

Privacy, Identity and Security Concerns: Enterprise Strategic Decision Making and Business Model Development for Mobile Payments in NFC



DR. JONATHAN LIEBENAU
DR. SILVIA ELALUF-CALDERWOOD
DR. PATRIK KARRBERG
DEPARTMENT OF MANAGEMENT
LONDON SCHOOL OF ECONOMICS AND POLITICAL
SCIENCE (LSE)

TPRC 40

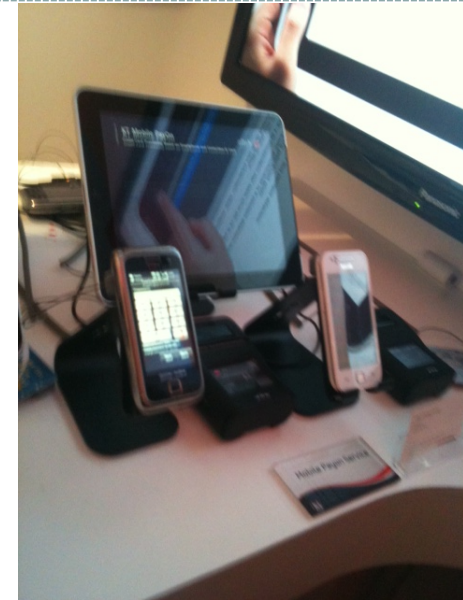
The Research Conference on Communication, Information and Internet Policy
George Mason University, Arlington VA, 2012

Relevance



- Since 1999, when Microsoft was called by the EU to Brussels to explain the do-NET passport, EU laws have held a stronghold on privacy (Goldsmith and Wu, 2006)
 - Facebook & photo tag (21 Sept!)
- “Data Protection Working Party Directive” is by default the highest privacy standard in the world with broad & stringent requirements (EU Article 29)
- 1998 EU data protection directive regulates “data controllers: that is, anyone who processes data they collect”

Examples of NFC cards



NFC as a test case for Privacy, Identity & Security



- Technology (huge expectation/slow adoption)
- Smartphones adaptation and ubiquity of usage
- Public transport operators early adopters (Mezghani, 2008)
- Location-based services in NFC (Pee, 2011)
- Verification & validation of hypotheses
- Control of settings at user vs. operator level (Shire, 2010)

Enterprise Strategic Decision Making



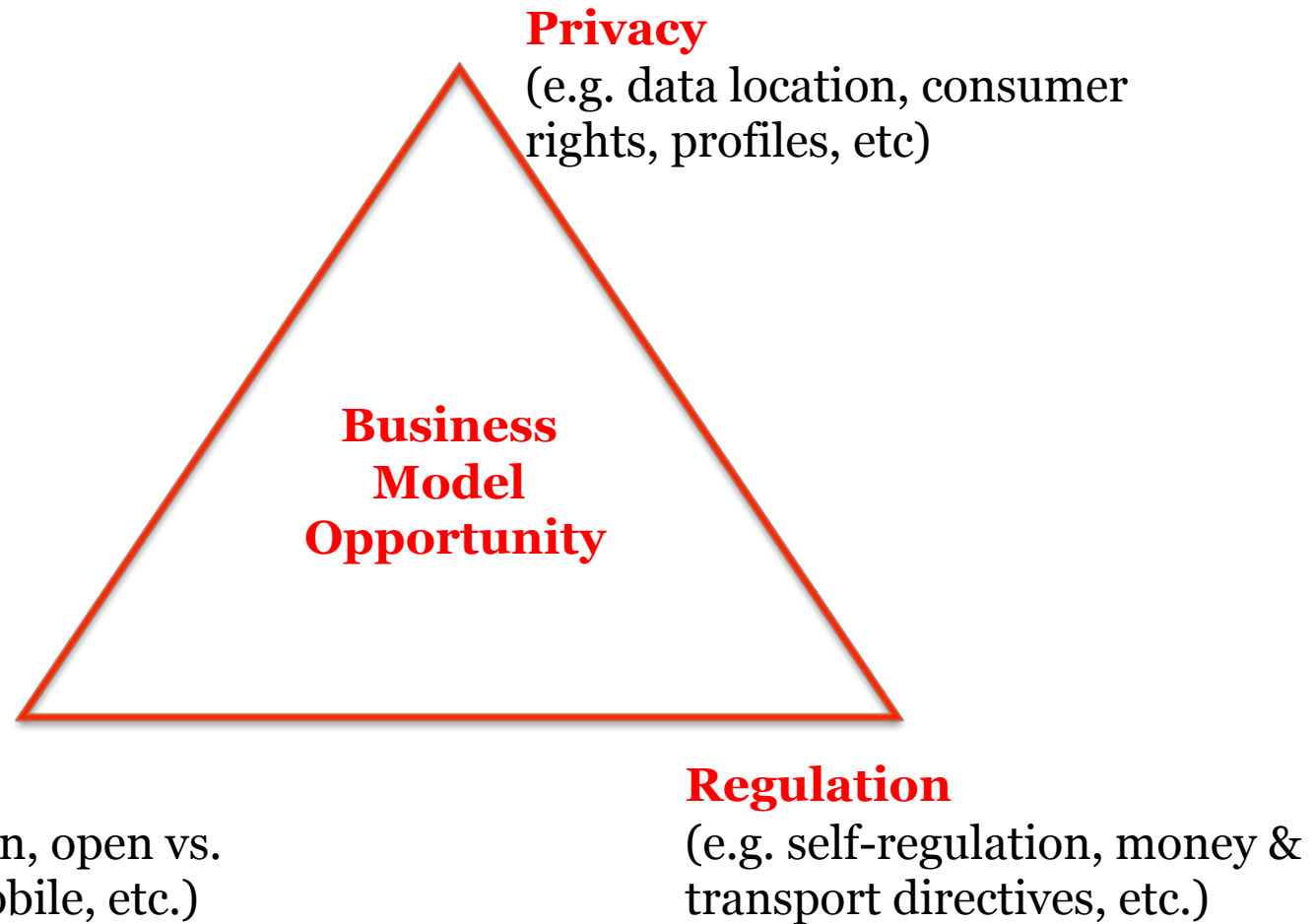
- Comparative study: variations among transport operators viz. creation of a “brand” payment system
- Private or partial-private ownership vs. state ownership (e.g. Octopus, Oyster)
- Different approaches: brand consolidation vs. revenue
- National regulation as a provider of a framework for the development of services (e.g. Finland)

Business Models Analysis



- Economic foundations of business models for implementing NFC
- Differences among architectures & technologies (Chan and Foster, 2009; Lewis, 2010)
- Regulatory regimes affecting transport operations & consumer rights (e.g. security vs. privacy)
- Arising privacy challenges (Avenel, 2011 and Bosckish et al, 2008)

Components of the Analytical Model



Privacy/Regulation/Technology



- Analysis of data by transport providers or 3rd parties
- Information shared between services & providers
- Emerging regulation protecting the privacy rights of individuals (see list in paper)
- Data leaks, reputational risk
- Redefining privacy re. consumers/users' perception; multiple identities

Strategies: Transport systems and payments



	London	Helsinki	Hong Kong	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 for 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.

Expanding beyond transport cards

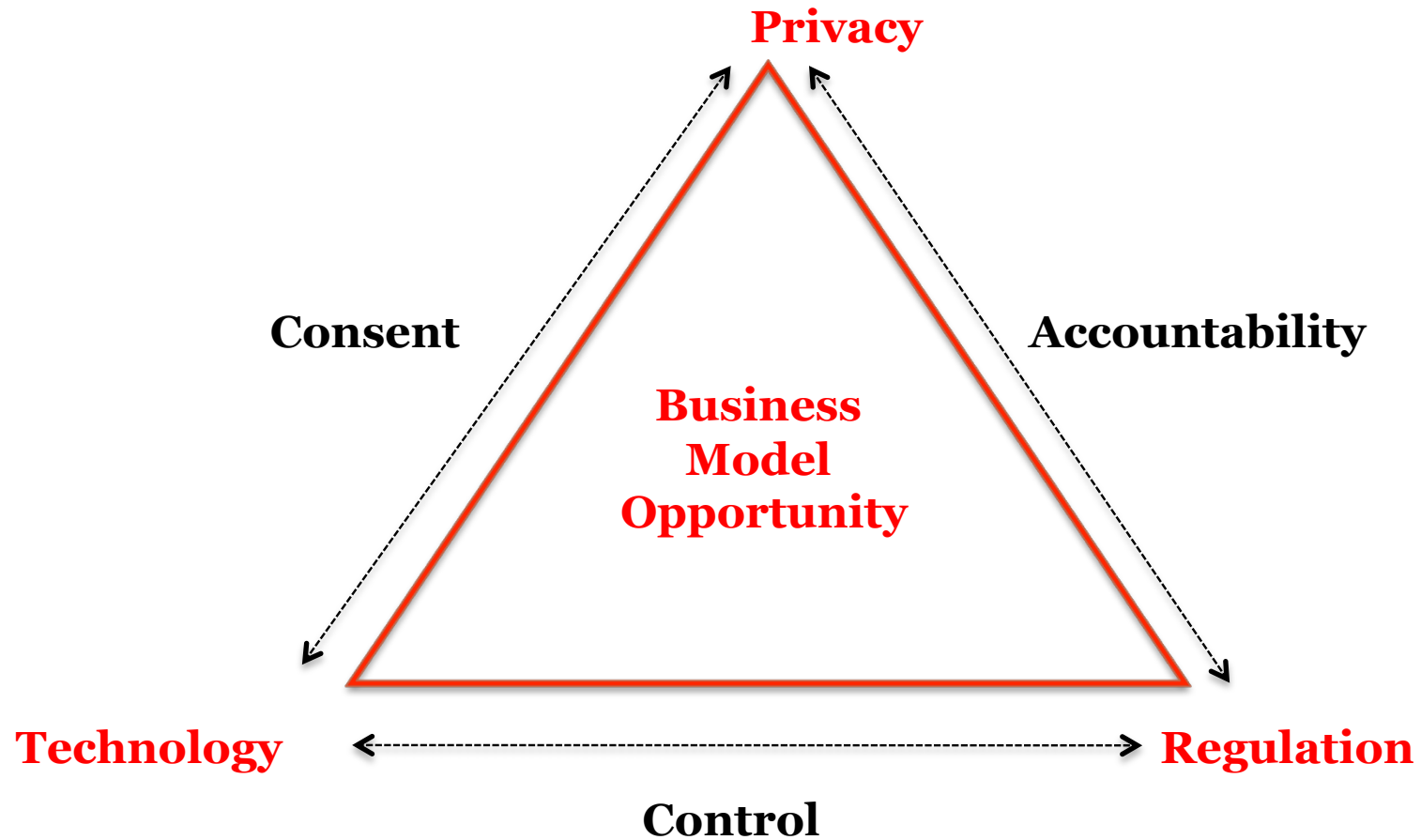


- Protection (regulation) vs. innovation
- Privacy control (mechanisms of control)

Leading to 3 themes:

- Control
- Consent
- Accountability

Consent, Control and Accountability



Rolling business models



- Trust, contracts, time and renewals for data collection and sharing (Bertele et al., 2011)
- Design for trust by services & type of requirements
- Self regulation vs. regulatory framework
- Evaluation of compliance; also a higher level of understanding of technical uses & variations (Miragliota et al., 2011)

Conclusions



- **New regulatory practices**
 - Self-regulation vs. controlled regulation
 - Move beyond “regulation vs. innovation” with “privacy” as “pawn”
- **Accountability for service** (e.g. Her Majesties Treasure 2010 Regulation to Implement E-Money Directives)
- **Governance of NFC practices vs. technology**
- **Stakeholders’ cooperation to enable sustainable NFC payment systems**

Some references



- Avenel, Y. (2011). SmartCards Trends - Smart- Security, Trust & Privacy. La Falaise, France, Omnipress Publication, Issue 6, Volume VII: 24.
- 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.
- 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.
- Chan, E. and P. Foster (2009). Octopus. Hong Kong, China, Center for Business Case Studies, Hong Kong University of Science and Technology: 28.
- Communities, C. o. t. E. (2009). Commission Recommendation on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio-Frequency Identification. Brussels, Belgium, Commission of the European Communities: 10.
- Goldsmith, J. and T. Wu (2006). Who Controls the Internet? : Illusions of a Borderless World. Oxford, Oxford University Press
- Her Majesty Treasury. (2010). Laying of regulations to implement the new E-Money Directive - Consultation Document. London, UK, HM Treasury: 112.
- Lewis, P. (2010). London's Oyster Card Revolution to Evolution. London, UK, Transport for London: 17.
- Miragliotta, G. and F. Renga (2011). Mobile Payment: Expectations vs Reality. Milan, Italy, Politecnico di Milano - Department of management, economics and industrial engineering (www.osservatori.tv): 16.
- Mezghani, M. (2008). Study of electronic ticketing in public Transport, European Metropolitan Transport Authorities (EMTA): 56
- Pee, L. G. (2011). Attenuating Perceived Privacy risk of Location-Based Mobile Services. European Conference of Information Systems 2011. Helsinki, Finland.
- Shire, C. (2010). How Secure is NFC? A review of the security needs of Transport Schemes using NFC. London, UK, Infineon Technologies: 20.