels of precision the card reader stores this information and in some cases interacts with the central system. Typically tens of thousands of card readers are installed. For buses, trams and the like, vehicle equipment details and sales information from card readers are transferred to the central system through mostly wireless telecom connections.

A centralised information clearing system is used where event data are collected and which manages the transport card system. It can be divided into two parts: event handling and client management. Event handling keeps track of current and future event information and processing, including error handling and recovery. Customer relationship management facilities deal with maintaining the registry, billing and reporting. The central clearing system contains essential databases storing transaction information and customer data. If the central clearing system is a shared system, several travel card systems can be connected to each other. Connection can be made directly to the central terminal in different systems, or events can be routed to the terminal's central system in batches via the depot.

2.2 The context of NFC in transport

The first transport system to implement contactless payment was in Hong Kong when it deployed its Octopus card system in 1998. Other early adopters include Japan Rail East, which initiated a contactless Felica card which was launched in November 2001 at train stations within 100 km of central Tokyo. Later on, a mobile phone NFC 'travel card' called Suica Mobile was launched in 2006 by NTT DoCoMo. Oyster was introduced in London in 2003, and since then there has been a significant reduction in individual paper tickets sold.[1]

[1] A change in fare differentials has further encouraged the take up of Oyster cards. Over the five years to the end of 2007, the total number of ticketing transactions on bus and Underground services

Now many industry analysts have called for national roll-out strategies in the West to achieve critical mass for contactless cards, particularly on mobile phones. They argue that the benefits of such a drive would include efficient transport ticketing and convenient ways for users to store numerous loyalty cards in their mobile phone, while being able to monitor the usage and benefits through a graphic user interface on smartphones. Starting in 2004 various initiatives were launched by handset makers, carriers and service providers to implement and pilot contactless on mobile devices, resulting in NFC interfaces now being included in most mobile operating systems.

Many stakeholders have run pilots experimenting with NFC adoption and usability. These applications range widely and different kinds of business models have been put in place. The Transport for London (TfL) authority, for instance, is responsible for the planning, implementation and revenue collection of the Oyster card system. This is different from the case of Hong Kong, where the Octopus card was an initiative of local transport operators led by the metro operator, MTR, which owns 57% of the shares (Chan and Foster, 2009). These pilots consider all "flavours" of contactless payment, which include transport-specific transactions (as with the Oyster card), more general types of payment systems (e.g. Octopus), and NFC enabled mobile services These have proved important for public transport operators to determine the possible shortcomings and improvements to the local NFC implementation.

NFC payment systems are often celebrated for offering benefits to public transport authorities, operators and passengers (Mezghani, 2008). These benefits are often expressed in terms of value creation for each of these main stakeholders.

Public authorities claim that there are benefits derived from the creation of seamless journeys in public transport networks, the unification of ticketing systems, new sources of marketing data, better control of revenues and subsidies, the ability to extend the scheme to other modes of transport (e.g. taxis), the reduced cost of selling tickets, and improving the image of public transport.

Operators value the direct benefits from the potential of gaining new customers with modern approaches to ticketing, the increase of medium term operating profit and reduction in fraud, reduction in the use of cash, reduced cost of selling tickets, reduced maintenance costs, improving cash flow, increased speed of boarding (e.g. on buses), valuable opportunities to add "new services", and new

---

combined has been reduced by nearly 60% (Transport for London, 2010).

sources of marketing data for public transport management.

When spoken for, it is often claimed that passengers benefit from convenience and speed, the removal of the need to carry cash for payments, apparently seamless journeys in multimodal, multiple public transport schemes, easier ways to reload value or renew passes (e.g. pay-as-you-go schemes), the ability to issue a new card easily when it has been lost or stolen, and additional integrated services that can be appreciated as they become available.

In 2008 and 2009, research reports funded by the European Commission on public transport and the implementation of ticketing systems proposed a series of recommendations for the operation of those systems (Mezghani, 2008; Elliot & Whitcombe, 2009)[2]. These reports were particularly concerned about establishing new concepts of fares, for example in determining the responsibility for setting prices and for fare structures, ticketing (pricing spectrum and fare integration), types of electronic or mobile scheme, type of technology, interoperability, and the exploitation of e-ticketing data (e.g. information related to operations, cards and journeys), plus the analysis of how to calibrate the broader impact of e-ticketing schemes in the European context.

In many European countries where there are multiple travel card systems already in place, there is often a temptation to replace current incompatible systems with a new single centralised system. Examples from Finland and the Netherlands national card schemes show how large information systems take a long time and many resources to launch. As a result, some advocate changes to make the existing systems interoperable (Sulonen et al., 2010). Newly constructed travel systems, especially in Asia, benefit from the opportunity to design-in these technologies from the outset.

A new problem then arises as we try to make fare systems interoperable: each component system is likely to be built quite differently[3]. Introducing interoperability in a system where there are different

---

[2] The EU has multiple programmes researching the use of RFID and NFC as part of its FP7 research programme. The projects cover a wide range of areas, and there have been many reports written on experiences in the use of the technology in public transport from different locations in Europe.

[3] London has a fully integrated fare system determined by TfL, however, it is not possible to use the Oyster card in any of the other big cities in England, such as Manchester or Birmingham. In the Finnish case, the fare system when escalated at national level has encountered many problems when trying to integrate it all using contactless payments. In the Netherlands, integration at national level using contactless cards has been completed successfully, although there was from the outset minimal problems for integration.

back-end systems, data models, and security frameworks is expensive and prone to flaws. To guarantee interoperability, all involved transport operators will have to develop clear business rules, detailed and descriptive rights and duties as well as roles and responsibilities, established distribution of revenues by agreement, and standards for security.

2.3 Stakeholders in public transport ticketing systems

As data are exchanged within these growing systems, it is important that we are aware of the key stakeholders who have access to information, what kind of information, and how they process that information. This is important not only for governing a system but also ensuring that the system is legally compliant, particularly when dealing with information about individuals.

Modern transport payment systems merge information about our movements, our locations, and our finances. Information is likely to be processed by a number of organisations. As we move to new NFC transport systems involving mobile devices, the number of stakeholders and agencies involved grows dramatically. In turn, these entities have legal obligations to protect personal information.

As a general case, these can be summarised as shown in Figure 2:

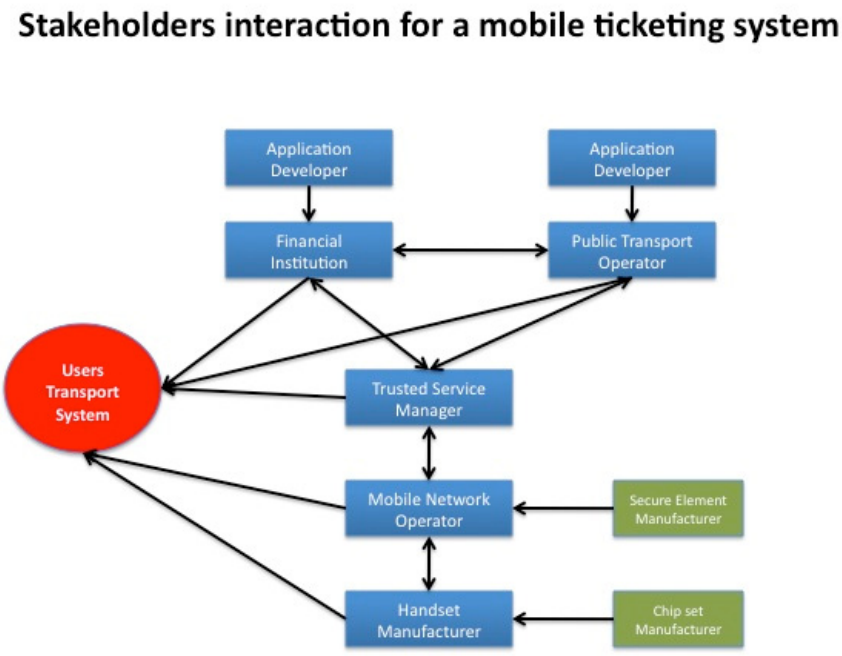

Figure 2. The roles of stakeholders and relationships in a generic mobile ticketing system

Public transport operators appear, in the eyes of users, to be responsible for the protection of consumers' rights while ensuring that they are able to use the transportation network. The transport operators tend to be interested primarily in ensuring that they satisfy their user base while minimising the risk of fraud. The public transport operators therefore verify tickets through a card reader, and this reader is enabled with privacy and security enhancements.

Financial institutions are expected to provide network security for financial transactions, together with privacy mechanism for personalised user data and to provide ease of use, access and user control. While public transport authorities usually have strict commercial limits to their remit, the commercial imperative is a foremost motive for the financial institutions involved.

Trusted service managers hold the role of assuring compliance in data handling. This function is very much promoted by telecom operators, and chip manufacturers as part of the fully integrated solution that provides privacy enhancement tools and services to public transport operators, while offering users an interface to manage personal information.

Mobile network operators, for NFC mobile ticketing, provide the communication network security over mobile internet and also ensure that other public transport operators comply with providing security against location tracking and preference threats.

Handset manufacturers provide NFC device security and are also responsible for mobile handset security against information leaks. Depending on the chosen technical implementation on the phones available for consumers use, an open debate on the level of security to be provided by such devices is required. This debate requires stakeholders to understand, how and when users are faced with the ways that services or apps exchange data from the handset with an external system such as the public transport authority. Those services or apps can be either downloadable, embedded, or residing in browsers.

2.4 Extending the stakeholders beyond transport

Seven features that affect dissemination of NFC emerge from the analysis of stakeholders in transport that can yield generalisations useful for the analysis of a wide range of applications. We describe these as power and authority challenges to stakeholders and to legislators, consumer responses, emerging business models, functional alternatives to NFC, conflicts that arise from powers to authenticate or verify users and mechanisms, and the prevailing logic that guides financial services organisations.

- The stakeholder challenge is at the heart of the commercialisation process and is expressed by who gets what share of profits; who encroaches on whose commercial/statutory territory; what old forms of associations/contracts exist and are likely to survive or what new forms are likely to emerge.

- The legislative challenges mediating among the technology, the privacy rights and the current and future regulation of business models:

    a. Regulations such as e-money/m-money directives

    b. Privacy law

    c. Rules and policies associated with jurisdictions (e.g. trade), subsidies (e.g. for broadband networks), competition (e.g. pricing; interconnection costs).

- The role of consumer behaviour taking into account consumer acceptance vis-a-vis privacy.

For example, interested parties will be comparing adoption rates internationally and how these vary depending on the application, such as whether the implementation is intended primarily for transport as opposed to small payments. Finally, the role of consumer groups' interests in monitoring and judging industry guidelines.

- New and/or idiosyncratic business models: in particular non-money payment related ones that offer opportunities to explore certain transaction and value issues aside from the "mainstream" financial and industry concerns. Examples of this include NFC for queuing, checking in services (as with restaurant reservations and flights) and close interpersonal contact for the purpose of data exchange. All this together has implications for e-wallets and any other future fully integrated contact services using financial information from customers.

- Alternative non-NFC based service solutions, to which NFC was promoted as a main solution provider (e.g. biometrics; SMS codes; barcodes, etc).

- Authentication: There are a variety of potential ways to structure authentication that pit SIM cards against phone embedded authentication mechanisms, versus network or cloud-based procedures, versus some combination of mechanisms and procedures. SIM cards may be too slow at the moment for fast throughput in the transport system gates such as those used on the London Tube. However, an embedded NFC in the device could be combined with closed system authentication, open standard with a proprietary certification authority, or other combinations. Additionally, NFC authentication implementations can increase their utility by taking into account if the system will accept multiple identities, unique identities, or multi-purpose identity.

- Costs: Some transport operators such as TfL are more concern on relinquishing the control of transactions to financial institutions such as credit card issuers. The logic behind this is to reduce the back end costs for public transport operators[4]. Marginal costs provide insufficient incentives for TfL to deal with the costs of issuing additional charge or contactless cards. This approach is very different from the Hong Kong case, were Octopus acts as a financial

[4] TFL plans to cut 4% of costs by shutting down Oyster as its functions are integrated into other NFC devices

institution aimed to provide not only fare collection but all the other services those organisations can provide.

By generalising the roles of stakeholders we can better understand possible configurations and alternative structures and relationships. It is also likely that each stakeholder has an interest that will be expressed both technologically, in terms of design, and as relations in service delivery or the conduct of business.

3. Transport Insights

To understand better the context of NFC for public transport ticketing, we have conducted in-depth studies into the use of NFC in public transportation systems in six cities: primary case studies of London, Hong Kong, Helsinki and Tokyo, with supplementary insights on Berlin and Seoul. Our study has focused on the interrelatedness of businesses, the associated technologies and the trends towards comprehensive electronic payment systems as well as other applications of NFC for improving procedures.[5] We address the four interrelated components of NFC within transport systems:

- The business models for implementing NFC and their economic foundations.
- The differences among the architecture and technologies.
- The regulatory regimes affecting both transport operations and consumer rights.
- The arising privacy challenges.

[5] We have not ventured into the behavioural dimensions of NFC use, although they hold implications for our findings and we believe that such research is needed.

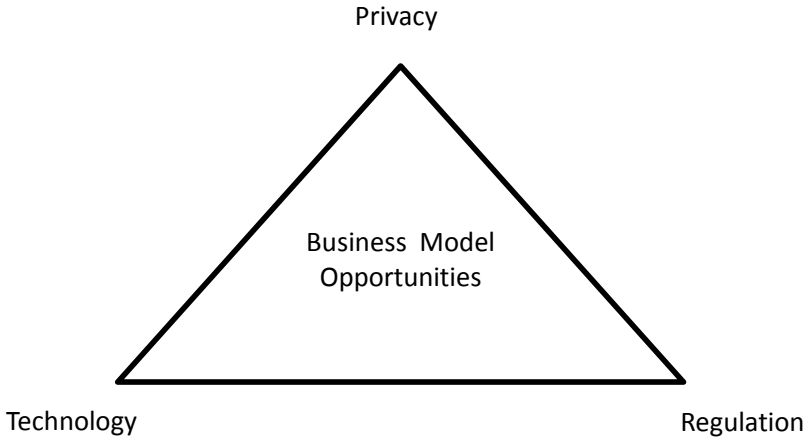

Figure 3: Key components of the analysis

The business model opportunities provided by NFC are central to our study. We study these opportunities by looking at the interactions among the technology, regulations, and privacy.

The case studies were selected in the first instance by taking into account the early adoption and success of implementing contactless cards in public transport. The transport systems are long established and have confronted (or are currently confronting) changes in stakeholder interrelationships and public acceptability. Many of these systems are also growing and changing as they interact with non-transport related business models.

While we investigated these cases, we focused our attention in particular on the arising information systems and, in turn, the privacy risks. This was often seen in the form of conflicts between traditional business models and users' preferences, such as the unwillingness of users to have personal data transferred from network operators to other commercial enterprises for marketing purposes. The following sections of this report are structured around a referential theoretical framework linking the three elements of the core research to the method of analysis as described in Figure 3.

3.1 Privacy

Consumers are concerned about how their personal information is being used without their knowledge or consent and increasingly fear that protections are failing them.[6] Unless users are informed about how

[6] For example, the 2008 Flash Eurobarometer on Data Protection in the European Union capturing 'Citizens' perceptions' found high levels of concern across the EU, available at

their information is used they will be unaware of the true nature of the risks of misuse and abuse.

Traditionally, organisations informed users about what they do with their personal information, and this allowed users to identify problems. For instance, in banking and credit transactions this comes in the form of monthly statements that account for how funds are used. Users are informed about whom they have been interacting with on a reporting basis. This after-the-fact reporting is usually complemented with consent at the point of transaction: users authorise payments, make telephone calls, and actively participate in initiating a transaction. Somewhere along the way there is supposed to be regulatory and legal mechanisms that protect the individual and ensure that the organisation complies with basic rules.

In an online environment some of these interactions are harder to identify; clicks may lead to purchases that result in credit card transactions, the individual then receives some notification about the transaction in the form of receipts, acknowledgements, and monthly statements. Nonetheless in both these environments questions of consent still arise: how do we properly inform consumers about what is being done with their information and how do we garner their approval? Regulators, consumers, and industry are consequently engaged in intense debates about 'opt-in', where consumers must be expected actively to consent to information processing, versus 'opt-out', where individuals' personal information is used until the individual contests the practice. There are also potential disputes about which organisation is actually responsible for adhering to which privacy rules, particularly across contractual relations and borders.

In the contactless and NFC transaction worlds these challenges are likely to grow. Public transport systems may indicate to consumers that they are conducting a transaction by allowing entry-gates to open, or merely a sound acknowledging that the contactless card has been read. The introduction of NFC in transport systems allows for the greater collection of personal information that the individual may not be aware of through the use of audit logs. Transport authorities may know where an individual entered a transportation system, the time of day, and when the individual left. Analysing the data sets over time could allow those with access to the data to derive biographical information, even travelling partners, and anomalies. Consumers are expected to trust that the system will not wrongly charge them, or charge them without their knowledge and consent; and that no one is mining the data.

---

http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf

As NFC expands to mobile devices, new opportunities arise. . Mobile phones have interfaces that may permit individuals to keep track of transactions to ensure that there has been no abuse or fraudulent activity. Users may become more aware of how much information is collected because they can see the audit logs, and perhaps see exactly what information is being disclosed and how it is being processed. Equally, however, the expansion to mobile devices can increase the risks as new stakeholders join in on the processing of personal information. Unless regulated by agreements, technology, and possibly law, banks and mobile phone network providers, or even handset and applications developers may gain access to travel histories and track individuals' movements. Using these services may generate new kinds of personal information, allowing new ways to profile individuals, while making governance of the information systems more difficult.

The shift from contactless cards towards NFC payment systems is occurring at a time when consumers are being given new and stronger privacy rights. Privacy laws are proliferating as more countries introduce data protection laws that govern the use of personal information by both the public and private sectors. Constitutions and human rights protections provide the foundations for these laws to ensure that individuals are not recognised merely as consumers, but also as citizens. In some jurisdictions, such as within the European Union where the Council of Europe's European Convention on Human Rights and the European Union Directive on Data Protection both apply, consumers are endowed with fundamental rights that protect them from surveillance by both public and private actors.

The task then becomes one of finding ways to ensure that new implementations of systems and services are compatible with privacy rights. This resolution is not necessarily easy and settlements are not uncontested. Just as the online behavioural tracking industry has clashed with privacy regulators around the world about whether their tracking of internet users comply with privacy laws, we are now seeing conflicts emerging about privacy and mobile devices. For instance, when news emerged of some mobile devices collecting location data, this gave rise to a variety of actions including a U.S. congressional hearing, regulatory queries and assessment (in Canada and Europe), and even court action (in California and South Korea).

NFC has yet to encounter this level of scrutiny, possibly because very little is commonly known about how information is shared among services and providers. The current conventional wisdom is that firms that do not turn their attention to privacy needs will alienate customers. How this applies to NFC

remains to be seen particularly as implementations move beyond transport systems. The unique character of transport systems as critical public services limits discussions about choice (opt-in and opt-out, for instance), but as NFC proliferates into more consumer-oriented domains, companies may be obliged to earn the trust of consumers through greater protections.

The long-term trends in corporate information security, which could be extended to corporations serving users on the mobile internet, can be described as rising risks of data breaches and changes in boundaries. Reputational risk arises from breaches; reports of breaches of personal data are compulsory in several jurisdictions, with the result that businesses are becoming acutely aware of those risks. High profile malicious hacks have brought negative attention to companies that have since acted to enhance protections. Simultaneously, changing boundaries and duty of care arise; users engage with a wide array of mobile services and have levels of security far below those applied within financial institutions or telecom carriers. As mobile services extend into commerce and payments then all stakeholders will have significantly to increase their levels of security.

Security breaches involving customer data imply privacy breaches with potential implications for corporate profitability. An analyst from the European Network and Information Security Agency concludes:

> Failure to implement appropriate information security measures might have severe consequences for the implicated organisation. Under privacy law, failure to implement security measures might result in damages for breach of contractual obligations (e.g. negligence or breach of a fiduciary relationship). The increasing statutory obligations that have been introduced through laws on banking, data protection and healthcare are an additional source of security requirements. Security has become an issue of concern for shareholders and management that affects the positioning towards corporate liability. (Mitrakas, 2006)

Interactions such as ‘opting in’ as opposed to ‘opting out’ are embodied in procedures and structured relationships between users and vendors and can come to characterise a vendor’s respect for the autonomy of a customer. This leads to preferences that affect business models in relation to the ways in which customers are willing to engage in interactions, influenced by their attitudes towards the use of personal data. The mechanisms we use embody these functionalities, for example offering levels of

security, providing back up or controls over the operations of mobile devices.

Some national legislatures and responsible companies have implemented privacy elements central to the character of NFC, such as the preference to 'opt in'. However, other elements create conflicts between traditional business models and users' preferences, such as the unwillingness of users to have personal data transferred from network operators to other parties (including companies or government agencies), or when interactions leave a data trail.

As applications converge, the problem arises as to if, when, where, how and why identifiers are used: which services and providers will have access to which identifiers, and how can protections and safeguards be designed into the technologies? The use of unique identifiers has long caused consternation in public policy debates, and more recently in controversies over how mobile phones and operating systems use and share identifiers with applications and third parties. Unless properly considered and designed accordingly, NFC can combine and amplify these perceived concerns as individuals can be identified uniquely as they conduct their daily lives in an unprecedented manner.

While privacy awareness is at an all-time high, we see an increasing diversity of privacy understandings occurring as technological capabilities widen. As many companies have experienced, different user groups respond differently to user education, empowerment initiatives and control settings, user interfaces, and privacy policies. The deployment of ubiquitous services and products enabled by NFC, particularly when applied to vast infrastructures such as transportation, would have to cater simultaneously to all these user groups and populations.

Stakeholders cannot focus only on risks and threats. That is, we cannot become overly concerned by the need to mitigate risk and worry about when the privacy axe will fall on a poorly-prepared stakeholder. Indeed, there are great opportunities in this domain where users can be empowered through advanced techniques to maintain their privacy in new ways. Just as the OECD noted with its work on identity management,[7] while there are opportunities for the better use of resources, overcoming barriers to growth and fostering innovation, facilitating global services, improving user convenience, the OECD also noted that when properly designed and implemented, security and privacy

[7] OECD (2009), "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers", OECD Digital Economy Papers, No. 160, OECD Publishing. http://dx.doi.org/10.1787/222134375767

can be enhanced through new methods. These opportunities should be identified and these services and products must be amongst the first deployed so that users can see how they meet their own interests and not merely the needs of the service providers, application developers, or third-party aggregators.

3.2 Technology

The most pervasive aspect of the implementation of NFC technology is its current integration with mobile devices. Mobile devices offer opportunities to collect and generate large amounts of significant, potentially commercially valuable, and highly detailed and possibly intrusive personal information. Some guidelines about how these datasets can be collected and should be handled have already become influential, but new opportunities are constantly being created. NFC use may create problems that merit extensive further investigation.

The storage and handling of data are affected by the increasing use of outsourcing, virtualization and cloud computing. It could be argued that mobile services have been delivered in a "cloud" way since the early days of the mobile internet. Extensive coordination of data among several parties has contributed to the ability to deliver digital contents to multiple devices with varied screen sizes and capabilities. However, as content delivery is not only carried out within walled gardens controlled and verified by one firm but increasingly in a market of multiple service providers, the user can no longer be sure of where or how user data are being collected or used. This poses a reputational risk for service providers, as users could become reluctant to use new services due to privacy concerns, or draw negative conclusions regarding service providers because of problems arising from interactions with third parties. Non-trusted service environments could be expected to inhibit business models as users become hesitant to engage, which could affect economies of scale and create isolated "service silos".

Even as the risk of privacy increases because of the multi-purpose nature of many NFC applications, NFC-enabled mobile phones offer defences not generally available with traditional systems like credit or loyalty cards. With interfaces and processing power, it is possible for mobile NFC applications to use visualisations, application locks, passcodes, and even biometric tools to govern consent and transactions. Some device makers already offer remote functions where the phone can be locked and wiped clean of its content, certainly not a feature a lost or stolen wallet can provide. It could therefore be argued that using an NFC enabled mobile phone provides some opportunities for greater security

than merely swiping a credit card. The mobile phone also offers alternative and innovative ways of protecting the identity of users through minimising the flows of personal information using both inventive user-interfaces and cryptographic services. This could be applied to the design of NFC systems now and would be appreciated by many consumers.[8] The worse alternative is to wait for a controversy and campaigns to force developers to consider security and privacy, and to then compel a change in user behaviour after they have already grown accustomed to more insecure methods.

3.3 Regulation

In a perfectly legally compliant world, both public and private sector organisations would identify the privacy and security problems in advance of the launch of a new system or service. They would question how their new product and service is compliant with existing laws, and make changes as required. Respecting privacy is more complicated than merely assessing legal compliance. Despite the way that laws and regulations tend to follow well behind technology, the citizen's right to privacy and the citizen's expectation of privacy are often articulated in effectively technology-neutral principles, constitutions, and human rights conventions.

In addition to being a human right, privacy is also subjective and contextual. It is often difficult to tell in advance exactly what component of a service will give rise to privacy concerns, and in turn, generate negative attention. To deal with both of these challenges, in-depth privacy impact assessments (PIAs) are used, that include engagement with key stakeholders and external experts to help identify previously unforeseen risks. As with recent cases involving new social networking applications, even where external reviews were incorporated prior to launch, business critical problems emerged. It may be impossible to identify all the privacy risks in advance because of the complicated nature of this domain. For this reason PIAs focus on communicating how, while designing a new service or technology, an organisation comprehensively managed its responsibility to limit the processing of personal information, and then stating how the organisation identified any arising risks and explained how they are further mitigated.

When regulatory enforcement finally catches up, the regulators and the judicial bodies will be looking to see how much effort went into being careful with the processing of personal information.

[8] Brands, Stefan (2000). Rethinking Public Key Infrastructures and Digital Certificates', MIT Press.

Arguments about changing social norms will not resonate strongly with bodies that are responsible for enforcing laws; while evidence displaying how privacy was designed into a system will likely be persuasive.

3.4 Business Models

The convergence of digital services still provides significant market opportunities to communications firms (Karrberg and Liebenau, 2006; Elaluf-Calderwood et al., 2011). That is, what we are seeing now is the result of recombining components of separate industries into a new value chain, where a new level of interdependence is created, acting as an opposing force against user control by enhancing specifiability, verifiability, and predictability. However, in order to establish interoperable standards, modular interfaces among technology components must be developed, which is also a prerequisite for firms to support integration among partners and suppliers.

As mutual dependencies exist among markets, profit optimisation would strike a balance between the number of users and prices, where one side could subsidise the other. Take the example of a mobile site portal: the platform owner has to balance, amongst many things, having an attractive price for users while maintaining an attractive revenue share for content providers. One way of doing this is to devise an exchange regime where users' personal information becomes a source of revenue in itself. It is sensible to think that consumers would like to control such payments with their own data, as services do not come for free. Cross-subsidies usually consist of fees only, but now we can see the emergence of a more varied exchange regime that also covers time, as priced by advertisement agencies, and the price that actors need to set on user data. In a functioning market contracts for service exchange need to reflect both the simplicity of the technology use and the intricacy of the regulation framing the provision of the services.

The future of NFC seems to be linked to the creation of a system that feeds well into the needs of consumers, the use of the technology and regulatory compliance. Hence the components of our model can be transposed from the case study of public transport to other business areas such as retailing, media services, logistics and social enterprises.

4. Contentious issues

NFC and contactless-enabled transport ticketing systems allow for the vast collection and sharing of information. From the point of view of the contactless card-carrying passenger, it is not clear what information is involved, who is holding the information, and how they are using it. As business models change and new ones emerge, we need to be able to understand the implications for privacy.

4.1 Transport cards

Transport for London was quick to advertise that one of the benefits of the Oyster scheme was that individuals could see online the most recent transaction history, if they chose to register to do so. This data-rich functionality complemented features such as automatic topping up of the card when the balance became depleted, and disabling and replacing the card in the event of its loss or theft. In recognition of sensitivities about the extent of the information accumulated they agreed to minimise the data retention of the transaction logs held on their server to eight weeks. Although this is arguably a long period of time, this policy was established before the advent contactless cards and later NFC systems when such databases were perceived as essential elements for fraud detection and error management. Now with NFC, processing on the device could allow for a reduction in retention periods. TfL also released an anonymous pay as you go (PAYG) option that does not require individual identification in order to obtain a card, and credit can be added by using either cash, debit, or credit. Though this option was only launched at a later stage, this pay as you go card is highly popular, possibly to some degree because of the consumer perceived higher degree of privacy afforded.

There is a more confusing array of contentious functionalities associated with expanding our considerations to financial services. Financial services are often required to monitor transactions in order to detect fraud, and this tends to result in the greater collection of personal information and the extension of the period of retention of audit data. The logging of travel journeys is very different from the logging of financial transactions, and so a separate data store may be required and different rules may be applied to processing, data retention, access, etc. When payment systems are central to the process it is practically inevitable that law enforcement agencies as well as businesses will pay attention to how money laundering may be enabled and disabled. Criminals may take advantage of unregulated or insecure systems, followed by disputes that will need to be resolved about how centralised systems will ensure individuals against loss or abuse or wide-scale fraud and surveillance.

As business models and technologies change, processing of personal information may become more pervasive. A transport system that does not require identity will clash, on privacy grounds at least, with the financial world that is increasingly identity-intensive. Even if a travel card can be purchased anonymously (using cash), when a payment credential is used for topping up the account great care is required to ensure against de-anonymisation. That is, if the natural state is currently 'anonymity' because it is just easier to manage the disbursement of cards, maintaining that anonymity requires great care and clear intention when other identifiers come into play. Anonymity is quickly lost. It is possible that if an individual used a credit card to purchase the anonymous card, then an identifier can be linked. Or at a later time if an individual uses a debit or credit card to add funds to the card, it is possible that the unique ID of the card is bound to the identifiers of the payment methods. This is by no means inevitable particularly as obtaining information from banks is not a trivial exercise. However, even the aggregation of non-identified information can become identifiable as activity on the account can become an identifier in itself; it is easily possible that travel habits and movements, once analysed sufficiently, could allow for unique traits to be discerned.

Bringing together payment and transport systems may yet result in conflicting consumer demands. As with banking, consumers may become more interested in gaining access to transactional logs to see how funds have been expended. Credit cards and bank account logs are familiar to individuals and so enhanced transparency may be required as NFC applications move beyond just transport. Ensuring that this can be done on a pay as you go basis, without relying on identity, may prove challenging to other legal regimes. This does not necessarily become easier as users willingly register personal information for accounts. Privacy requirements apply even as 'anonymity' is willingly removed and individuals merge financial, registration, and travel information. How the back-offices deal with this is just as important as how e-wallets may eventually be designed.

As governments seek to register individuals' SIM cards as though they were bank accounts or passports, and the mobile devices are linked with payment systems with their own identifiers, the best-case scenario may be that there will be mayhem of identifiers, combined with regulatory conflict. For instance, the sharing of information across institutions, from TfL to other transport networks, or to other institutions in the case of a payment system, requires re-analysis. The use of a single persistent identifier would be highly problematic, as it will allow for the profiling of customers at various points

of sale and may increase the likelihood of fraud, particularly if this 'identifier' is also a payment card number. While credit card companies have detailed security standards for vendors, travel card systems may need to build some of these protections into their more processing-capable technologies. A multiplicity of identifiers, with the lack of an identifier by default, that are directed and unlinked is not only the privacy ideal, it is a representation of the fragmented world we live in. Convergence is a threat in itself.

The case of Hong Kong also provides insights into these issues. The types of personal information collected by the Octopus card include name, contact details, identification type and number, age and date of birth, card number and card usage data. (Octopus, 2010) Octopus' personal data policy is very loose in defining the terms of how this information can be used. For example it lists, as possible uses of the data, actions such as:

> Processing an application for one of our services; the normal management, operation and maintenance of the Octopus payment system, including audit; designing new or improving existing services provided by Octopus, its subsidiaries and its affiliates (that is, any other entity which directly or indirectly controls Octopus, is controlled by Octopus, or is under common control with Octopus) for customers' use; marketing of goods and/or services by us, Octopus subsidiaries, affiliates or any of Octopus selected business partners.

Defined in this way there is a wide-ranging remit. Octopus cards can also be linked to the user's credit card, which potentially permits another organisation to collect information.[9] This wide remit was the cause of controversy when in October 2010 Octopus confirmed that it earned about 44 million Hong Kong dollars (US$5.7 million) over four-and-a-half years from the sale of personal information with six companies for marketing purposes. Until then, the private company denied any such processing took place.

The use of Octopus continues to expand to new services such as in employment, education, small financial and personal transactions, and even entering residences. As this expansion occurs it is essential to know what happens with the identifying and transactional information. That is, if Octopus is used for transacting with a third party, what information does that third party get? Does the shop,

---

[9] http://www.readwriteweb.com/archives/hong_kongs_octopus_card.php

employer, school etc. get the name and other information, a unique ID of the card, and/or other payment information?

In the case of Helsinki, the use of travel cards is recorded in a database. This information can be accessed to aid transport capacity planning, where the main intention is to aggregate statistics regarding the volumes of people on various journeys. Nevertheless, the movements of individual travel card users are saved and can be retrieved later for other purposes. For example, the information from the transport system has been used for crime investigations in serious cases. Simultaneously, Finnish citizens have the right of data protection, in that organisations must protect the information they collect and grant individuals right of access to their personal information. Already the Privacy Commissioner of Finland has intervened in other transportation data collection systems, and so future development of NFC must incorporate privacy as a design feature.

4.2 The marketplace beyond transport cards

Now that mobile phone manufacturers are mass-producing a wide range of NFC enabled phones, we are likely to see the introduction of even more stakeholders and new business models. Three aspects of the marketplace allow us to identify differences in emerging business models. We identify these as regulation, innovation, and privacy.

Regulation: Institutional influence on stakeholders and technology exist in at least three forms: commercial platforms (competition), industry standards (standardisation), and direct regulatory intervention (legislation). Taking the domain of NFC for transport as an example, we have seen how card technology manufacturers influence usage experiences and data collection methods. Mobile phone manufacturers and software vendors also facilitate development of interfaces for NFC usage. Technology and business innovation tend to precede the regulator and industry standardisation forums. Forum and industry standard activities have been slower to establish commercial critical mass for their specifications as they have been focusing on so-called “secure parts” either in phone SIM cards or in the hardware of mobile devices.

Innovation: Proprietary platforms are often developed by one firm which can be radical and disruptive to established business models. Industry standardisation efforts are slower and tend to favour incremental innovation of current services taking all stakeholders in the forum into account. The rapid

roll-out of some proprietary solutions demonstrates the potential speed of innovation in contrast to the effort to establish a widespread industry standard, a process in which each stakeholder vies for dominance. New platforms, potentially disruptive compared to existing standards, create choices for firms to choose the new technology or wait for emerging consensus around industry standards. In the NFC business system, secure part manufacturers have strived towards creating control points around their own technology whereas others have developed their NFC platform related to their own operating system by themselves, benefitting from lower coordination costs[10].

Privacy control: It is possible to innovate on privacy with the careful handling of a diversity of identifiers. Competing models could allow users to choose what information is disclosed and how it is used, but no dominant designs have emerged so far. Authentication could be done on devices, the SIM card, or in the network. A "secure part" solution is attractive to banks and financial services because it appears to be compatible with familiar banking practices. A disruptive player may provide both open and closed NFC services, allowing a diverse system with multiple relationships of security to coexist (Clark 2011). It is also possible to enable transactions where no personal information is shared and policies and technologies are designed so that no transactional information is generated. Any claim that information is not shared would have to be auditable through technological, expert, and regulatory review.

The case for open devices is supported by the strength of having a set of multiple mobile platform access points with potentially one protocol for exchanging communication and a relative simple and direct way to enhance and implement levels of security. Furthermore, the lack of a strong link to bank accounts make it accessible by consumers who otherwise would have been excluded from using certain services (e.g. no age limit in NFC applications in the Rovio game "Angry Birds", allowing the purchase of units of trade). The case for secure devices, strongly backed by the chip manufacturing industry relies on a foundation for the development of customisation by mobile platform and type of service, traceable and identifiable links to a unique user identity which will be verified on each transaction, and the provision of hardware or software embedded encryption and authentication mechanisms.

---

10 Point of view expressed by role key players subjects interviewed for this study

There is a migration from bespoke ticketing technology to "media neutral" payment applications (e.g. bank card, mobile payment, credit card). This is partly driven by the desire to embrace the payments industry – due to security and privacy issues and regulatory compliance – and not just by the need to use bespoke transit solutions.

In London the identification of problems related to the system is complicated by the lack of standardisation, and the lack of a clear driver for expansion, mainly a stronger relationship between TfL and associated vendors and operators. The Octopus experience is different, driven by a goal of maximum interoperability beyond contactless payments, including open deals with applications and services providers, and operators; the number of stakeholders involved has not been a deterrent to the expansion of the card (Ma et al., 2008).

Octopus expansion drivers have carefully kept control over the tussles between the demands of consumers and the supply of services, and have successfully managed to provide a good balance between the perceived added consumer value: fast passage through gates, ability to buy and top-up tickets in advance, to view balances, manage tickets via handset or similar mobile devices, and develop Octopus as a main cash replacement. Octopus is also able actively to use its stakeholder status with the regulating authority to block the entrance of EMV/credit card providers to compete with a combined Octopus and credit card. So there is a conflict of interest when a public authority (MTR/Octopus International) is regulating its potential partners; it challenges the basic principles of an efficient network market.[11].

Although the future for NFC is drifting towards its use on mobile phones either as embedded software and/or hardware, other stakeholders such as newer payment services and even location-based social networking services present new competitive business models to deal with NFC, some systems will be able to liaise better with the challenges of integration than others. It is still open to discussion how NFC will deal with customer's loyalty or rewards. Some major stakeholders in m-payments seem to have taken a cautious approach to NFC; others are taking a more innovative approach by creating some kind of loyalty structure that is quite loose and adaptable to the needs of vendors.

In Japan there is a well-established regime on these type of "exchanges". For example, Sony's Edy

[11] Economides, 2003

enables users to cash in loyalty points from contactless tickets (such as Japan Railways (JR) tickets, ANA flight tickets and McDonalds coupons) directly into electronic money through an "exchange rate" offered by the service provider. Customers can buy JR tickets and get 2% cash back when they buy business tickets and 1% cash back on economy tickets. JR compensates Sony and Edy in a separate transaction when users cash in their JR loyalty points as electronic cash in convenience stores at tens of thousands of service points across Japan.

We must go further in questioning the role of the institutions that govern how the various profiles are managed: this could be the device manufacturer, the software designer, or some other entity providing the back-office operations. When and how do these institutions combine user information and accounts? Some of the convergence is perhaps necessary for the provision of the additional services, but some of it may be ascribed to exploiting technical positions within the architecture to become a nerve centre for all these transactions. Have all the options been considered, including the securing of anonymity, or ensuring transactions disclose minimal information?

Concurrent with the marketing of the first mass-produced NFC enabled mobile phones, two lines of thought are emerging from the debate on NFC secure implementation. One of these two lines is to increase the security features of NFC into the SIM card. This is strongly supported by the manufacturers of the cards and mobile operators. Their reasoning is that by using this type of hardware security, it is easier to comply with regulations and provide a secure service to customers. The other line of thought is to have a combination of secure and unsecure elements on NFC, allowing the expansion of the system based on relevant "killer" services and applications. One example of this is the release of the very popular Angry Birds game with the support of Nokia, where there is no need to use the secure element to conduct peer to peer data transactions to provide entertainment to the users of the mobile phone.

In our transport studies, the case of Oyster for London can be considered a closed system where there are limited opportunities to provide services within the system; Transport for London has not shown any strong interest in developing the Oyster card for acceptance outside its network. It has devised an alternative approach by bringing Visa, and other card provides, into its network. This is driven by the need to find external funding to upgrade their IT network.

In the case of Octopus, from the start of its implementation and due to the mixed composition of the

companies providing the services, there has been this drive to have an open market for business models, with a low entry demand, allowing small and large merchants to accept the card, providing a nurturing environment for the expansion of the card payment system.

In Japan, Felica Networks started as a joint venture with three revenue streams: mobile operators and handset manufacturers, users, and application providers.[12] Felica Networks has managed to establish a national standard where all mobile operators use the same mobile electronic wallet licensed by Felica Networks and interoperable with all other contactless Felica schemes in the country (Sony's Edy, Seven Eleven's Wanaco, and several others). They operate a "p-mark" privacy certification system under the umbrella of the Ministry of Internal Affairs and Communications requiring the registration and compliance of any stakeholders dealing with personal information.

In contrast, Hong Kong's Octopus is not integrated into any mobile wallets. Sources within MTR also recognise the challenges posed by coordinating six mobile operators, numerous mobile phone manufacturers and potential other stakeholders around the same table to sort out technical standards and commercial agreements.

5. The transport case and other business cases for NFC

In our transport cases, contactless technologies have been implemented amongst others for reasons of economic efficiencies, operational efficiency, and user convenience. In Hong Kong and Japan, travel cards (Octopus and Suica respectively) have emerged as alternative methods of payments, so-called "e-money". In the case of Japan such e-money cards have been integrated into a national standard for mobile wallets, accepted by all mobile telecom operators.

The combination of contactless technologies such as NFC with mobile phones provides the benefit a graphic interface from which users can monitor details of their ticket and the remaining balance. In the case of Japan Rail (JR), the mobile e-wallet can also be used for complementary services such as "on-train" purchases of food and beverages and a loyalty card programme. In this case the mobile wallet allows for access to specific data on the chip when it has the right keys, i.e. it can access and display information regarding the rail 'card' but also a payment 'card' and loyalty 'card'. As the scheme is

[12] Further details on the licensing fee can be found in the correspondent appendix on the Tokyo case.

accepted in all shops across the country, JR loyalty points could be exchanged for purchases with its commercial partners in real-time (such as electronics retailer BicCamera). Japanese airline operator, ANA, operates a similar ticketing and loyalty card scheme for air travel. The contactless token economy in Japan took a step forward when McDonald's introduced a mobile wallet discount coupon system in 2011. Multiple NFC cards can be connected to a user's mobile phone, enabling a wallet with multiple cards. Several of the mobile contactless systems in Japan allow users to connect a credit card for convenient and automatic top-ups and post-payment.

JR is a listed company and its non-transportation business has grown the past few years, assisted by mobile wallet payments, while the growth of its core business, transport, has been flat (Okajima 2008). As a leading executive in JR expresses it (Okajima, 2008): "Some day, people would be calling JR East an information service company. None of us could even imagine it would happen before the advent of Suica."

In this case of additional services and accounts being credited with points, this is all being conducted in the back-office of the emerging 'information service' company. Vast amounts of information are being brought together and managed by a single entity. This is not much different from how it is currently managed today. Rather, it just introduces new market entrants into that position as single-overseer of a large information system. An important potentiality for NFC and e-wallets is where these transactions and the necessary auditing can be conducted on the device. Such a design could radically reform the direction of business models, and would have significant implications for privacy, security, and even fraud-prevention.

The use of NFC outside of public transport is already under development and traditional companies are seeking to use their growing information resources to join new markets. However, prior success does not mean that we will necessarily see NFC applied in a widespread way into a multi-purpose and multi-level platform. Although contactless cards have been successfully implemented for granting access to public transport networks in major cities, the high levels of adoption is in part due to lower costs for card introduction, a simple membership scheme, an accessible top-up rechargeable format, and a relatively simple first application of entry and exit to a transport network. Within the transport setting there are also clear guidelines on data protection and consumer rights. For instance, individual users are city-residents with rights due to the (often) subsidised nature of public transport, or administered by

governments that have to respect the rights of citizens. This also places responsibilities on the service providers in that they must shoulder the liabilities of any arising errors or failures.

Even the public transport case for NFC is facing a significant shift in business cases, and the implications for ensuring the effectiveness of its own service remain to be known. Credit card companies and other actors may soon be in positions to manage these NFC services with ease. We can imagine a day when Transport for London will no longer issue Oyster cards. What are the implications for residents, consumers, and citizens if the credit card companies, or other third parties take over Oyster's services?

As other business models arise to build on the work done by the first-movers in transport, these approaches will have to reflect upon the nature of the protections and safeguards for consumers. Some particular types of business models might, through the use of NFC, allow the creation of parallel and alternative "financial services" using localised facilities or identity/profiling services. If this becomes commonplace, what form of governance would apply to this environment? Which regulatory framework will be in place to protect consumers and providers of NFC services?

Table 5a presents a stakeholder comparison among four of the major cities studieed showing relations with the transport operator, the trusted service provider, the apparent goals of the trusted service provider, and trends on the use and/or implementation of the card system and finally the privacy implications of the trend.

The entities that are the key stakeholders in the potential and new deployments are often very different from the early movers in this domain. They are regulated in very different ways, and have significantly different interests and motivations for investing. This uncertainty over governance is occurring even as the levels of personal information and the potentials for using that information for various purposes increases dramatically. The sensitivity of the information is thus growing even as the restrictions that were previously understood and deployed are more uncertain and weakening.

Much of the necessary debate in this domain will be about what qualifies as personal information.[13] On

[13] To see the regulatory discussion on this in Europe, see the conclusions of the committee of European privacy commissioners in the Article 29 Working Party Opinion 4/2007 'On the Concept of Personal Data', June 20, 2007, available at

the face of it, many may not consider their transactional information 'personal', while unique identifiers are perhaps more obvious, and personally identifiable information such as subscriber information is most obviously 'personal information'. In transportation, all of the above information can be personal and thus falls under the remit of data protection law. Transactional information about locations can disclose movements even if the user's name is unknown, and when faced with the contactless device identifier it may be possible to reconstruct a profile. Location, as many mobile operating system designers and mobile operators have come to learn, is personal information even if the individual's name is not involved. As we have seen in recent cases, it is often the information that people find most worrying when it is collected and disclosed.

	London	Helsinki	HK	Tokyo
Transport operator	TFL (Public sector)	Helsinki Transport (Public sector)	MTR (Public/Private sector)	JR (Public/Private sector)
Trusted contactless provider	TFL	Helsinki Transport / Bus operator (as going to national interoperable/multi-card system	Octopus International: JV with MTR (HK government) as majority share holder	Felica Networks: JV with Sony (equipment mfg) as main shareholder, Telco DoCoMo with large minority, JR only 5%
Goals of trusted service provider	Public service, not for profit	Public service, not for profit	Commercially driven	Commercially driven
Trend	TFL decreasing influence over the future of Oyster (allowing EMV billing). Collaboration with credit card firms. Up to credit card firms to integrate with mobile and possible 'wallets'.	National interoperability with two or three cards, no NFC commerce at this point.	Expand Octopus into mainland China. Full on competition with credit cards. No mobile app in sight.	FeliCa commercial network, already national and full mobile integration. Expand transaction volume in Japan. Compete/collaborate with credit cards (post-paid).
Privacy implications of trend	Diverse set of parties and jurisdictions may yet conflict.	Contained within the transport system, and within regulations that apply to public sector.	Continuous challenge from commercial interests in order to compete with credit cards	Regulated by 'p-mark', but there are weak regulatory frameworks for privacy protection in Japan.

Table 5a. Stakeholder comparison for public transport systems using contactless or NFC

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

In table 5b we show a high order comparison of the contactless elements (in future NFC) for four of the cities researched in detail for this study.

Contactless transport scheme	Oyster	Green Card	Octopus	Suica
e-payments with transport cards	No plan	No plan	Deployed	Deployed
contactless loyalty and coupon system	None implemented	Under evaluation	Variable schemes for loyalty and bonuses	Many flavours of schemes for both loyalty & coupons

Table 5b: A comparison of contactless wallet functionality in London, Hong Kong, Helsinki, and Tokyo

Any information that can be linked to an individual is personal. The definition of personal information in the EU Directive on data protection includes "any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, menial, economic, cultural or social identity."

It is possible to devise mechanisms akin to 'cash' or paper coupons where no subscriber or profile information is exchanged. For this to be preserved throughout the chain, personal information cannot enter into the transaction upon storage or payment. If it is possible to later re-identify the individual through some means, i.e. linking transactions together to find an identifiable individual, then it was not anonymous to begin with, and the full weight of data protection law falls upon the interaction. Identifiers have a way of leaking into transactions, particularly those that identify users across multiple services. Preserving anonymity requires great care and probably some advanced cryptography. Failing that, when using identifiers they must be directed to a specific purpose, e.g. the administration of a coupon to see if it was spent, but not linked to the credit card used to complete the purchase. This task, again, is very difficult to ensure both technologically and from a policy perspective because it governs not only the functioning of NFC but also the back-office operations.

6. NFC: Control, consent and accountability

From our understanding of the relationships among stakeholders, the precedents and intentions of business models, and the state of policy discussions, we can see that the key determining factor for the near future of NFC is the power relations that emerge. Power in relation to this technology is determined by structures of control, practices of consent, and structures of accountability.

Controls are exercised by stakeholders but, as we have seen, their relationships differ greatly from case to case within public transport. Outside of that realm the differences are even more diverse. Newly emerging stakeholders, especially in the form of mobile telecom operators and other proprietary intermediaries, standards setting bodies and user groups seek controlling roles, also. For instance, carriers own the SIM card in phones, not the purchasers of the mechanism.

Furthermore, the design of the technology is a determining factor, as controls that are built into the systems through features of SIM cards differ from those that are built into the main body of mobile devices, and further differ from software controls that might be the responsibility of payment systems operators (e.g. banks, credit cards, etc.). Other control points operated by vendors will also emerge. A continuing issue will be to determine where those control points are. As the SIM card is owned by mobile network operators and they have the control over the keys to access the secure area of each card, where most of the contactless and NFC key data for exchanges are stored. Some other players might use ways to bypass the SIM card and offer services without those security features.

Consent has been dealt with in this report in relation to the "opt in" feature, but we also suggest other means to improve on this critical approach to meeting the expectations of users. We are convinced that both successful business models and effective public policy will rest heavily on the resolution of the social contract that is embodied in the means of ensuring that users' privacy is protected and that they are satisfied that they have provided clear and limited consent. The individual must also be able to withdraw consent. Consent must map against what is occurring at all levels in the transactions. If an individual does not understand that location and profile information is being shared across services, then this must not be occurring at the level of the identifiers or at a policy level across the organisations involved in the transactions. This means that all organisations throughout the transaction are accountable to following the rules of processing authorised by the act of consent.

The liabilities that are distributed throughout the systems in which NFC are used may be the most critical feature of the short-term growth of this technology. Who bears the risks, both for monetary losses and for breaches of privacy and data security, will be factored in to each decision process. Which bodies are liable to be sued and how losses might be distributed will be a critical feature. Some of this will be determined by courts and legislatures, but too vague a notion of liability is likely to be expressed as reluctance to fund on the part of investors.

Here we can take the stakeholder analysis further while describing the relationships among stakeholders and how their multiple and interrelated interests create severe competition problems. The clash of business models, with architectures that allow various third parties to make use of transactional information conducted by others is likely to result in conflict. That is, previously it was simple; there was a single transport system that was interacting with a single payment service. Now there are telecommunication networks, mobile companies, operating system developers, financial services companies, and even application developers who expect to benefit from information about transactions. Who makes decisions about control, consent and accountability within this fragmented and conflicted domain?

At the outset of the report we introduced our triangular focus of themes affecting business models for NFC: technology, regulation, and privacy. In this section we will merge these themes with how stakeholders are jockeying for position by deploying various expressions for power: control, accountability, and consent.

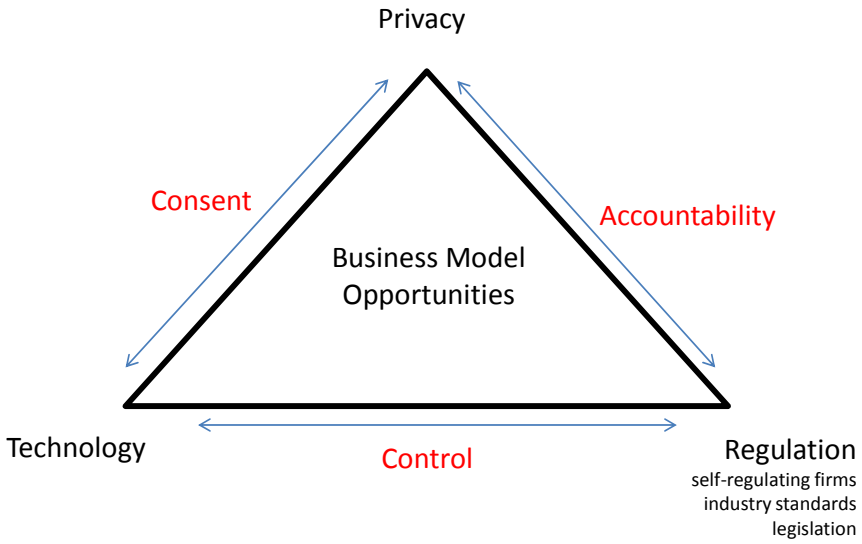

Figure 6: Interactions between the elements of the model showing consent, control and accountability

There are at least three kinds of groups responsible for making these decisions: companies that are investing in NFC (those making strategic business choices), regulators and policy makers who must make decisions about the extent to which these scenarios are acceptable, and consumers themselves who may become more empowered through the diversity of choices. It is not so simple as to assume that these groups have absolute freedom over how to make these decisions. Companies individually have varying abilities to make influential decisions based on what roles they play and the extent of their market reach. A mobile network provider has very different capabilities from an operating system developer or the transport provider. Similarly, regulators and policy makers are restricted by their remits and jurisdictions, and even with the timing of their interventions. Finally, consumers have been affected by pricing pressures such as reduced prices for using NFC over paper or other tickets.

The pressure points for all these decisions are set around who has control, what are the consent regimes, and where liabilities lie. In turn, the potential efficacy of different business strategies when providing consumers with new services will rest upon these. The introduction of new services with their combination of NFC technology and personal identifiers raises questions as to who has control, who gives consent, and what the status of that consent is. It also holds implications for who holds liability. Following on from these larger questions are the design details: how and what information is stored and transmitted, which information is collected, and how is it processed?

If identity management can be done successfully, NFC can achieve what many other technologies have failed to do: enhancing privacy and security while also supporting improved use of resources, overcoming barriers to growth and fostering innovation, facilitating global services and improving user convenience.

Spoilers may try to take advantage of consumer behaviour knowledge to induce consumers to give away their privacy in exchange for services and goods. This notion of "giving away" personal information is a fallacy, however, as individuals always retain their privacy rights even after a transaction has taken place. Yet advocates of the idea of allowing NFC to develop a strong structure for business models without overt consideration of data protection and further regulation defend this position by expressing their concern that too much regulation might severely limit its development. As discussed above, this is a common argument in technology policy that often conceals competitive elements: some business models are preserved and others are hampered through regulation. Regardless, the rise of consumer concern over privacy combined with the great potentials for empowering consumers through the use of advanced techniques places a burden upon companies and technologists to design their systems to consider privacy from the outset. Just as the deployment of RFID in Europe requires consideration of the impact upon privacy through privacy impact assessments, NFC business models and technological designs need to consider how their choices implicate privacy.

7. Determining relationships

7.1 Structure of interactions

Contactless card schemes, such as Oyster, Green Card, Octopus, and Suica, could be seen as rule-making governance mechanisms with various remits from respective regulators to control flows of user data. Users could be under the impression they are involved in fees-only transactions when in reality they are also disclosing user data. In some cases (such as Oyster PAYG) the user does not have to disclose identity information and may choose to not share any user data with the contactless card operator. However, in most cases involving value added services such as subscriptions (travel cards), currency exchanges (loyalty cards), or post-payments (credit cards) the identity of the user will be verified by operators before an offer can be made. Particularly in cases of tailored offers, prior knowledge of user preferences or user profiles are almost always needed.

One way of looking at it is that the duration of interaction between users and operators therefore varies between one-shot transactions (anonymous, and contingent renewals. The structure of interactions between NFC providers and users could therefore be described in terms of relational contracts with different grades of completeness (Brown et al. 2004). Complete contracts are possible in situations where a precise specification of the trade could be described in volume, grade, and delivery terms. Incomplete contracting induces a more intensive contact between buyer and seller focusing on quality. Business model opportunities can in part be seen as structured by the characteristics of such interactions between NFC operators and users.

Another way of approaching the problem is that through minimal disclosure and directed identifiers, walls may be built up so that an individual can enjoy privacy-preserving multi-purpose and cross-boundary interactions, even repeatedly. Much of it comes down to the design of the system, and the subsequent regulations. These might not necessarily be of a legal nature but if privacy-preserving practices are to become a norm then there needs to be some mechanisms to audit compliance.

The table below generalises contentious situations regarding consent and accountability when users are under the impression they enter a complete contract, but may in reality enter an incomplete contract due to lack of control over their user data:

Structure of interactions	Complete contracts	Incomplete contracts	Contentious issues with consent and accountability with regards to user data
Traders' relationships	Anonymous	Trust; retaliation for cheating	Users will be gravitate towards complete contracts if they don't trust the NFC operator with their data
Offers	Public	Private	Users could give consent to a transaction without being aware of what user data is collected (and traded yet again) and accounted for by the NFC operator
Duration	One shot	Contingent renewal	Users pay for a service or product, but can't be sure for how long their data will be kept or who is liable for disposing of it

Table 7. NFC schemes and relational contracts: Adapted from Brown et al. (2004) and Bowles (2004)

7.2 Privacy threats to stakeholders

Privacy respect does not end with mere legal compliance. Rather, NFC systems designers must address how abuse is limited, how consent and control of the user are implemented into the NFC, disclosure is

minimised, and how only relevant parties are granted access to the information, while also considering how individuals are interacting with the system. The 'laws of identity' developed by Kim Cameron[14]http://www.identityblog.com/?p=354 provide a useful framework for analysing how these decisions may be designed into technologies and services. Cameron's identity framework builds from a similar origin to NFC and public transport, in that identity used to be the preserve of few players, often monopoly services, which in most cases are government. The changing business environment meant that more stakeholders were getting involved, and the 'laws of identity' establishes some of the basic rules these participants must consider in order to protect the individual. Rather than establishing a single ideal technique, the laws of identity are an understanding of the 'metasystem' that provides many of the benefits sought after by each stakeholder while protecting the rights of the individual citizen and consumer. An example of this 'meta-system' is an NFC enabled wallet with a number of cards, or even a wallet of wallets.

Services using NFC capability on a device having a collective user interface (or access) to the various services on the secure element – a so called 'wallet' may then be assessed under these rules with regards to the protection of privacy. First, a service gathered under a 'wallet' must only reveal personal information with the consent of the individual, and so we must consider how the individual's approval is sought. Any information must then be disclosed for limited uses, and this hinges on how the uses are communicated to the individual. Then this approach would verify that information must be disclosed only to the fewest parties, e.g. the wallet must manage identifiers in ways that even the wallet provider itself may only collect transactional information, and that only if it is necessary. Following on from this, information that is disclosed should be directed at that service, e.g. the credit payment transaction involves a credit card number, the loyalty scheme has a separate unique identifier, the transport network receives another separate identifier, and there is no need unnecessarily to share identifiers without the individual's consent. Ultimately, the integrity of the entire wallet relies on the technology being able to do these things. It must sustain directed identifiers, it must accommodate multiple stakeholders securing the transactions from the technology to the individual user through directed transactions, it should ensure limited disclosures for limited uses, and it should promote user awareness and involvement.

[14] http://www.identityblog.com/?p=354

7.3 Design

Among the design decisions for NFC are those related to data characteristics, security, transmission protocols and usage settings, and all of these have privacy implications. Basic design of data capacity and formatting can be deliberate in accommodating certain kinds of data mining practices. Security design choices include capabilities for trusted versus non-trusted functionalities. Protocols designed in address various forms of calibration that affect, among other things, speed and proximity capabilities. Finally usage settings determine how the mechanism might be used as a reader, a writer, or both a reader-writer.

Design decisions for secure elements currently commonly proceeds without reference to the power relations as expressed by control, consent and accountability. Better practices will only emerge after procedures are in place to accommodate the input from the analysis of user experiences with regard to privacy. The resulting design improvements will both increase the likelihood of success in commercialisation and the acceptability of NFC to users.

In terms of NFC the role of the trusted service managers is important. Mastercard has been running a scheme with Gemalto for this role. Similarly, Ericsson has enabled the same strategy with mobile operators. Gemalto has defined their role very narrowly, based on GSMA guidelines[=]. The specification for the role was defined in 2009 by the Global Platform White Paper (Global Platform, 2009) which presented some workable recommendations of designs in relation to trusted services managers.

7.4 Analyzing privacy

Although NFC is not a traditional type of innovation, we see a concensus emerging on ways to tackle privacy concerns. Consideration of privacy at the design of the technologies and services is necessary in order to avoid potential regulatory pitfalls. Investments in NFC may be poorly-placed unless a regulatory backlash is considered within the risk mitigation strategies at the earliest stages. There are analogies with internet business models that have provoked regulators many years after heavy investments were made.

For specialists, analysing shifting market and institutional relationships and seeing how technology is affecting the use of information is a common practice. However, this approach may miss the detailed

legal issues that are enabling or preventing changes in relationships, and treat the technology merely as an object being developed to respond to market dynamics.

Most manufacturers of NFC chips, along with the NFC Forum, have tried to describe privacy as primarily a technical issue and they merely monitor the protocols and the transfer methods. This is a preferred path leaving the issues of security to the telecom operators, regulators and users. Issues such as security could be well covered in this approach, but a latent risk of this approach is to ignore legal issues, as well as some key actors, even the users, and considerations such as individual attitudes and social norms.

The other set of specialists is primarily concerned with the legal aspect of NFC. For them to take a legal approach is to establish a preferred framework for regulation, but at the moment there is no law that considers NFC, and it may be years before relevant regulatory guidance emerges. When regulations do emerge, early entrants into this market may be punished for not adequately considering privacy and security. Alternatively, the regulation may emerge too late to have any significant impact on the technology practices and services.

Analysing privacy requires us to heed technological and legal changes, monitor information flows and all the implicated institutional actors. Importantly, however, our proposed analytical approach lets us include the individual, whether regarded as a citizen, consumer, or data subject. Including the individual is not necessarily a novel approach. Marketing research and human-computer interaction researchers have long considered the individual and/or the user and adoption dynamics. Within a privacy research approach, however, the user is an individual who is legally protected as a citizen and a consumer.

It is useful to differentiate between the individual's intended actions and their actual behaviour induced under certain conditions. Legal protection may not always be adequate to prevent the infringement of the user's privacy. Many perfectly legal agreements are digitally signed and entered into without being viewed or understood. In the established arena of the web and physical ("High Street") purchases of goods and services, this is subject to widespread scrutiny – in the case of the web, from user and consumer groups who very rapidly highlight and condemn poor quality or sharp practices, and in the case of the mainstream physical market, a large section of the media is dedicated to "watchdog" actions on consumer rights. However, where NFC is concerned, few such safeguards exist and it is difficult to

investigate malpractice. It would be relatively easy for NFC providers and partners to follow the law, strongly steer consumers towards certain behaviours in ways that could be considered sharp practice, and escape widespread censure.

This lack of "soft" protection has a few analogies in the current marketplace. Firstly, some banks impose high charges on account holders and although this is legal it is poorly understood by the consumer. Secondly, a householder is in theory free to switch between competing utility companies, but the way in which energy costs are calculated can be opaque. Thirdly, some airlines and rail companies exploit legal loopholes to make it difficult to claim refunds for delays. These examples do not concern privacy, but do serve to illustrate how legal protection does not always adequately protect consumer rights. In the case of NFC privacy, a potentially long history of personal data and transactions, which the consumer may only dimly recall, could be even more easily exploited. Any privacy analysis should include a section analysing the practical implications of NFC providers' privacy policies, bearing in mind that they will almost certainly comply with the letter of the law, yet may discretely circumvent its spirit and purpose.

Even more traditional privacy analyses need to be updated to consider the relationships among institutions. One of the leading techniques for analysing privacy in a setting is a privacy audit. A privacy audit is applied traditionally to organisations that have specific and well-established legal requirements, and in turn, the privacy audit will ascertain whether information in that organisation is processed in accordance with the law. It is very much a test of compliance within an organisational setting. It is therefore inappropriate for applying to a context where the legal regime is not yet explicit about an innovation and when the innovation itself is in a formative stage.

Many privacy experts recommend applying a recent, structured technique for assessing privacy within such unstructured environments: the privacy impact assessment (PIA). These are emerging as a best practice in many countries and settings, and are required by law in others (e.g. the U.S. Federal Government has required PIAs for all new government systems since the E-Government Act of 2002). This will allow experts to understand better how the system was designed to consider privacy through minimal processing of information, where the control is been excised, how this control can be with the well understood implications, and how consent is managed and adhered to. It can also define for many possible cases guidance rules for dealing with accountability and tussles that will emerge from the NFC

business models.

PIAs are not easy. They take time and other resources. They require expertise and attention. They require coordination across federated services. Just as app stores have found problems in ensuring that all applications have privacy policies, it will be difficult to ensure that every stakeholder in a process has considered privacy and is accountable with regards to privacy law. Regulators will likely reach for PIAs as a first resort, as it has been applied already to RFID technologies. This may cause much delay and consternation in the deployment of NFC.

The alternative is to design privacy into the use of NFC right down to how the identifiers are managed. Business models will have to consider privacy in the way they approach the processing of personal information. If done properly, NFC will spur new forms of innovation. If not, it could be stunted.

8. Conclusions

This white paper has focused on NFC as a technology that has reached maturity for adoption. We investigated contactless technologies and their use as a faster and more efficient metropolitan ticketing system, through the current development plans to be integrated in mobile phones, to its expansion to provide many other services (e.g. other forms of ticketing, micro payments, loyalty schemes, etc). All these developments have significant implications for consumers and societal behaviour.

For the cases studies the comparison among transport systems demonstrates varieties of implementation in technology and business models. All these various systems can coexist, but given the infringements of rights that some elements of the expansion of systems threaten, new regulatory practices are going to be demanded. In April 2011 the EU decided to encourage self-regulation for the near future expansion of NFC. The overall goal is to allow a period for free competition and quick development of economically sustainable business models using the technology. This is consistent with our own conclusions, which focus on the development of business models and the protection of the rights of consumers.

The current approach to choosing between “opt in” and “opt out” is inadequate for NFC applications. Although consent is an important part of the perception of having control of one’s privacy, users cannot adequately asses how effective and at what point the individual knows when there is a default opt in or

opt out. Rather, using Kim Cameron's 'laws of identity' approach, developers and businesses could, at the outset, consider how they involve the individual in each transaction and to what extent personal information is implicated. NFC and its use on various platforms, most notably mobile phones, has great potential for involving and informing the user in ways that is currently impossible with the simple NFC-as-a-card implementation. It is therefore necessary to devise ways to inform users about the manner in which their information is used that is clear and unobtrusive, and in turn to ensure that information is only processed accordingly.

We foresee that are ways to overcome the limitations of this consumer control problem to accommodate other stakeholders of the NFC business environment. An effective measure will be to create mechanisms for quick assessment for each new service that is provided for NFC in regards of the practical aspects of implementation e.g. data retention, location, and distribution. This can be used as a "fact sheet" by industry and regulators to provide a comprehensive understanding to consumers. This sort of "fact sheet" might be analogous to the way McDonalds provides a calorie count to people buying meals.

Information that is recorded and stored by different NFC stakeholders ought to be bounded by a contractual obligation of a "last use by date for data". Certain NFC services require storing data for shorter periods of time than others, or they might not require stored data at all. By establishing a maximum time for storage of data that is economically sustainable within the business model there will likely be benefits in reducing potential fraud and violations of the privacy rights of consumers. This must not only be done in the form of a policy principle. Rather, auditable statements must be provided, backed up by technological design, with serious penalties applied for failing to adhere to their claims.

Many consumer concerns have not yet been addressed by the current providers of NFC services. Clear guidelines need to be provided about the procedures for registering complaints and for rectifying violations. This outlook will be more complicated when mobile based e-wallets become popular features, when more people make use of multiple authentication features and when there is access to a large number of different kinds of funding sources (e.g. credit cards, banks, etc.).

Our comparative research also shows the value of clarifying accountability terms for NFC use. Much of the attention paid to accountability is focused on the determination of the limits for transactions. In contrast, too little serious debate is in evidence about cases of fraud or unlawful use of personal

information by others. Clarifying and embedding preventive measures for accountability will have a strong positive effect upon the development of business models. Unless properly designed and deployed, NFC could very well make matters worse in this regard.

The governance of the NFC system is constituted of multiple stakeholders, some of them obtaining significant control over the potential market of NFC services and applications. Coherence and consistency are required as users become familiar with new ways of deploying NFC. If one NFC interaction varies significantly from another, while hiding the levels of protections and invasiveness, then the entire system is poorly served and the technology can become maligned much as RFID was. Greater cooperation is required amongst stakeholders to resolve practices for interfaces, minimise legal ambiguities, and to come to agreement on best practices in the issuance and validation of cards. While the industry pays considerable attention to this at hardware and software levels they have not taken into account the business significance of it in relation to how to handle the multiple identities and models of services. This recommendation does not affect current systems in place to deal with the validation of transactions. It is highly likely that someone will at some time soon have to be responsible for deciding which third parties can or cannot participate in the NFC system by issuing and validating 'cards'.

To conclude, it is not so simple as to say that NFC is inevitable because of its widespread use. Nor is it inevitably going to expand because key market players have decided to include the technology within their devices and services. But as we have seen with transport, the potential for NFC is immense and may yet challenge some of the well-established market participants and provide new and fertile grounds for business and trade. NFC, if deployed well, like many innovations, has much to offer. However, the risks to personal privacy must be addressed. This is not only to protect against surveillance, but it is essential to ensure that there is confidence in the marketplaces that may yet emerge with widespread use of NFC.

The key danger is that the discussion of privacy in this domain will degenerate into debates over 'regulation' vs. 'innovation', as we have seen in so many other technology policy debates. For NFC to thrive, privacy must be considered in the design of the technology, the platforms, and the services. The key questions raised throughout this report must be answerable by all stakeholders in the emerging system: how are you informing and involving citizens and consumers, protecting their information from unnecessary collection and use, and ensuring that any arising risks are mitigated? One day the

law will catch up, and regulators wonder what their roles are and, though it may be overly optimistic, we can hope that there will be very little for them to do. Not because NFC failed to live up to its potential, but because the positive opportunities for transforming markets and the ways that we engage with citizens and consumers have been harnessed to the benefit of all.

Appendices

Appendix 1 – London

The UK Context

In the UK the partial privatisation of public transport has created difficult conditions for the implementation of a standard collection system. The communications regulator, OFCOM, describes the need to further integrate ticketing in order to reduce travelling times[15]. The case of London has always been exceptional due to the very large number of trips generated in the city, which makes the implementation of any new ticketing systems a major stakeholder in the whole of the UK transport market. Around 70% of all National Rail journeys begin or end in London, and the revenue from fares for Transport for London alone was £2.5 billion in 2009.

In 2009 the Department for Transport decided to provide £20m in funding over the following five years to enable nine of England's largest urban areas to make the switch to NFC-compatible transport ticketing systems. There is an overall goal to implement NFC in the entire London network before the Olympics in 2012. Also in 2012, Transport for London launches "touch and go" bus payments with NFC enabled credit and debit cards. Part of the reason is the influx of foreign nationals for the Olympics and it would save the transport authorities costs if they can limit the issuance of travel cards. It is therefore technically an incremental step rather than a major leap to embed such credit cards chips in phones, similar to Felica payments in Japan. As Transport for London is moving towards phasing out its Oyster system, they indicate that initiatives for mobile ticket payments are more likely to come from mobile handset makers and financial institutions than from themselves. If the UK succeeds with such mobile NFC payments in the transport system, it will be approximately 10 years after it was introduced in Japan.

The Oyster card

London Underground implemented its first travel card in 1983. By 1989 this card was integrated with the national rail-ticketing network. A major change in the administration of ticketing revenue took

[15] Based on a report written by Methley in 2008

place in 1998 when the Prestige company was awarded the contract for ticketing services and a process to roll out the creation of a faster, revenue-driven ticketing system began. After a number of years in the pipeline, the Oyster card was launched in 2003. This was presented as a bespoke solution able to deal with the problems of scale on the London Transport network. Underground revenue lost due to irregular ticket travel have subsequently fallen from about 4% in 2002 (before the launch of Oyster) to less than 1.5% by the end of 2007[16].

The Oyster card is an RFID smart card used for electronic ticketing. Oyster is simple: one purchases the card, tops up with cash either at terminals or online, then swipes the card at a reader when taking a train or bus trip. Ticket costs and concessions are automatically deducted. The Oyster card makes ticketing much more efficient for the consumer: no paper tickets, no handover of cash, little or no interaction with ticketing staff, and speedier processing when entering the train station or bus. For the transport authorities, there are cost savings and operators suffer far fewer instances of ticket payment avoidance or counterfeit tickets. The original Oyster card was a subscription only card, which reduced the costs of travelling in some cases by 50%. In 2004 the Oyster "pay as you go" (PAYG) option was launched, and between 2007 and 2010 the Oyster card PAYG service was extended to national rail services within London's transport zones. In 2007 a trial of NFC for mobile transport ticketing was carried out in London involving 500 customers, the largest such trial up to that time[17].

Future plans to implement bankcard or credit card and mobile application acceptance are planned across the TfL services for the 2012-2015 period. However, these have been delayed due to technical glitches that are still not satisfactorily solved from the point of view of TfL, involving especially transaction speeds, which are expected to be less than half a second for a smooth passage of the transaction.

According to figures sourced by TfL (Lewis, 2010) there are 12 million active cards in use, with the number of people travelling daily on the London Transport network estimated at 3 million. Every weekday in London, 6.3 million journeys are made on London's buses, 3.5 million on the Tube and by rail, and 0.2 million on trams, light rail and river boats; of those 80% are using Oyster.

---

16 http://www.ltmuseum.co.uk/assets/downloads/London_Transport_-_April_2009_A4.pdf

17 http://www.nfc-forum.org/resources/white_papers/NFC_in_Public_Transport.pdf

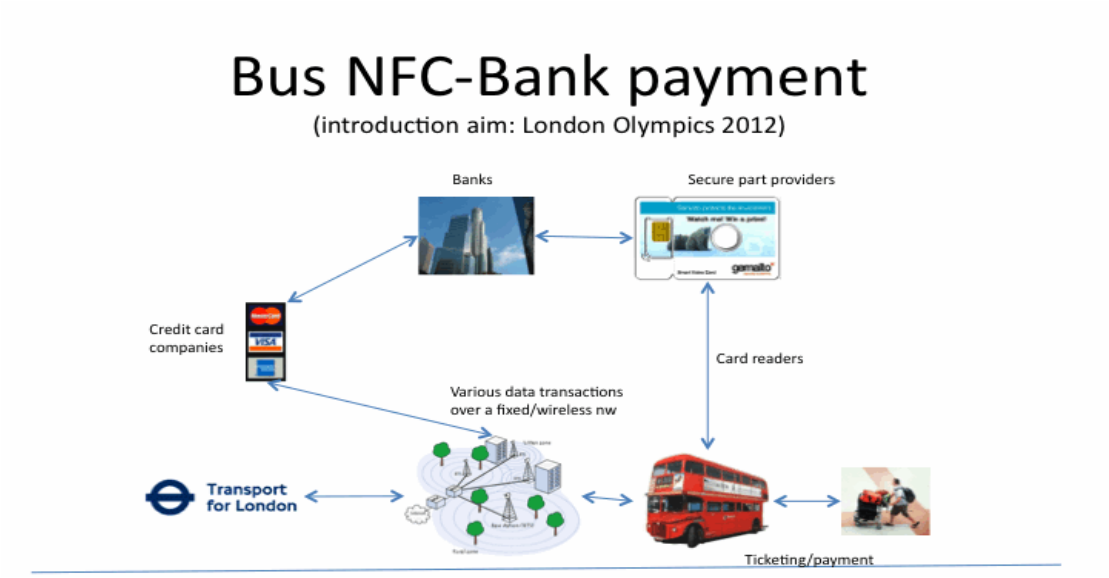

Figure A1: The use case for London Transport NFC in buses

The Oyster card has been considered a success, given the 12 million active cards. At the start of their implementation a number of problems appeared, due to malfunctioning of the technology or human errors. Further studies are now focusing on how users' behaviour might be affected by the use of devices where the initiation and acknowledgement of a transaction is passive rather than active.

The adoption was slow and not free of trouble. Users have been incorrectly charged due to software problems; the card was also hacked shortly after its official release. There have been complaints about abuse of requests for information about individuals' travel patterns. The numbers of requests from the Metropolitan Police to London Transport have been constantly increasing since 2007. The Met made 6,576 requests in 2010 and was turned down 810 times. One major drawback is that the individual user from where the data is sourced is not informed of a police search request until a prosecution occurs.

Overcharging is a continuous issue that has become worse since the first figures on complaints were published in 2008. In 2010 there were around 190,000 complaints involving a record £60 million of claims.

Appendix 2 – Hong Kong

Mainland China and Hong Kong

Although control of Hong Kong was handed back to the People's Republic of China in 1997 after

almost a century of British rule, significant differences remain in how public transport communications are regulated between Hong Kong and Mainland China. Despite these persistent inconsistencies, the Chinese government has an overall goal to standardise future regulation whilst keeping the most valuable aspects of the regulation inherited from the British system and furthering the role of Hong Kong in developing the Chinese economy. Hong Kong is administered through a special government regime that allows a more visible type of government. That has direct influence on the use of personal information in Hong Kong as it is governed by the legacy Personal Data (Privacy) Ordinance of 1996, and regulated by the Office of the Privacy Commissioner.[18]

The Octopus Card

Hong Kong started the Octopus Card as a public transport pass in 1997. A limited-purpose stored value card was issued by Creative Star Limited (CSL), a company jointly owned by transport operators, primarily for payment of transport services provided by them in their role as core users. The card scheme was launched in the third quarter of 1997, when it was exempted from the restrictive definition of multipurpose stored value cards under the government's Banking Ordinance. This was done in recognition of what was intended as a restricted range of services and because the risk of its use to the payment system and cardholders was considered slight. Subsequently, apart from the core use, the card could also be used to pay for goods and services provided by shops and kiosks within the station premises ("non-core use"); these kinds of uses were regarded as ancillary or incidental uses and were limited to 15% of the value of all transactions carried out with the card. In April 2000, CSL was authorised as a special purpose deposit-taking company to issue Octopus cards under the Banking Ordinance. The authorisation of CSL allows Octopus cards to be used for a wider range of transactions, including some that are non-transport related, with a view to enhancing the convenience for

[18] EMV vs. NFC payments: Hong Kong, Japan and beyond: In Hong Kong and Japan, NFC-enabled electronic money is challenging the credit card companies for smaller transactions involved in shopping and ticketing. In Hong Kong the Octopus scheme has so far been separate from EMV cards not allowing Octopus functionality on any credit cards. Octopus cards have become an alternative payment and salary method for migrant workers from Mainland China. Japan saw its NFC rollout competing with credit cards through lower transaction fees. However, in Japan post-paid NFC cards are offered with credit card payments under schemes offered by mobile operator NTT DoCoMo, and credit card companies JCB and VISA. Such post-paid NFC schemes boasted more than 20 million users in March 2010. The recent expansion and some 750,000 transactions registered up until May 2010.

Octopus has made inways in Mainland China through its introduction in Shenzhen and other regions. The nature of Octopus as a commercial and international standard as a clearinghouse gives its parent companies incentives to expand further. The fact that China is a laggard in credit card utilisation makes it likely that conflicts might occur between stakeholders. Keeping in mind that Octopus is built on proprietary technology from a foreign equipment manufacturer could arouse interest in Mainland China for developing their own proprietary technology.

cardholders. Accordingly, the ceiling on non-core use was raised from 15% to 50% of the aggregate value of transactions. However, the card continues to be officially regarded as mainly transport-related (BIS, 2001). Over time the Octopus card has had different periods of expansion and development, as summarized in table A2.

Time	Events
1992-1997	The MTR Corporation Limited takes the lead in reviewing automatic fare collection. Five major public transport operators established a join venture to oversee contactless smartcard systems development and implementation
1997	Octopus smartcard system launched with full integration on travel across public transport systems in Hong Kong
2000	Octopus wanting to develop the card vast commercial potential, applied and obtained a Special Purpose taking Company authorisation from the Hong Kong Monetary Authority[19] to expand its use to a wider base of different applications
2001	Octopus stakeholders sign a change on the company status from non-profit making to profit making
2003	Octopus wins its first overseas contract to supply its Clearing House System for the national contactless smartcard scheme in the Netherlands
2005	Introduction of a common brand with loyalty programs over the transport and commerce networks
2006	Octopus extends its acceptability to main land China – Shenzen region, and Automatic Add Value Service extended
2007	Octopus wins a contract to develop and implement a contactless smartcard payment in Dubai
2008	Octopus launches is co-brand credit card with Citibank. A credit card with the Octopus function.
2010	Mayor security scandal due to the Octopus company selling consumers data to third parties. New regulatory demands to be put in place on Octopus
2011	Progress in enabling multiple modes of Octopus interfaces, expansion to other service areas

Table A2: Octopus timeline - Sourced from Octopus Holdings Ltd report online

Figure A2 showed the use case for the Hong Kong demonstrates how banking services are integrated in the value proposition for ticketing.

[19] http://www.info.gov.hk/hkma/

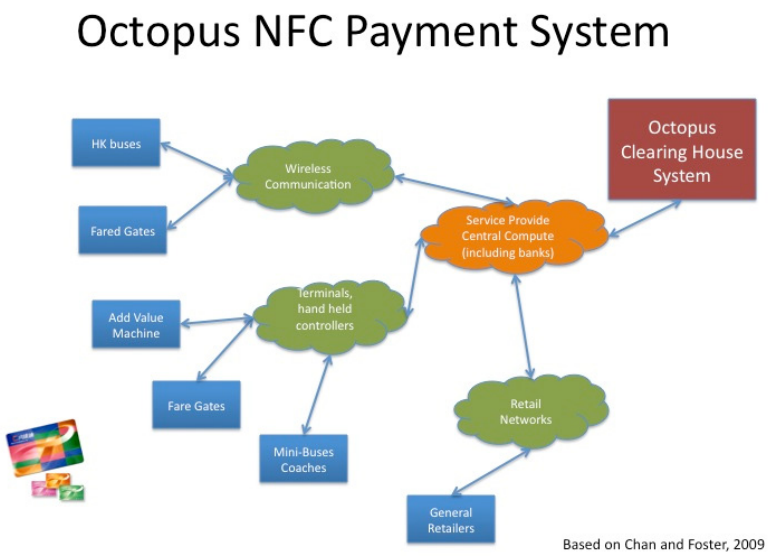

Figure A2. Octopus NFC

The Octopus card has the support of Hong Kong's five major transportation companies. Although some of these companies compete directly for riders, the saving they achieved by implementing a shared smart card system appear to have outweighed any competition concerns (Clark, 2005). There has been a lot of cooperation in establishing an equitable, or even an acceptable distribution of profits.

Besides these advantages, the RFID technology for Octopus has been embodied in a variety of forms, including key chains, mobile phones and watches. Additionally Octopus has offered incentives in savings, and its acceptance over the whole transport network makes its use attractive to consumers (Chan and Foster, 2009).

Octopus was also free of narrowly technology-related problems in the early stages of adoption. Very few failures of the Octopus card were reported. In Cantonese, Octopus has a second name that translates as "goes everywhere", a name that is very descriptive of the uses of the card that has, to a great extent, replaced cash in Hong Kong. Octopus cards can also be used as an electronic form of identification. Many Hong Kong workers clock-in and out of job sites with the same card they use to get there. Instead of using keypads or key fobs for access control, businesses authorise the Octopus card most residents already carry to unlock doors. Schools use Octopus for roll call, buying food, checking out library books and making school payments (Chan and Foster, 2009).

This type of use leverages the existing successful micro-e-money payment system for other forms of

payment, such as Hong Kong employee travel and entertainment cards, and corporate purchase cards for small purchases, which are normally paid through petty cash. Some personalized Octopus smart cards are used to remit small sums of money to destinations with the help of a remittance system such as Western Union, but there has not yet been any impact on regulatory and licensing requirements for such a transaction (Ma et al., 2008). This of course has implications in relation to Hong Kong and China laws on internal migration.

There have been several major leaks of data that have been widely publicised in the international media. The most serious one was a sale by the Octopus operator of information relevant to consumers that fell foul of the Hong Kong privacy laws. According to the existing Privacy Ordinance, it is against the law to use personal data for direct marketing unless the individual has been informed. Octopus confirmed in October 2010 that it earned about 44 million Hong Kong dollars (US$5.7 million) over four-and-a-half years from the sharing of personal information with six companies for marketing purposes. Until then, the private company denied any such sale took place.

Appendix 3 –Helsinki

The Finnish Context

Finland has a history of early trials and implementations of wireless technologies. Helsinki City Transport (HKL) has offered an SMS-based mobile ticketing service since 2001 and the presence of Nokia has ensured early trials of NFC. NFC could be seen as an element of so-called intelligent transportation systems (ITS), which is at the centre of national traffic and even export policy. Public transport makes up 15% of total personal traffic in Finland.

Helsinki, Espoo and several other towns have an integrated ticket system[20]. The same NFC ticket, called "The Green Card", can be used for travelling on buses, trams, the metro, and commuter trains, operated by Helsinki City. Finland HKL's turnover will reach approximately EUR 140 million in 2010, which amounts to less than 5% of Oyster revenues in London.

"Matkahuolto[21]" is a holding company controlled by private bus companies in Finland, and they

[20] http://www.hsl.fi/EN/ticketsandfares/Pages/default.aspx

[21] http://www.matkahuolto.fi/en/

operate a smart card not compatible to the Green Card. The Ministry of Transport and Communications work on a harmonisation scheme in order to enable interoperability of travel cards across Finland. Guidelines by the ministry of transport in their latest 2008 plan include amongst others the following[22]:

- The national government part-fund the city public transport if this contributes towards increased utilisation of public transport, it increases the competitiveness of public transport, and the cities themselves increase their investments.
- The national government should increase access to public transport and increase conditions for pedestrians and cyclists
- Ease of use for using public transport and ticketing should increase while public procurement of regional transport should improve

Even though a small market, implications of Finnish technology and policy have an impact on the European debate on privacy. Finnish technology providers also have influence beyond their size in the international markets.

The Green Card

Helsinki travel cards are contactless integrated circuit cards or proximity cards that are based on the ISO 14443A standard with a reading distance of 1 to 8 cm[23]. They replaced paper tickets in the area's public transport system by the end of 2002. The price of a ticket depends on whether passengers travel within one municipality or between municipalities, as well as on the type of the ticket and how and where it is purchased. One can choose the length of the period from 14 to 366 days. The longer uninterrupted period is chosen, the more economical is the travelling. The amount of value loaded into the card can be between 5 and 400 euros. The same card can be loaded with both a period ticket and top-up for individual travel.

Mobile ticketing is widespread, especially with the popularity of SMS travel tickets, which make up one fifth of all tickets and a third of tram tickets sold. The user can purchase a single ticket

[22] http://www.lvm.fi/c/document_library/get_file?folderId=57092&name=DLFE-3102.pdf&title=LVM 31/2008
[23] http://www.hsl.fi/FI/matkustajanopas/faq/Sivut/default.aspx

that is valid for one hour by sending a text message, but no season tickets or otherwise advanced opportunities for employers to pay for it etc. exist (Juntunen 2010).

The Helsinki Metropolitan Area Council (YTV), Helsinki City Transport, and the railway company VR acted as partners in introducing the Green Card. Usage of travel cards is recorded in a database. This information can be accessed to aid transport capacity planning. The movements of travel card users are saved and can be accessed for later retrieval. The data from the transport system has been used for crime investigations in serious cases (Hosein 2003). The Finnish Ministry of Transport and Communications are coordinating a stakeholder group where the future of regional transport integration and technology solutions, including NFC are dealt with.

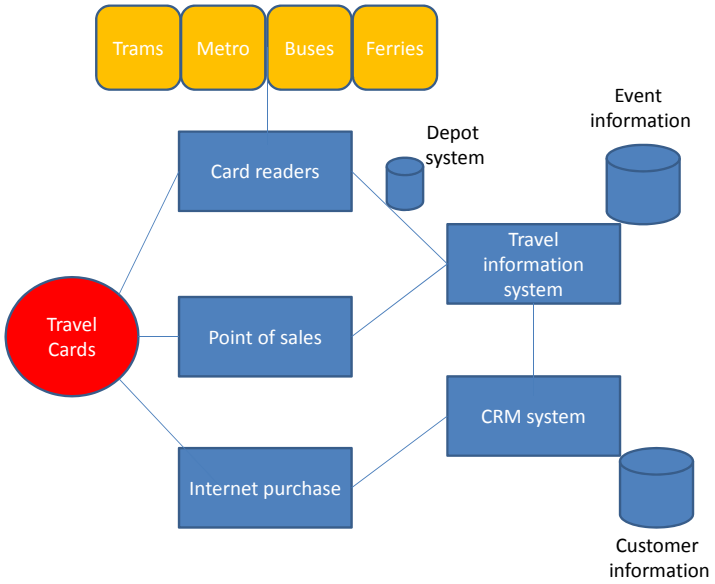

Figure A3. The use case for Helsinki – NFC in public transport

Helsinki City Transport's (HKL) main task is to produce tram and metro services, be responsible for Helsinki's track infrastructure and promote jointly with and with the help of its partners the transport in the Helsinki region[24]. The usage of the Green Card is limited to the large urban areas. The Ministry of Transport is responsible for mediating efforts to harmonise the two main

[24] http://www.hel.fi/hki/hkl/en/About+HKL HKL employs over 1,000 public transport employees who drive trams and metro trains, control traffic, maintain equipment, track and property, plan and implement new projects. HKL's turnover will reach approximately EUR 140 million in 2010. HKL's most important partner is Helsinki Region Transport (HSL).

schemes in Finland, the other scheme is jointly operated by the private bus companies. According to a consultation carried out by Sulonen et al. (2010) the European experience has not been encouraging in terms of meeting dead-lines and economic targets in launching nationwide travel card schemes[25], and they recommend to make current systems interoperable instead by multiple readers and gradual migration.

SMS tickets are also available, however so far the user cannot purchase the ticket in advance and activate it when needed, as the ticket‘s validity expires shortly after it is purchased. Moreover, the user can only buy one type of ticket and cannot receive any discounts that they might otherwise be eligible for. In addition, the user can only pay the ticket post-purchase on their mobile phone bill, which makes it impractical for the user‘s employer to pay for the ticket and also causes issues for those users who are not the operator‘s subscribers.

Appendix 4 - Tokyo

The Japan Context

Tokyo is served by two main urban transport networks: Japan Rail (JR) operating overland trains and the metro subway system. JR was gradually privatized starting in the early 1990s and traded on the stock market 2006 onwards. JR East serving the metropolitan area of Tokyo had an average of more than 16 million passengers and 12500 trains operating per day on average in 2009. JR’s total ticket revenues were 1.6 trillion yen (about £13bn) in 2010. Even though JR operates with several companies throughout Japan, the NFC travel card “Suica” is interoperable with major rail operators in Japan (the remaining areas in west Japan to be integrated by 2013)[26]. Privacy law in Japan is regulated through the constitution and overseen by the Ministry of Internal Affairs and Communications.

The Suica Card

In November 2001, an NFC travel card service called Suica became available in 424 Japan Rail East train stations located within 100 kilometres of central Tokyo (Bradley et al 2005). JR

[25] As an example they mention the Netherlands where planning began in 2001, agreements were signed 2003, the first card was rolled out 2007, and the complete system was operational in 2009.

[26] http://www.jreast.co.jp/investor/factsheet/pdf/factsheet_09.pdf

enables Suica as means for payment at retail outlets inside its train stations and in 2009 was the sixth largest operator in the Japanese domestic retail industry (Nikkei Shinbun 2009). Currently all mobile phones in the Japanese market are NFC enabled. NFC is used seamlessly for public transportation not only for ticketing but also for providing information such as maps and timetables (Fitzpatrick 2011). The first mobile NFC wallet (Suica Mobile) was launched by Felica Networks in 2004, a joint venture owned by Sony (53%), DoCoMo (38%), and Japan railways (5%). No major data breaches related to Suica have been recorded up to date.

Mobile wallets

In order to achieve fast roll-out of mobile NFC wallets DoCoMo set aside ¥20 billion for subsidizing installation of NFC readers. Merchants received the subsidized reader/writers in exchange for a small fee for each transaction (about 2% to 3%). These fees were lower than credit card fees, which averaged 3% to 5% for small merchants (Bradley et al 2005). The Felica Networks business model in the joint venture builds on three revenue streams (Bradley et al 2005):

1. License fees from carriers purchasing mobile FeliCa chips (DoCoMo was exempt from fees as one of the founders and owners)
2. Providing platform management services (transaction fees): Applications were not preinstalled on mobile FeliCa chips/phones; Instead users downloaded apps into 5-kilobyte memory area that had room for about 5 to 10 applications. FeliCa Networks received a fee for every app a user download
3. Hosted services (transaction fees): To provide application providers with hosted services such as authentication and storage of apps identity users.

Electronic money started to take off in Japan 2005 onwards with a steep rise in the number of cards issued from 30 million in 2005 to about 80 million in 2007. The value of transactions is expected to increase from 176 billion yen in 2006 to 3.269 trillion yen in 2012 (Sugiura 2009). In Japan electronic money is a competing force with the credit card system, a trend also seen in Hong Kong, but not in London or Helsinki. In April 2006 NTT DoCoMo started its “ID” service, an

NFC wallet scheme offering post-paid services connected to a credit card of choice. Users are able to pay for purchases of up to 10,000 yen (Euro 65) per month by holding their handsets close to compatible reader devices. Purchase amounts appear on their monthly phone bills and users later receive the invoice from the credit card companies (Ezell 2009).

e-money schemes in Japan (offered by)	EDY (Bitwallet)	Suica (JR East)	Nanako (7-Eleven)	Waon (EAON)	ID (NTT DoCoMo)
Number of cards users	66.2 million	39.6 m	15.1 m	21.2 m	16.3 m
Number of available shops	275 thousand	154k	86k	120k	524k

Table A3: Major e-money schemes in Japan. Source: Nikkei MJ (10 Oct, 2011)

EDY is the largest e-money scheme in Japan with more than 10 million mobile e-wallet users and part of on-line retail firm Rakuten. Users of EDY and other NFC schemes can either user their NFC card to make payments or download the associated application to their mobile phone and use the built-in NFC capability in their phone instead when making payments.

Due to new business models and opportunities for fraud emerging with the introduction of nationwide NFC payments a "payment agent registry system" has been introduced by the Consumer Affairs Agency (CAA)[27]. The registry system operates as follows: NFC payment agents (third party payment brokers) need to register in the list which is made public by the CAA; stores should clearly display if they use agents, if they are registered, and contact details for the agent; if this information is not displayed properly the agent will be removed from the list.

The Prepaid Card Law is influential on NFC payments. However, there remains some lack of

[27] The Agency itself being established in Sep 2009 http://www.caa.go.jp/en/

clarity with regards to the definition of electronic money (Sugiura 2009):

> "as opposed to promotional coupons, points, mileage and coupons earned through transactions or at no cost, electronic money is currently issued in the amount deposited therein. Thus, electronic money becomes 'based on a contractual relationship with a creditor, that which is issued having received the recorded amount as consideration, the transfer of which has the effect of settling a range of monetary obligations authorized by contract.'

In Japan privacy concerns related to mobile services (NFC was only a minor part of this) led the regulator to introduce a "PrivacyMark", introduced on April 1st 2005[28]. Privacy has been taken seriously in Japan by the regulator and service providers since the beginning and beyond of the mobile Internet. In this sense NFC privacy became for the Japanese an issue much earlier than in Europe, due to more advanced and potentially intrusive services

Appendix 5 – The two secondary cases: Seoul and Berlin

Parallel to the main cases reviewed, we conducted a brief review of two secondary cases. They were chosen either for the well developed level of use of the NFC technology generally (Seoul), or in the case of Berlin for the strong and clear position of the bodies regulating privacy to be committed to protect it from abuses of the technology.

Seoul

In South Korea, SK Telecom initiated an 'NFC Zone"[29] with preliminary tests in 2010 using RFID[30]. In August 2011, SK Telecom declared that all new smartphones to be released in the South Korean market will be NFC enabled[31]. In Korea mobile consumers use NFC equipped phones for a range of small transactions, such as food and other small purchases, or parking payments.

---

[28] http://privacymark.org/ - this website refers to a privacy certification that all firms handling personal data need to acquire

[29] The announcement was at at the GSMA's Mobile Money Summit in Singapore this year.

[30] http://www.rfidjournal.com/article/view/2372/2

[31] http://www.nearfieldcommunicationsworld.com/2011/08/01/38901/sk-telecom-all-new-smartphones-must-come-with-nfc/

An RFID Privacy Protection Guideline has been active since 2005[32] and also is applicable to NFC. Researchers in Korea have actively looked into the many uses of RFID and possible breaches of security, privacy and mobile systems. This literature is mainly technical and focusing on the ways to reinforce or detect security breaches. The body of relevant legislation focuses on defining the elements that communicate in RFID transactions, what is forbidden (e.g. recording personal information, using RFID tags to collect personal information, linking article information in an RFID tag to personal information). It also makes a clear distinction between tags that are built in or attached, which is a relevant difference when defining what is in use and what not.

The legislation goes further towards explaining how the tag can be deactivated and making the user aware that this is the case. There is a clear ban on tag implantation in the human body, and the installation of an RFID reader needs to be clearly indicated and easy for a user to notice. The legislation is fully comprehensive in terms of how to manage the technical measure for the data protection, assessment of privacy, changes and enhancement of user awareness, management of data collected and even the review of the guidelines themselves.

There is no similar legislation in place for Europe, or the UK, in terms of explicitly stating the boundaries of the use of the RFID or NFC tags. For example, the German approach, as we will see below focuses on the protection of privacy, which is a different approach from the Korean one, which focuses on the technology. The EU approach stresses the protocols to be used and how they can be used but is not explicit on banning for example RFID implantation in the body.

Berlin

Deutsche Bahn started trials on NFC with the help of Vodafone in 2008[33]. Deutsche Telecom and O2 Germany joined efforts and trials were completed in around 500 sites in Germany. Their plan was to roll out NFC before the end of 2011, a feasible goal given that the infrastructure for readers is already place. Their view of an integrated, city, regional and national fare system[34] for the use of NFC is a very different case from the situations of London and Hong Kong.

---

[32] The authors of this report only have been able to find an unofficial translation to the full content of the law at http://www.worldlii.org/int/other/PrivLRes/2005/3.html

[33] http://www.nfctimes.com/project/germany-three-telcos-join-national-railway-touchtravel-project

[34] http://www.smartinsights.net/?2011/03/10/369-national-nfc-transport-ticket-to-come-in-germany

Germany has taken the initiative in many aspects of NFC implementation and they have also been innovators in regulation at national and EU level. Their view on establishing a business system for secure and trusted transactions of NFC is due in part to the strong lobbying of many NFC chip manufactures based in Germany. The EU agreed in April 2011 to a smart tag deal based on self-regulation that aims towards supporting the manufacturing industry[35] and is consistent with German lobbying interests.

References

R1: Supplementary material about laws and regulations

EC (European Commission) (2000), Directive 2000/31/EC of the European Parliament and the Council on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market, 8 June 2000, Official Journal (OJ) L 178, p. 1-16, 17 July 2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT.

EC (2007), Directive 2007/64/EC of the European Parliament and of the Council on Payment Services in the Internal Market, 13 November 2007, OJ L 319, p. 1-36, 5 December 2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:01:EN:HTML.

EC (2007), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee, the European Central Bank and Europol - A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0679:EN:NOT.

EC (2008), "Key Challenges for Consumer Policy in the Digital Age", Roundtable on Digital Issues, Speech by Meglena Kuneva, London, 20 June 2008, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/08/347.

EC (2008), Report on Fraud regarding Non-Cash Means of Payments in the EU: the Implementation of the 2004-2007 EU Action Plan, Commission Staff Working Document, SEC(2008)511, Brussels, 22 April 2008, http://ec.europa.eu/internal_market/payments/docs/fraud/implementation_report_en.pdf.

EC (2008c), Proposal for a Directive of the European Parliament and of the Council on Consumer Rights, COM(2008)/614/final, Brussels, 8 October 2008, http://ec.europa.eu/consumers/rights/docs/Directive_final_EN.pdf.

EC (2009), Report on cross-border e-commerce in the EU, Brussels, SEC(2009)283 final, 5 March 2009, http://ec.europa.eu/consumers/strategy/docs/com_staff_wp2009_en.pdf.

EPC (European Payments Council) (2010a), White Paper on Mobile Payments, 1st Edition, 18 June 2010, Brussels, www.europeanpaymentscouncil.eu/documents/EPC492-09%20White%20Paper%20Mobile%20Payments%20version%202.0%20finalrev.pdf.

EPC (2010b), "Driving Forward the SEPA Vision", Annual Report 2009, www.europeanpaymentscouncil.eu/documents/EPC050-10%20EPC%20Annual%20Report%20v%201.0%20final.pdf

[35] http://www.reuters.com/article/2011/04/06/eu-smarttags-idUSLDE7351XC20110406

R2: Bibliographic references

Adnet, F. and G. Fremiot (2009). Near Field Communications (NFC): Take Off at Last? . Paris, France, Greenwich Consulting France: 17.

Avenel, Y. (2011). SmartCards Trends - Smart- Security, Trust & Privacy. La Falaise, France, Omnipress Publication, Issue 6, Volume VII: 24.

Baker, S. (2010). The Privacy Problem: What's wrong with Privacy? The Next Digital Decade Essay on the Future of the Internet. B. Szoka and A. Marcus. Washington D.C, Tech Freedom: 483-508.

Bank-of-Finland (2003). Card, Internet and mobile payments in Finland. Helsinki, Finland, Financial Markets Department: Online Report http://129.3.20.41/eps/dev/papers/0405/0405004.pdf.

Bertele, U., A. Perego, et al. (2011). Observatory on NFC & Mobile Payment - Mobile Payment: Expectations vs. reality. MIlan, Italy, Politecnico di Milano - School of Management: 16.

Beynon-Davies, P. (2011). The Enactment of Personal Identity. European Conference of Information Systems 2011. Helsinki, Finland.

BIS (2001). Survey of Electronic Money Development. Basel. Switzerland, Committee on Payment and Settlement Systems - Bank for International Settlements: 112.

Blaquiere, A. (2009). E-Ticketing. Toulouse, France, CIVITAS Cities-To-Cities Exchange: Promoting Transport Management Systems: 4.

Blaquiere, A. (2009). How to Change Mobility - Final Policy Recommendations Report. Toulouse, France, CIVITAS -Cities-To-Cities Exchange: Promoting Transport Management Systems: 100.

Bockisch, A. and C. Cantu Alejandro (2010). Trust in Partner Relationships for NFC Applications. KTH Computer Science and Communication. Stockholm, Sweden, KTH - Royal Institute of Technology: 84.

Bowles, S., 2004. Microeconomics behavior, institutions, and evolution, New York ;Princeton N.J.: Russell Sage Foundation;Princeton University Press.

Branzei, O., I. Vertinsky, et al. (2007). "Culture-Contingent signs of trust in emergent relationships." Organisational Behaviour and Human Decision Processes(104): 61-82.

Broex, A. and R. De Vulder (2008). What is the Value of Mobile Payments, Mobey Forum Mobile Financial Services Ltf: 12.

Brown, M., Falk, A. & Fehr, E., 2004. Relational contracts and the nature of market interactions. Econometrica, 72(3), pp.747-780.

BSI (2010). Technical Guidelines RFID as Templates for the PIA-Framework. Bonn, Germany, Federal Office for Information Security (BSI - Bundesamt fur Sicherheit in der Informationstechnik): 26.

CERP (2007). Working Paper on future RFID Research Needs, Information Society (Cluster of European RFID Projects): 25.

Chan, E. and P. Foster (2009). Octopus. Hong Kong, China, Center for Business Case Studies, Hong Kong University of Science and Technology: 28.

Chen, L.-d. and R. Nath (2008). "Determinants of mobile payments: an empirical analysis." Journal of International Technology and Information Management.

Chidembo, N. (2009). Exploring Consumer Adoption of NFC-Enabled Mobile Payments in South Africa. School of Information Technology. Pretoria, South Africa, University of Pretoria: 111.

Clark, C. L. (2005). "Shopping without cash: The emergence of the e-purse." Economic Perspectives

by the Federal Reserve Bank of Chicago(4Q): 34-51.

Clark, S. (2011). NFC Business Models - White paper: Summary and key findings. Monmouth, UK, SJB Research: 18.

House of Commons, (2008). Ticketing and Concessionary Travel on Public Transport London, UK, House of Commons Transport Committee: 242.

Communities, C. o. t. E. (2009). Comission Recommendation on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio-Frequency Identification. Brussels, Belgiun, Comission of the European Communities: 10.

BMG Consulting (2008). e-cards in Kaunas Schools. Kaunas, Lithuania, BMG Consuting: 3.

Courtney, T. and L. Harrison (2010). NFC Near Field Communications - Smart Card Technology International. London, UK, Smart Card Technology International NFC: 92.

Crotch-Harvey, T. (2009). NFC - Near Field Communications, IDTechex: 26.

Dahlberg, T., N. Mallat, et al. (2006). "Mobile Payments: A Review of Past, Present, and Future Research." ECRA (Electronic Commerce Research and Applications) Journal's Special Issue on Mobile Payments.

Das, T. K. and B. S. Teng (2004). "The risk-based view of trust: A conceptual framework." Journal of Business and Psychology 19(1): 85-116.

Dass, R. and S. Pal (2011). Exploring the Factors Affecting the Adoption of Mobile Financial Services Among the Rural Under-banked. European Conference of Information Systems -2011. Helsinki, Finland.

Dave, R. (2010). Privacy in Mobile-Ticketing - Network Security Seminar. Aalto, Finland, Aalto Univeristy: 6.

De Jong, E. (2007). Status of Mobile Payments. Utrecht, Netherlands, Thaesis B.V: 44.

Downes, L. (2010). A Market Approach to Privacy Policy. The Next Digital Decade: Essays on the Future of the Internet. B. Szoka and A. Marcus. Washington D.C, Tech Freedom: 509-528.

Duverne, C. (2009). Ready to take Off - Key initiatives for the Commercial Success of NFC, NXP: 27.

Economides, N., 2003. Competition Policy in Networked Industries: An Introduction. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.172.8291&rep=rep1&type=pdf [Accessed August 16, 2011].

Edwards, J. (2007). Near Field Communication in Japan, Australia Japan Business Association: 9.

Elaluf-Calderwood, S., B. D. Eaton, et al. (2011). Mobile Platforms as Convergent Systems: Analysing Control points and Tussles with Emergent Socio-technical Discourses. Mobile Communications (to be published in September). G. Scerbe, Intech - Open Access Publisher

Elliot, J. and A. Whitcombe (2009). The Use of Near Field Communications (NFC) technology in mobile phones for public transport ticketing. Guildford, Consult Hyperion in behalf of the UK Department of Transport: 52.

European Payments Council (2011). Draft - Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines. Brussels, EU, European Payments Council: 117.

European Payments Council and GSMA. Association (2010). EPC-GSM Mobile Contactless Payments Service Management Roles - Requirements and Specifications, European Payments Council (EPC): 69.

European Payments Coucil and GSMA (2010). EPC – GSMA Mobile Contactless Payments Service Management Roles Requirements and Specifications, GSM Association and the European Payments Council (EPC): 69.

Eze, U. C., G. Goh Guan Gan, et al. (2008). "Modelling User Trust and Mobile Payment Adoption: A conceptual framework." Communications of the IBIMA 3: 224-231.

Ezell, S. (2009). Explaining International IT Application Leadership: Contactless Mobile Payments. Washington, USA, ITIF - The Information Technology & Innovation Foundation: 60.

Falke, O., E. Rukzio, et al. (2007). Mobile Services for Near Field Communication. Munich, Germany, University of Munich: 18.

FeliCa Networks, 2011. Outlines of Mobile FeliCa, Available at: http://www.slideshare.net/echangeurba/outlines-of-mobile-felica.

Fitzpatrick, M., 2011. BBC News - Near field communication transforms travel in Japan. Available at: http://www.bbc.co.uk/news/business-13216267 [Accessed October 7, 2011].

Flodin, J. (2010). Social Networks in an NFC Context. Computer Science and Engineering. Lulea, Lulea University of Technology: 45.

NFC Forum, (2011). NFC in Public Transport - January 2011. Wakefield, MA, USA, NFC Forum: 33.

GlobalPlatform (2009). GlobalPlatform's Proposition for NFC Mobile: Secure Element Management and Messaging - White Paper, Global Platform: 36.

Gomes, R. (2007). Introduction to NFC. 16th IST Mobile & Wireless Communications Summit. Budapest, Hungary, Philips: 34.

GSMA (2011). "GSAM Publishes Mobile Privacy Principles." Retrieved May 2011, 2011, from http://www.gsmworld.com/newsroom/press-releases/2011/5992.htm.

Gutwirth, S. (2002). Privacy and the Information Age. Boston, Rowman & Littlefield Publishers Inc.

Her Majesty Treasury, (2010). Laying of regulations to implement the new E-Money Directive - Consultation Document. London, UK, HM Treasury: 112.

Hosein, G., 2003. Privacy, Technology, and Europe: A report for Japan's Ministry of Public Management, Home Affairs Postal and Telecommunications 373, Available at: http://personal.lse.ac.uk/hosein/pets/japan_pets.pdf.

Huomo, T. (2008). Near Field Communication in the Public Transport Industry - Research Summary. Tampere, Finland, VTT: 22.

InfoCom (2011). Innovations Spotlight - Operator Initiatives in Near Field Communications Technology. Stuttgart, Germany, InfoCom Telecommunications Consultancy: 24.

Isomursu, M. (2008). "Tags and the City." PsychNology Journal, 6(2): 131-156.

ITEA (2009). Taking a touching approach to transport ticketing and home care for the elderly. Oulu, Finland, VTT: 2.

Jansse, M. and A. Johan (2011). Challenges for Adopting Cloud-Based Software as a Service (SAA) in the Public Sector. European Conference of Information Systems 2011. Helsinki, Finland.

Jefferson, T. (2009). Making mobile Wallets a Success - White Paper. Oxford, UK, The Human Chain: 12.

Jefferson, T. (2011). White Paper - The Changing Face of Mobile. Oxford, UK, The Human Chain: 8.

Jefferson, T. (2011). Alternative NFC Form Factors - White Paper. Oxford, UK, The Human Chain: 8.

Jefferson, T. (2011). What is the role of the microSD form factor in the NFC market? Oxford, UK, The Human Chain: 2.

Jefferson, T. (2011). NFC payments in Europe - What is the opportunity? Oxford, UK, The Human

Chain Ltf: 9.

Juniper-Research (2009). Mobile Ticket to Ride! - Mobile Ticketing Applications and Markets: Transport, Sport and Entertainment 2009-2014. Basingstoke, Hampshire, Juniper Research 6.

Juniper-Research (2009). Transaction Complete! NFC Solutions, Juniper Research: 6.

Juntunen, A. (2010). Near Field Communication in Mobile Ticketing - Business Model Analysis. School of Science and Technology - Faculty of Information and Natural Sciences. Aalto, Finland, Aalto University: 80.

Juntunen, A., S. Luukkainen, et al. (2010). Deploying NFC Technology for Mobile Ticketing Services – Identification of Critical Business Model Issues. Ninth International Conference on Mobile Business / Ninth Global Mobility Roundtable. Athens, Greece, IEEE.

JR East, 2011. Suica - JR East Corporate Web Page. Available at: http://www.jreast.co.jp/suica/index.html [Accessed October 11, 2011].

Kärrberg, P. & Liebenau, J., 2006. IT and Telecoms Convergence: Mobile Service Delivery in the EU and Japan. In Mobility Roundtable. Helsinki: Helsinki School of Economics. Available at: http://sprouts.aisnet.org/478/1/Policy_Issues_2_2.pdf [Accessed September 25, 2011].

Kallineken, A. (2010). Studies on User Experience of Touch-Based Interaction with NFC Enabled Mobile Phones. Information Technology Department. Tampere, Finland, Tampere University of Technology: 97.

Kietzmann, J. H. (2005). In Touch Out in the Field: Coalescence and Interactive Innovation of Technology for Mobile Work. Department of Information Systems. London, UK, London School of Economics and Political Science: 267.

Kim, P. H., K. T. Dirks, et al. (2009). "The Repair of Trust: A Dynamic Bilateral Perspective and Multilevel Conceptualization." Academy of Management Review 34(3): 401-422.

Knights, D., F. Noble, et al. (2001). "Chasing shadows: Control, virtuality and the production of trust." Organization Studies 22(2): 311-336.

Lehrer, C., I. Constantiou, et al. (2011). A Cognitive Processes Analysis of Individuals' Use of Location-Based Services. European Conference of Information Systems - 2011. Helsinki, Finland.

Lehtonen, M., T. Staake, et al. (2006). The Potential of RFID And NFC in Anti-Counterfeiting - Improving Customs Processes with RFID and NFC Technology to Fight Illicit Trade. St Gallen, Switzerland, ETH Zurich - University of St Gallen: 13.

Lewis, P. (2010). London's Oyster Card Revolution to Evolution. London, UK, Transport for London: 17.

Linstone, H. A., M. Turoff, et al. (2002). The Delphi Method - Techniques and Applications. California, USA.

Lüke, K.-H., H. Mügge, et al. (2009). Integrated Solutions and Services in Public Transport on Mobile Devices. I2CS Innovative Internet Community Systems. Jena, Germany.

Ma, L. C. K., P. Banerjee, et al. (2008). "Diffusion of the "Octopus" Smart Card E-Payment System: A Business and Technology Alignment Perspective." International Journal of Business and Information 3(1): 14.

Madlmayr, G. (2008). A mobile trusted computing architecture for a near field communication ecosystem. iWAS ’08: Proceedings of the 10th International Conference on Information Integration Web-based Applications & Services, Linz, Austria.

Methley, S. (2008). Transport Final Report. Great Chesterford, Essex, UK, Quotient Associated and Plextek in Behalf of OFCOM: 53.

Mezghani, M. (2008). Study of electronic ticketing in public Transport, European Metropolitan Transport Authorities (EMTA): 56.

Mitrakas, A, (2006) “Information Security and Law in Europe” Information and Communications Technology Law 15 (1) 33-53

Mobey (2010). Mobile Remote Payments - General Guidelines for Ecosystems - White Paper, Mobey Forum - Mobile Financial Services: 56.

NICHES (2008). New and Innovative Concepts for Helping European Transport Sustainability Towards Implementation, Niches+ (EU project): 7.

Nikkei Marketing Journal (2011), “Major e-money schemes in Japan”, table, 10 Oct, 2011

Nikkei Shinbun (2009), “Japanese Retail Players Ranking”, quoted by Japan Railway, access: http://www.jreast.co.jp/life_service/shopping/index.html

Nokia (2007). White Paper Near Field Communications. Finland, NOKIA: 8.

Nokia (2007). One touch services in Vienna. Vienna, Austria, Nokia: 2.

Nokia (2007). White Paper Near Field Communication. Helsinski, Finland, Nokia: 8.

NTT DoCoMo, Inc.: Mobile FeliCa (2006), Harvard Business School

Octopus (2010). Personal Data Policy. Hong Kong, Octopus 5.

OECD (2011). Consumer Protection in Online and Mobile Payments -Draft Report. Paris, OECD Committee on Consumer Policy: 41.

Ofcom (2007). Communications Market Report. London, UK, Ofcom: 187.

Ofcom (2007). The Communications Market 2007 - Converging Communications Markets. London, UK, Ofcom: 87.

Ofcom (2008). Decision to Make the Wireless Telegraphy (Exception) (Amendment) (No 2) Regulations. London, UK, Ofcom: 25.

Okajima, M (2008), “The Suica Revolution – East Japan Railway Company’s Corporate Transformation”, C-IQ, January 2008, access: http://c-i.tv/fileadmin/c-iq/02/CIQ_20080114.pdf

Pee, L. G. (2011). Attenuating Perceived Privacy risk of Location-Based Mobil Services. European Conference of Information Systems 2011. Helsinki, Finland.

Pellerin, R., C. Yan, et al. (2009). "Player Profile Management on NFC Smart Card for Multiplayer Ubiquitous Games." International Journal of Computer Games Technology 1(1): 9.

Persoon, M. (2009). Mobile Banking and Payments. Gothenburg, Sweden, Berg Insight: 4.

Polasik, M., T. P. Wisniewski, et al. (2009). Modelling Customers' Intentions to Use Contactless Cards for Retail Payments. Torum, Poland, National Bank of Poland: 37.

Portale, V. (2011). The evolution of Mobile Payment in Italy. Milan, Italy, Politecnico di Milano 16.

Preuss, P. (2008). Rhein-Main-Verkenhrsverbund, RMV2go: 21.

Resatsch, F. (2009). Developing and Evaluating Ubiquitous Computing Applications - Using the Example of Near Field Communication in Germany. Munich, Germany, Technische Universitat Munchen.

Rousu, J. (2008). Virtual File Repository for Mobile Phones. Department of Electrical and Information Engineering. Oulu, Finland, University of Oulu: 78.

Samar, V. J. (1991). The Privacy to Right. Philadelphia,USA, Temple University Press.

Saros, J., D. Lindström, et al. (2009). A Platform for Pervasive Infrastructures, Ericsson: 6.

Schmid, K. (2008). Short & mid-term NFC Success Stories. WIMA. Monaco: 32.

Shire, C. (2010). How Secure is NFC? A review of the security needs of Transport Schemes using NFC. London, UK, Infineon Technologies: 20.

Shoham, I. (2011). Silos all over again: The case of authentification management. ID Credentials. W. Atkings. London, UK, Smart Card Technology International.

Smart, G. (2011). Smart Card Technology International - ID Credentials. London, UK, Global Smart: 120.

Smart, G. (2011). Smart Card Technology International Near Field Communications. London, UK, Global Smart: 148.

SmartCard (2009). Smart Card and Identity News. Worthing, England, Smart Card News Ltd: 19.

SmartInsights (2011). Smart Insights Weekly - Issue 3. Marseille, France, Intelligent SARL: 29.

SmartInsights (2011). Smart Insights Weekely - Issue 4. Marseille, France, Intelligent SARL: 27.

SmartTrust (2009). The role of SIM OTA and the Mobile Operator in the NFC Environment: 12.

Solove, D. (2007). The Future of Reputation: Gossip, rumour, and privacy on the Internet. New Have, CT, USA, Yale University Press.

Solove, D. (2007). "I've Got Nothing to Hide." San Diego Law Review 44: 745-772.

Solove, D. J. (2004). The Digital Person - Technology and Privacy in the Information Age. New York and London, New York University Press.

Steffen, R., J. Preißinger, et al. (2010). Near Field Communication (NFC) in an Automotive Environment - Use Cases, Architecture and Realization. 2nd International Workshop on NFC, Monaco, France.

Steinmeier, S. (2006). The Near Field Communication (NFC) Technology Roadmap, NXP: 25.

Stroh, S., D. Schneiderbauer, et al. (2007). Next Generation eTicketing. Germany, Booz Allen and Hamilton: 11.

Sulonen, R, Aura, T, Jununen, A (2010), Travel Card-Sharing Framework, Aalto University, report 23 Nov 2010

Sugiura, N. (2009). "Electronic Money and the Law: Legal realities and future challenges." Pacific Rim Law & Policy Journal Association 18(3).

Tekes (2009). SmartTouch City of Oulu - Services through NFC technology. Oulu, Finland, ITEA Smart Touch, City of Oulu - Project: 12.

TNS-VRL (2010). Mobile Payments: barriers and opportunities for take-off on the Italian Market. Prepaid Summit : Europe 2010. Milan, Italy: 23.

Tomlinson, E. C. and R. C. Mayer (2009). "The Toll of Causal Attribution Dimensions in Trust Repair." Academy of Management Review 34(1): 85-104.

Tuilkka, T. and M. Isomursu (2009). Touch The Future with a Smart Touch - VTT Research Notes 2492. Helsinski, Finland, VTT: 283.

Van Damme, G., K. Wouters, et al. (2009). Offline NFC Payments with Electronic Vouchers. MobiHeld 2009. Barcelona, Spain.

Van Esbroeck, K. (2011). The Future of NFC: key conditions for success. Near Field Communications. L. Harrison. London, UK, Smart Card Technology International: 57-60.

Virgo, P. (2011). Citizen or subject: The politics of personal identity. ID Credentials. W. Atkings. London, UK, Smart Card Technology International: 16-19.

Warren, S. and L. Brandeis (1890). "The Right to Privacy." Harvard Law Review IV.

Weber, J. M., D. Malhotra, et al. (2005). "Normal acts of irrational trust: Motivated attributions, and the trust development process." Research in Organizational Behavior: An Annual Series of Analytical Essay and Critical Reviews 26: 75-101.

Wilcox, H. (2011). Juniper Transport White Paper. Basingstoke, UK, Juniper Research Limited: 6.

Wilcox, H. (2011). Scan and Go - Transport Ticketing on the Mobile. Hampshire, UK, Juniper Research: 6.

Wilcox, H. (2011). Hitting the N-Mark with NFC. Hampshire, UK, Juniper Research: 5.

Wilcox, H. (2011). Whitepaper - Mobile Money Goes Mainstream. Baginstoke, Hampshire, UK, Juniper Research Limited: 5.

Working Party, (2010). Article 29 Data Protection Working Party - Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications. Brussels, Belgium, Working Party: 11.

Yu, A. (2008). NFC and Future Mobile Technologies. Southbridge, MA, North East Regional Computing Programme: 19.

Zetter, K. (2009). "Medical Records: Stored in the Cloud, Sold on the Open Market." 2009, from http://www.wired.com/threatlevel/2009/10/medicalrecords.

Zimmer, M. (2010). Privacy Protection in the Next Digital Decade: "Trading Up" or a "Race to the Bottom". The Next Digital Decade Essays on the Future of the Internet. B. Szoka and A. Marcus. Washington D.C, Tech Freedom: 477-483.

Zmijewska, A. (2005). Evaluating Wireless Technologies in Mobile Payments – A Customer Centric Approach. Proceedings of the International Conference on Mobile Business (ICMB'05), Sydney, Australia, The IEEE Computer Society.

Zmijewska, A. and L. E. (2006). "Mobile Technology Adoption - A Case Study." Journal of WSEAS Transactions on Information Science and Applications 1(3): 96-104.

Zmijewska, A. and E. Lawrence (2006). Implementation Models in Mobile Payments. Proceedings of The IASTED International Conference on Advances in Computer Science and Technology (ACST), Puerto Vallarta, Mexico.

Zuba, R. (2008). NFC Successful Launch and Future Opportunities. mobilekom 2008. Austria: 21.